A Tort Perspective on Cyberbullying

*Denis Binder**

The Internet has opened the world to the rapid dissemination of knowledge. It has also, like every revolution, opened the door to new crimes and torts. The law is now responding to the new phenomenon of cyberbullying.

School bullies used to ply the hallways, schoolyards, and playgrounds. The traditional victims of bullying knew who their bullies were.

These traditional bullies still exist, but the Internet and social media have created a whole new class of bullies, who, often anonymously, from a distance, use the Internet, to electronically torment their victims through smart phones, tablets and personal computers, and any other forms of electronic communications on blogs, bulletin boards, chat rooms, Twitter, and their own websites. They post, text, hack, and instant message. Photos are photoshopped to picture a person in a false light. Their aim is to disparage, humiliate, or torment the victim. Social media empowers, but also destroys. The harassment can be felt 24/7. Occasionally the victim's distress has been so great that the victim has committed suicide.[1]

Attention is focused on teenage bullying both because it is very common and because teenagers often have insecurity issues as they traverse the difficult years between childhood and adulthood with hormones kicking in. Teenagers are also well known for sarcasm and meanness, both of which are manifested in cyberbullying incidents. The Internet, through its various electronic means, is an integral part of the culture and lifestyle of today's younger generation. They are electronically wired.

However, cyberbullying is not limited to students. Adults can also be perpetrators and victims.

---

* Professor of Law, Chapman University Dale E. Fowler School of Law. S.J.D. 1973, L.L.M. 1971, University of Michigan; J.D. 1970, A.B. 1967, University of San Francisco.

1 *See, e.g.*, Vidovic v. Mentor City Sch. Dist., 921 F. Supp. 2d 775 (N.D. Ohio 2013) (cyberbullying based on national origin).

Traditional bullying was physical, often with psychological complications. Today's cyberbullying is psychological, often with physical complications. Traditional bullying was limited in time and space. Today's cyberbullying can occur at any time on a global basis through the World Wide Web.

The prototypical case involved thirteen-year-old Megan Meier in O'Fallon, Missouri, an upper-middle-class community thirty-five miles northwest of St. Louis.[2] Megan suffered from depression since the third grade and was receiving medication for attention deficit disorder and bipolar syndrome.[3] She was teased for being fat. Megan had considered suicide in the past. Her friendship with Sarah Drew, a close friend, had recently ended.

Megan created a MySpace account. She shortly connected with sixteen-year-old Josh Evans.[4] The two bonded on the Internet. Megan was happy.

"Josh" was not Josh, though. Indeed, he did not exist. He was the creation of Lori Drew, Sarah's mother, who lived four doors away. Lori created Josh with Sarah and an eighteen-year-old employee, Ashley Grills, to determine if Megan was "trashing" her daughter. It evolved into a campaign to inflict pain on Megan. Lori had posted a photo of a boy, without the boy's permission, as Josh.

The online relationship turned negative when "Josh" sent this message: "I don't know if I want to be friends with you any longer because I heard you are not a very good friend." The exchanges became increasingly unfriendly. His final message said: "You are a bad person and everybody hates you. Have a shitty rest of your life. The world would be a better place without you."[5]

Megan was devastated and committed suicide in her bedroom the next day on October 16, 2006. This tragedy reverberated nationally.

The prosecutor for St. Charles County, Missouri, declined to prosecute because he could divine no crime under state law. Instead, the United States Attorney in Los Angeles proceeded with a felony conspiracy count and several misdemeanor charges

---

2 For a detailed analysis of the case, see Kristopher Accardi, *Is Violating an Internet Service Provider's Terms of Service an Example of Computer Fraud and Abuse?: An Analytical Look at the Computer Fraud and Abuse Act, Lori Drew's Conviction and Cyberbullying*, 37 W. ST. U. L. REV. 67 (2009).

3 Steve Pokin, *Megan's Story*, MEGAN MEIER FOUNDATION, http://www.meganmeierfoundation.org/megans-story.html [http://perma.cc/F9ML-Q3WK].

4 *Id.*

5 *Id.*

against Lori Drew for alleged violations of the Computer Fraud and Abuse Act.[6]

In essence, she posted on MySpace in violation of MySpace's terms of service. He claimed jurisdiction because MySpace, the host, is headquartered in Beverly Hills, California. Ashley Grills was granted immunity to testify against Lori. The criminal charges were based on Lori Drew (1) setting up the MySpace account under a fictitious name, (2) acquiring information about Megan, and (3) inflicting emotional distress upon Megan. The federal statute provides that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" has committed a crime.[7]

The jury convicted Lori Drew of three misdemeanors and deadlocked on the conspiracy charge. The federal district judge subsequently threw out the case, holding the federal statute did not apply.[8] It was unconstitutionally vague and failed to provide "minimal guidelines to govern law enforcement."[9]

The impact of the Megan Meier case and similar cases prompted states to enact cyberbullying statutes.[10] Irrespective of the availability of criminal law for cyberbullying, causes of action are available under tort law. They include defamation, intentional infliction of emotional distress, the prima facie tort, and state statutes, if available.

Potentially liable parties include the bully, parents of the bully, school districts, and Internet service providers ("ISPs").

I. STATUTES

A. Hate Crime Legislation

If the cyberbullying is based on the victim's sexual identity, race, religion, or sex, then existing hate crime statutes may apply. For example, California's Hate Crime Statute criminalizes crimes committed based on the following characteristics of the victim: disability, gender, nationality, race or ethnicity, religion,

---

6 18 U.S.C. § 1030 (2012).

7 *Id.*

8 United States v. Drew, 259 F.R.D. 449, 468 (C.D. Cal. 2009). The judge held the statute was unconstitutionally vague, had notice deficiencies, and did not provide minimal guidelines to govern law enforcement. *Id.* at 466–67.

9 *Id.* at 464.

10 One provision, in addition to general anti-bullying statutes, is to ban the creation of an impersonation website, as was done with "Josh Evans." *See, e.g.*, CAL. PENAL CODE § 528.5 (West 2016).

sexual orientation, or association with a person or group with those actual or perceived characteristics.[11]

Hate crime statutes should be a major cause of action in cyberbullying complaints in states with these statutes. Homophobic and racist statements seem to abound in cyberbullying cases. Many cases involve students committing suicide after being cyberbullied for being gay.[12] The New York case of *T.E. v. Pine Bush Central School District* is an example of cyberbullying based on religion.[13] Years of anti-Semitic taunting of Jewish students were not effectively addressed by the school district. The court held that the school's knowledge that the responses were inadequate can constitute deliberate indifference for purposes of liability.[14] The U.S. Supreme Court has held that a school district's "deliberate indifference" to a student's sexual harassment of another student violated Title IX of the Education Amendments of 1972.[15]

B. Cyberbullying Statutes

Every state, and the District of Columbia, has anti-bullying statutes. Their breadth and depth vary greatly. Many have been amended to include cyberbullying among the actionable offenses.[16] Questions to ask about these statutes are:

1) Are they criminal, civil, or both?

2) Do they provide a private cause of action?[17]

---

11 CAL. PENAL CODE §§ 422.55, 422.6 (West 2016).

12 *See, e.g.*, Walsh v. Tehachapi Unified Sch. Dist., 997 F. Supp. 2d 1071, 1073 (E.D. Cal. 2014).

13 T.E. v. Pine Bush Cent. Sch. Dist., 58 F. Supp. 3d 332 (S.D.N.Y. 2014) (lawsuit was brought pursuant to Title VI of the Civil Rights Act of 1964, 42 U.S.C. § 1983, and New York's Civil Rights Law).

14 *Id.* at 379; *see also* Zeno v. Pine Plains Cent. Sch. Dist., 702 F.3d 655, 673 (2d Cir. 2012) (racial taunting and harassment resulting in award of $1,000,000 plus fees and costs).

15 Davis *ex rel* LaShonda D. v. Monroe Cty. Bd. of Educ., 526 U.S. 629, 633 (1999).

16 ARK. CODE ANN. § 6-18-514 (West 2016); CONN. GEN. STAT. ANN. § 10-222d(a)(2) (West 2016); FLA. STAT. ANN. §§ 784.048(2), 1006.147(3)(b) (West 2016); GA. CODE ANN. § 20-2-751.4(a) (West 2016); MASS. GEN. LAWS ANN. ch. 71, § 37O(a); N.H. REV. STAT. ANN. § 193-F:4(II)(b) (West 2016); N.J. STAT. ANN. § 18A:37-14 (West 2016); N.Y. EDUC. LAW § 11(7) (McKinney 2016); S.D. CODIFIED LAWS § 13-32-15 (West 2016); TENN. CODE ANN. §§ 49-6-4502, 4503 (West 2016); VT. STAT. ANN. tit. 16, § 11(a)(32) (West 2016).

17 For example, California expressly grants a private cause of action. CAL. CIV. CODE § 52.1(b) (West 2016). On the other hand, the New Hampshire statute expressly provides that it does not create a private right of action for enforcement of the chapter against any school district, chartered public school, or the state. N.H. REV. STAT. ANN. § 193-F:9; *see also* Gauthier v. Manchester Sch. Dist., SAU #37, 123 A.3d 1016, 1019–20 (N.H. 2015) (holding that § 193-F:9 barred a lawsuit brought against the school district for failing to notify the parent of bullying within forty-eight hours).

3) What do they cover?[18]

4) What are the penalties?

5) Do they only apply to schools?

6) If so, do they apply to off-campus bullying, or just on-campus acts involving school computers, servers, and networks?[19]

7) Do they apply to private schools as well as public schools?[20]

8) Do they apply to the parents of minor perpetrators?

9) Do they apply to all perpetrators, minor or adult?

10) Do they grant immunity to school boards, administrators, or employees?[21]

A problem with such statutes is that if written or construed too broadly, they may interfere with the First Amendment freedom of speech rights of the student.[22] The Supreme Court held in *Tinker v. Des Moines Independent Community School District* that student protests are protected by the Free Speech Clause of the First Amendment.[23] The dividing line between protected speech and unprotected speech is unsettled, but it is clear that threats of physical violence are not protected.[24] The

---

18 For example, the North Carolina anti-bullying statute expressly includes building a false profile or website, posing as a minor in an internet chat room, email or instant messaging, or following a minor online. N.C. GEN. STAT. ANN. § 14-458.1 (West 2016).

A commonality in the statutes is to reference cyberbullying in terms of "electronic communications devices." *See, e.g.*, CAL. PENAL CODE § 653.2(b) (West 2016). For an analysis of California's approach to cyberbullying, see generally Atticus N. Wegman, *Cyberbullying and California's Response*, 47 U.S.F. L. REV. 737 (2013).

19 For example, New Hampshire's anti-bullying act applies to both on-campus and off-campus "if the conduct interferes with a pupil's educational opportunities or substantially disrupts the orderly operations of the school or school-sponsored activity or event." N.H. REV. STAT. ANN. § 193-F:4(I)(b); *see also* TENN. CODE ANN. § 49-6-4502(a)(3)(B) (West 2016).

20 California permits a private postsecondary educational institution to adopt rules and regulations designed to prevent hate violence. CAL. EDUC. CODE § 94367(f) (West 2016).

21 For example, Tennessee's statute grants immunity to school employees who promptly report acts of harassment, intimidation, bullying, or cyberbullying to the appropriate official in accordance with the procedures set forth in the school district policies. TENN. CODE ANN. § 49-6-4505(c) (West 2016); *see also* CONN. GEN. STAT. ANN. § 10-222*l*(a) (West 2016).

22 *See, e.g.*, People v. Marquan M., 19 N.E.3d 480, 486 (N.Y. 2014).

23 Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969) (holding students wearing black armbands to protest the Vietnam War were protected under the First Amendment).

24 For detailed analysis of the First Amendment issue, see generally Matthew Fenn, *A Web of Liability: Does New Cyberbullying Legislation Put Public Schools in a Sticky Situation?*, 81 FORDHAM L. REV. 2729 (2013); Daniel Marcus-Toll, *Tinker Gone Viral: Diverging Threshold Tests for Analyzing School of Regulation of Off-Campus Digital Student Speech*,

Court held that prohibitions on expressive conduct could be upheld if the conduct "would 'materially and substantially interfere with the requirements of appropriate discipline in the operation of the school.'"[25]

In *United States v. Alvarez*,[26] the Supreme Court noted that the First Amendment does not protect fighting words, true threats, incitements, obscenity,[27] child pornography, fraud, defamation, or statements integral to criminal conduct.[28] Websites for the purchase of illegal drugs are not protected.[29] A posting about killing a teacher should not be protected.[30]

On the other hand, the parody of a school principal should be protected speech.[31] Similarly, bad reviews and student comments on a professor's teaching are protected speech.[32] The embarrassment of administrators is not a ground for banning student non-school sponsored material.[33]

II. ON-CAMPUS OR OFF-CAMPUS CYBERBULLYING

We start with the premise that school boards have more power to regulate on-campus speech and conduct than off-campus speech and conduct. The issue remains open as to the extent of the jurisdiction of school boards to punish off-campus cyberbullying. Much of the traditional schoolyard bullying occurred on school grounds. Today, anyone with an electronic connection anywhere in the world can initiate a cyberbullying attack. Anyone else in the world can join in if the website used to incite the attack is an open one. The communications may be through an off-campus web host. The only "on-campus" link might be that a few students, teachers, or administrators will see it and discuss it at school.

The Supreme Court held in *Morse v. Frederick*[34] that the school could act against on-campus vulgar and lewd speech. However, Justice Brennan, in his concurring opinion in *Bethel*

---

82 FORDHAM L. REV. 3395 (2014); Renee L. Servance, *Cyberbullying, Cyber-Harassment and the Conflict Between Schools and the First Amendment*, 2003 WIS. L. REV. 1213.

25 *Tinker*, 393 U.S. at 509 (citing Burnside v. Byars, 363 F.2d 744, 749 (5th Cir. 1966)).

26 United States v. Alvarez, 132 S. Ct. 2537 (2012).

27 *Id.*; *see also* Bethel Sch. Dist. No. 403 v. Fraser, 478 U.S. 675, 685 (1986) (holding the school district was able to prohibit and punish lewd and vulgar speech or behavior).

28 *Alvarez*, 132 S. Ct. at 2544.

29 Morse v. Frederick, 551 U.S. 393, 397 (2007).

30 Wisniewski v. Bd. of Educ. of Weedsport Cent. Sch. Dist., 494 F.3d 34 (2d Cir. 2007).

31 Layshock v. Hermitage Sch. Dist., 496 F. Supp. 2d 587 (W.D. Pa. 2007); *see also* Beverly v. Watson, 78 F. Supp. 3d 717 (N.D. Ill. 2015) (attempt by administration to shut down an off-campus professor blog critical of the administration).

32 Schmisky v. Higgins, 2014 WL 1710962 (Cal. Ct. App. Apr. 29, 2014).

33 Burch v. Barker, 861 F.2d 1149 (9th Cir. 1988).

34 *Morse*, 551 U.S. at 410.

School District v. Fraser, wrote that the situation would be different with off-campus speech: "If respondent had given the same speech outside of the school environment, he could not have been penalized simply because government officials considered his language to be inappropriate."[35] Chief Justice Roberts in his majority opinion in *Morse v. Frederick*[36] echoed Justice Brennan's concurrence in *Fraser*: "Had Fraser delivered the same speech in a public forum outside the school context, it would have been protected."[37]

State and federal courts have wrestled with the defining line between the ability of school boards to discipline off-campus web postings that reflect poorly on some students, teachers, or administrators. A consensus seems to be evolving around the issue of whether or not the act had a substantial interference (substantial disruption) with school discipline or the rights of others. Looking to language in *Tinker*, "conduct by the student, in class or out of it, which for any reason . . . materially disrupts classwork or involves substantial disorder or invasion of the rights of others is, of course, not immunized . . . ."[38]

Courts have upheld disciplinary actions against students whose off-campus postings carried over to the school campus, such as in *Kowalski v. Berkeley County School*.[39] The student's off-campus website singled out a specific student for harassing, bullying, and intimidation, tagging her with herpes.

Postings that interfere with the work and discipline of the school, that create a substantial disorder and disruption in the school, that interfere with students' rights to be secure and left alone, are subject to disciplinary action by the school.[40]

An off-campus rap entitled "PSK The Truth Needs to Be Told," which named two teachers and described violent acts against them, was not protected speech.[41] The rap was directed at the school and contained threats of physical violence.[42]

Yet, off-campus electronic postings are not necessarily subject to school discipline, even if made directly toward students at the school. For example, a student followed up on a creative

---

35 Bethel Sch. Dist. No. 403 v. Fraser, 478 U.S. 675, 688 (1986).

36 *Morse*, 551 U.S. at 393.

37 *Id.* at 405.

38 Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 513 (1969).

39 Kowalski v. Berkeley Cty. Sch., 652 F.3d 565 (4th Cir. 2011).

40 *Id.* at 573–74; *see also* Doninger v. Niehoff, 527 F.3d 41 (2d Cir. 2008); Boucher v. Sch. Bd. of Sch. Dist. of Greenfield, 134 F.3d 821 (7th Cir. 1998).

41 Bell v. Itawamba Cty. Sch. Bd., 799 F.3d 379 (5th Cir. 2015).

42 *Id.*

writing assignment the previous year of writing your own obituary by posting two mock obituaries of students at the school. The page said the site was not sponsored by the school and was for entertainment only. The student also asked readers to submit suggestions on who should die next, i.e. receive a mock obituary.

The media called it a "hit list," but it was clear that no student at school felt threatened by it. The court overturned the student's discipline and held the posting was protected speech.[43]

An off-campus tweet not posing a risk to the school was protected by the First Amendment.[44] Off-campus postings, that are neither school-sponsored nor at a school-sponsored event, and which do not present a substantial disruption at the school, are not subject to school discipline.[45]

III. DEFAMATION

Defamation, usually libel since the defamation is by written means, is generally defined as the publication of a false statement that holds one up to hatred, contempt, or ridicule, or causes one to be shunned or avoided. The publication need only be to one person.

Defamation would clearly apply in cyberbullying cases where the perpetrator is publishing a defamatory statement about the victim. The false statement constitutes libel since the electronic statement is in written form.

California defines libel as "a false and unprivileged publication by words . . . which expose any person to hatred, contempt, ridicule or obloquy, or which causes him to be shunned or avoided, or has a tendency to injure him in his occupation."[46]

Anyone publishing or republishing[47] the defamatory remark can be liable as a publisher. That would seemingly include the ISP. However, Congress in the Communications Decency Act of 1996, exempted ISPs from liability as publishers in Section 230, commonly referred to as the Internet Freedom and Family Empowerment Act. The section provides: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[48] Courts have held the immunity applies

---

43 Emmett v. Kent Sch. Dist. No. 415, 92 F. Supp. 2d 1088 (W.D. Wash. 2000).
44 Sagehorn v. Indep. Sch. Dist. No. 728, 2015 WL 4744482 (D. Minn. Aug. 11, 2015).
45 J.S. v. Blue Mountain Sch. Dist., 650 F.3d 915, 933 (3d Cir. 2011).
46 CAL. CIV. CODE § 45 (West 2016).
47 Khawar v. Globe Int'l, Inc., 965 P.2d 696, 704 (Cal. 1998).
48 47 U.S.C. § 230(c)(1) (2012); *see also* Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006).

even if the third party submitted a false profile[49] or if the ISP acted negligently.[50]

Under the privilege of fair comment, the common law generally protects the right to express an opinion, such as negative reviews or statements, but not false facts about movies, books, plays, and politicians, not to mention administrators and teachers.[51]

IV. INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

The tort of intentional infliction of emotional distress is a well-developed cause of action for a young tort that traces back to the mid-twentieth century.[52] The Restatement (Third) of Torts provides: "[a]n actor who by extreme and outrageous conduct intentionally or recklessly causes severe emotional harm to another is subject to liability for that emotional harm and, if the emotional harm causes bodily harm, also for the bodily harm."[53]

California adopted the tort in *State Rubbish Collectors Association v. Siliznoff*,[54] which involved physical threats, and then extended it to racial and ethnic insults in *Alcorn v. Anbro Engineering, Inc.*[55] The next, logical step will be to formally extend it to cyberbullying.

V. PRIMA FACIE TORT

The early common law was very strict in its pleadings. If a cause of action did not fit into one of the established writs, then it could not proceed. Thus, an intentional, wrongful act, no matter how egregious, which did not fit into such traditional writs as assault, battery, false imprisonment, trespass to chattels, conversion, or trespass, would fail.

The American common law therefore developed the catch-all "prima facie" tort,[56] based on dicta by Lord Bowen in the 1889

---

49 Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).

50 Green v. America Online (AOL), 318 F.3d 465 (3d Cir. 2003).

51 *See* RESTATEMENT (SECOND) OF TORTS § 566 (AM. LAW INST. 1977); *see also* Baker v. L.A. Herald Exam'r, 721 P.2d 87 (Cal. 1986); Schimsky v. Higgins, 2014 WL 1710962 (Cal. Ct. App. Apr. 29, 2014) (protecting inconsistently bad evaluations and reviews of adjunct professor).

52 For one of the most famous cases exemplifying this cause of action, see *State Rubbish Collectors Ass'n v. Siliznoff*, 240 P.2d 282 (Cal. 1952).

53 RESTATEMENT (THIRD) OF TORTS § 46 (AM. LAW INST. 2012).

54 *State Rubbish Collectors Ass'n*, 240 P.2d at 282.

55 Alcorn v. Anbro Eng'g, Inc., 468 P.2d 216 (Cal. 1970).

56 For a history of the prima facie tort, see Kenneth J. Vandevelde, *A History of Prima Facie Tort: The Origins of a General Theory of Intentional Tort*, 19 HOFSTRA L. REV. 447 (1990). *See* Morris D. Forkosch, *An Analysis of the "Prima Facie Tort" Cause of*

British case of *Mogul Steamship Co. v. McGregor, Gow & Co.*[57] He wrote: "[I]ntentionally to do that which is calculated in the ordinary course of events to damage, and which does, in fact, damage another in that other person's property or trade, is actionable if done without just cause or excuse."[58]

Justice Oliver Wendell Holmes advanced the prima facie tort in the 1904 Supreme Court case of *Aikens v. Wisconsin*: "It has been considered that, prima facie, the intentional infliction of temporal damage is a cause of action, which, as a matter of substantive law, whatever may be the form of pleading, requires a justification if the defendant is to escape."[59] He cited *Mogul Steamship* and the earlier Massachusetts decision in *Walker v. Cronin*.[60]

The prima facie tort remains underutilized and underrecognized. Under the prima facie tort, anyone who intentionally causes injury to another shall be liable unless the acts were privileged. The Restatement (Second) of Torts provides:

> One who intentionally causes injury to another is subject to liability to the other for that injury, if his conduct is generally culpable and not justifiable under the circumstances. This liability may be imposed although the actor's conduct does not come within a traditional category of tort liability.[61]

The prima facie tort has not been uniformly adopted in the United States. Jurisdictions are split on establishing the prima facie tort cause of action,[62] with many jurisdictions not recognizing it.[63] Others only allow the prima facie tort to proceed if no other cause of action exists.[64]

Action, 42 CORNELL L. REV. 465 (1957); Note, *The Prima Facie Tort Doctrine*, 52 COLUM. L. REV. 503 (1952). In New York, see Note, *The Prima Facie Tort Doctrine in New York—Another Writ?*, 42 ST. JOHN'S L. REV. 530 (1968).

57 Mogul S.S. Co. v. McGregor, Gow & Co., 23 QBD 598 (1889), *aff'd.* [1892] App. Cas. 25 (HL).

58 *Id.* at 613.

59 Aikens v. Wisconsin, 195 U.S. 194, 204 (1904)

60 Walker v. Cronin, 107 Mass. 555, 562 (1871) ("The intentional causing of such loss to another, without justifiable cause, and with the malicious purpose to inflict it, is of itself a wrong.").

61 RESTATEMENT (SECOND) OF TORTS § 870 (AM. LAW INST. 1979).

62 States that have recognized the prima facie tort include: California (Cervantez v. J.C. Penney Co., 156 Cal. Rptr. 198, 206 (Cal. 1979)); Delaware (Kaye v. Pantone, Inc., 395 A.2d 369, 373 (Del. Ch. 1978)); Missouri (Porter v. Crawford & Co., 611 S.W.2d 265, 268 (Mo. Ct. App. 1980)); and New York (Advance Music Corp. v. Am. Tobacco Co., 70 N.E.2d 401, 403 (N.Y. 1946)).

63 These jurisdictions include: District of Columbia (Nix v. Hoke, 139 F. Supp. 2d 125, 132 (D. D.C. 2001)); Florida (Whitney Info. Network, Inc. v. Gagnon, 353 F. Supp. 2d 1208, 1213 (M.D. Fla. 2005)); Ohio (Phung v. Waste Mgmt., Inc., 532 N.E.2d 195, 200 (Ohio App. 1988)); Pennsylvania (Hughes v. Halbach & Braun Indus., Ltd., 10 F. Supp. 2d

Cyberbullying should fall into the prima facie category in jurisdictions which accept the tort because of the intentional outrageousness of the act lacking justification. The intent is clearly to injure the victim.

VI. CALIFORNIA

Very few civil cyberbullying cases have worked their way through the judicial system. A California case, *D.C. v. R.R.*,[65] is not a good auger for the future even though California makes it illegal to use any electronic communication with intent to instill fear or harass another person.[66]

Daniel Caplin, a fifteen-year-old student at the private Harvard-Westlake School in Los Angeles, was an aspiring actor and singer with several gigs and an album coming out. He opened a website to promote his activities and allowed members of the public to post comments on a "guest book."[67] The responses were not always what he expected.

The favorable comments were accompanied by scurrilous comments, including homophobic slurs and threats of violence, which are all too common in cyberbullying scenarios. Thirty-four posts were viewed as offensive with six perceived as death threats. Twenty-three asserted Daniel was gay, some using the word "faggot."[68] One student wrote: "I want to rip out your fucking heart and feed it to you . . . I've . . . wanted to kill you. If I ever see you I'm . . . going to pound your head in with an ice pick. Fuck you, you dick-riding penis lover. I hope you burn in hell."[69]

Daniel's father, Lee Caplin, contacted Harvard-Westlake and the Los Angeles Police Department, which in turn contacted the FBI. The LAPD viewed the threats as credible and suggested the Caplins move. They moved to Northern California, placed Daniel in a school there, and the father commuted back and forth between Northern California and his business in Los Angeles. The Harvard-Westlake student newspaper published two articles

---

491, 499 (W.D. Pa. 1998)); Texas (Perdue v. J.C. Penney Co., 470 F. Supp. 1234, 1239 (S.D.N.Y. 1979) (applying Texas law)); and Virginia (Unlimited Screw Prod., Inc. v. Malm, 781 F. Supp. 1121, 1130 (E.D. Va. 1991)).

64 *See, e.g.*, Richard A. Pulaski Const. Co. v. Air Frame Hangers, Inc., 950 A.2d 868, 876 (N.J. 2008) (New Jersey); *see also* Long v. Beneficial Fin. Co., 330 N.Y.S.2d 664, 668 (N.Y. App. Div. 1972) (New York).

65 D.C. v. R.R., 106 Cal. Rptr. 3d 399 (Ct. App. 2010).

66 CAL. PENAL CODE § 653.2 (West 2016).

67 *D.C.*, 106 Cal. Rptr. 3d at 404–05.

68 *Id.* at 407–08.

69 *Id.* at 405. A more detailed version of the comments is found in the dissent. *Id.* at 440–45.

about the case, one of which disclosed the Caplins' new residence and Daniel's school. Harvard-Westlake did not suspend or expel the offending students. The Los Angeles District Attorney exercised prosecutorial discretion and declined to prosecute.[70]

Daniel and his parents, Lee and Gina Caplin, filed suit against six students and their parents, Harvard-Westlake School, the school's Board of Directors, and three school employees. The original complaint contained eleven causes of action, including: negligence, assault upon another with death threats and hate crimes, invasion of privacy, defamation, intentional infliction of emotional distress, negligent infliction of emotional distress, fraud in the inducement of a contract, and various conspiracy counts attached to these claims.[71] A statutory violation of California's Hate Crime Laws[72] was added later.[73]

Defendants sought to dismiss the case on several grounds, including: violation of California's anti-SLAPP suit statute,[74] protected speech pursuant to the First Amendment, and on a factual basis, the statement was meant as a joke, intended as "jocular humor."[75] The anti-SLAPP statute was enacted to protect public participants, especially opponents, of projects against lawsuits by the proposal's developers and supporters with the intent of muzzling the opponents. The statute is broadly written: "A cause of action against a person arising from any act of that person in furtherance of the right of petition or free speech under the United States Constitution or California Constitution in connection with a public issue shall be subject to a special motion to strike . . . ."[76]

The result is that the statute is often raised by other defendants, such as cyberbullies who claim both First Amendment protections and the statute as legal defenses. They claim that their views represent a matter of public importance.

The vicarious liability of the parents, if proven, is limited by statute to $25,000.[77] The case against the parents of the alleged cyberbully in *Caplin v. Harvard-Westlake* was subsequently

---

70 The Assistant District Attorney assigned to the case filed a declaration "stating that, based on the evidence, the district attorney's office declined to prosecute any of the students who had posted messages on D.C.'s Web site." *Id.* at 412.

71 D.C. v. Harvard-Westlake Sch., 98 Cal. Rptr. 3d 300, 304 (Ct. App. 2009).

72 CAL. CIV. CODE §§ 51.7, 52.1 (West 2016).

73 *D.C.*, 106 Cal. Rptr. 3d at 406.

74 CAL. CIV. PROC. CODE § 425.16 (West 2016).

75 Caplin v. Harvard-Westlake Sch., No. BC 332406, 2008 WL 4721598, at *2 (Cal. Super. Ct. Mar. 12, 2008).

76 CIV. PROC. § 425.16.

77 CIV. § 1714.1.

dismissed.[78] Other courts have reiterated the common law view that parents are not vicariously liable for the acts of their children, but can be liable for negligence in failing to supervise or control their children. For example, negligence could lie in not removing the offending page after learning of its existence.[79]

Harvard-Westlake invoked the mandatory arbitration provision in the school's enrollment contract. The provision provided the prevailing party would receive attorney fees and costs. The arbitrator held for Harvard-Westlake and awarded the school $521,227.68 from the parents. The California Court of Appeals held that only the prevailing plaintiff can recover attorney fees under California's Hate Crime Statute.[80] These fees were therefore improperly awarded and the case was remanded for reconsideration.[81] The court on remand awarded $208,928.34 in attorney fees and costs against the plaintiff parents, Lee and Gina Caplin, with the statutory rate of interest added to it.[82]

California has since enacted a statute that now purports to bar this type of clause in cases similar to that in *D.C. v. Harvard-Westlake*.[83]

CONCLUSION

We are still in the early days of the computer revolution. Social media has transformed the old schoolyard bully into the cyberbully. The schoolyard bully's anti-social behavior was usually limited in time and space. The victim could usually identify the bully.

Today's cyberbully can anonymously attack anyone anytime from anywhere with an internet connection. The resulting psychological injury may be severe in vulnerable victims, sometimes leading to suicides. The cyberbullies, often teenagers, can be especially malevolent, clever, and creative in their actions, ranging from threats to defamation. Teenagers who could never be a physical bully can easily become a cyberbully.

The law, both statutory and common, is responding to the new phenomenon of cyberbullying. However, an overall consensus has yet to emerge. In addition, resolution may depend

---

78 Caplin v. Harvard-Westlake Sch., No. BC 332406, 2011 WL 10653443, at *1 (Cal. Super. Ct. Nov. 1, 2011).

79 *See* Boston v. Athearn, 764 S.E.2d 582, 587 (Ga. Ct. App. 2014).

80 D.C. v. Harvard-Westlake Sch., 98 Cal. Rptr. 3d 300, 323 (Ct. App. 2009).

81 *Id.* at 325.

82 *Caplin*, 2011 WL 10653443, at *1.

83 CAL. CIV. CODE § 51.7 (West 2016).

upon a United States Supreme Court decision because of an ambiguity in students' rights of free speech from an off-campus source. Prosecutors are often unwilling to bring criminal charges because of a lack of clarity in the criminal law.

Legislatures are mandating that school districts adopt anti-bullying policies and procedures. Less than half, though, have to adopt cyberbullying measures.

A larger gap exists in that many statutes only apply to public schools. Courts will thereby have to apply, with the flexibility of the common law, existing rules in defamation, emotional distress, and the prima facie tort to the new cyber tort.

Moore's Law Versus "Man's" Law? How Cybersecurity and Cyber Terror Government Policies May Help or Hurt Entrepreneurial Startups

*David Groshoff**

"Creating malware is bad, but if you sell it to police, it becomes okay. . . . We are not lawyers, we are hackers, and we know that any kind of rules can, and will, be bypassed. It is our job."[1]

—Raphael Vinot

INTRODUCTION

In 1965, Fairchild Semiconductor's Gordon Moore (later co-founder of Intel Corporation) indicated that "the number of transistors capable of being placed on a chip or integrated circuit quadruples every three years due to innovations and the march of technology."[2] This phenomenon has become known as "Moore's Law,"[3] with indications that Moore's Law has become exponentially faster in moving technology forward.[4]

The Internet as we know it today was essentially invented in the 1970s, and the world wide web was invented in the 1990s.[5]

---

* Chair, and Associate Professor of Business, American Jewish University, Los Angeles. Ed.M., Harvard University; J.D., The Ohio State University; M.B.A., Northern Kentucky University; B.A., Indiana University; former founding General Counsel of DreamFund.com, an infrastructure software company founded by the 2007 National Entrepreneur of the Year and three-time *Inc. 500* CEO Kent Plunkett. I thank Kent Plunkett, Yong Zhang, Peter Crosby, and Mi Tang for their assistance in understanding cybersecurity from the entrepreneur's perspective. The Article is meant to be gender-neutral, and the non-gender-neutral language in the Article's title was employed for alliteration.

1 Raphael Vinot, *On Ethics in Information Technology*, BOINGBOING (June 13, 2015, 5:00 AM), http://boingboing.net/2015/06/13/on-ethics-in-information-techn.html [http://perma.cc/ZD7G-WSP2].

2 Peter Harsha, *IT Research and Development Funding*, *in* CHASING MOORE'S LAW, INFORMATION TECHNOLOGY POLICY IN THE UNITED STATES 1, 23 (William Aspray ed., 2004); *see also* Steve Mosier, *Telecommunications and Computers: A Tale of Convergence*, *in* CHASING MOORE'S LAW, INFORMATION TECHNOLOGY POLICY IN THE UNITED STATES, *supra*, at 29, 37.

3 Mosier, *supra* note 2, at 37.

4 *See* Harsha, *supra* note 2, at 23; Mosier, *supra* note 2, at 37.

5 *See* Mosier, *supra* note 2, at 35–36.

Moore's Law likely applies to the Internet[6] and web as well, for good and bad, with the bad meaning that laws, rules, regulations, and policy levers cannot keep up with a rapidly moving, technology-driven economy, which has led to very recent and well-publicized cybersecurity breaches that this Symposium and this Article research and discuss.

Perhaps the most widely known cyberattack in the paradigm existing during the past several years occurred at the former Dayton-Hudson Corporation, now known as Target Corporation.[7] In this cyber breach, called a "watershed moment" in Target's hometown newspaper by at least one expert,[8] the hackers captured customer data from payment cards via malware that had unknowingly been installed in Target's computer system through a Target vendor. While the cybersecurity breach against Target occurred in 2013, affected approximately 110 million Target customers, and was the end-result of a so-called "phishing scam" from a vendor,[9] the case has already

---

6 In 1995, the Federal Network Council officially defined the Internet as:

> the global communication system that—(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

Id. at 36 (citing *Definition of "Internet,"* NETWORKING & INFO. TECH. RES. & DEV. (NITRD) PROGRAM (Oct. 24, 1995), http://www.itrd.gov/fnc/Internet_res.html [http://perma.cc/6L45-Z9ET]).

7 *See, e.g.*, *Inside Target Corp., Days after 2013 Breach*, KREBS ON SECURITY (Sept. 21, 2015, 12:01 AM), http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/ [http://perma.cc/M7DD-SAS8] (indicating that Target has since hired outside consultants). Target also has created a so-called "cyber-fusion center" to improve security and sponsored a national cybersecurity forum. *See Inside Target's Cyber Fusion Center*, A BULLSEYE VIEW (July 21, 2015), https://corporate.target.com/article/2015/07/cyber-fusion-center [http://perma.cc/5AUT-7XCL] (indicating that Target Corp. planned to invest over $1 billion in cybersecurity in 2015).

8 Tom Web, *Cyber–Security Expert: Target Case is 'Watershed Moment,'* TWINCITIES.COM (Feb. 2, 2014, 12:01 AM), http://www.twincities.com/ci_25047596/cyber-security-expert-target-case-is-watershed-moment [http://perma.cc/DB4W-8YZQ].

9 Dan Goodin, *Epic Target Hack Reportedly Began with Malware-Based Phishing E-mail: Attack Hit Contractor Two Months Before the Compromise of 40 Million Payment Cards*, ARS TECHNICA (Feb. 12, 2014, 1:00 PM), http://arstechnica.com/security/2014/02/epictarget-hack-reportedly-began-with-malware-based-phishing-e-mail/ [http://perma.cc/7H35-A7DQ]. Initially,

> 'phishing' campaigns typically involved an e-mail that appeared to be coming from [an entity] convincing users they needed to change their passwords or provide some piece of information . . . . A fake web page and users' willingness to fix the nonexistent problem led to account takeovers and fraudulent transactions.
>
> Phishing campaigns have evolved in recent years to incorporation installation of malware as the second stage of the attack.

been included in business school and management program books.[10]

This cyber breach could cost Target several billion dollars, and that is before private litigation costs.[11] Target did maintain a cybersecurity insurance policy that covered approximately $90 million, according to an S&P estimate in June 2015.[12] Further, the cyber breach caused Target executives to testify before Congress and forced the company to face federal and state investigations relative to how the cybersecurity breach occurred. In response to a Secret Service official's statement that what occurred to Target was "highly technical and sophisticated," Target's CEO, Greg Steinhafel, asserted that the statement "show[ed] [that] it's not just our operation. It would be hard for any retailer to withstand this."[13]

Despite government calls against Target in early 2014, later that year, the federal government itself announced that its Office of Personnel Management was hacked, potentially compromising the personal data of approximately 4 to 20 million existing and former federal employees.[14] U.S. officials blamed this breach on hackers from China, possibly constituting cyberespionage, as "Chinese state-sponsored hackers are the leading suspects," who relied on a method of attack known as spear phishing.[15]

VERIZON, 2015 DATA BREACH INVESTIGATIONS REPORT 12 (2015), http://www.verizonenterprise.com/DBIR/2015/. In 2013, more than two-thirds of cyber-espionage compromising incidents involved phishing. *Id.* Approximately five malware events occur every second, which is after controls including intrusion prevention systems ("IPS"), intrusion detection systems ("IDS"), firewalls, and spam filters have done their work. *Id.* at 21.

10 *See, e.g.*, ANGELO KINICKI & BRIAN K. WILLIAMS, MANAGEMENT: A PRACTICAL INTRODUCTION 37–38 (7th ed. 2016).

11 *See, e.g.*, Ashlee Kieler, *Target to Face Class-Action Lawsuit from Banks over Data Breach*, CONSUMERIST (Sept. 16, 2015), http://consumerist.com/2015/09/16/target-to-face-class-action-lawsuit-from-banks-over-data-breach/ [http://perma.cc/GCU3-RJD8].

12 *See* Sonali Basak, *Worried About a Cyber-Apocalypse? AIG Wants to Sell You a Policy*, BLOOMBERG BUSINESS (July 22, 2015, 2:00 AM), http://www.bloomberg.com/news/articles/2015-07-22/worried-about-a-cyber-apocalypse-aig-wants-to-sell-you-a-policy [http://perma.cc/D2DG-RZR6].

13 Monica Langley, *Inside Target, CEO Gregg Steinhafel Struggles to Contain Giant Cybertheft*, WALL ST. J. (Feb. 18, 2014, 10:48 PM), http://www.wsj.com/articles/SB10001424052702304703804579382941509180758.

14 *See, e.g.*, Ellen Nakashima, *Chinese Breach Data of 4 Million Federal Workers*, WASH. POST (June 4, 2014), https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html [http://perma.cc/LUN2-TXBP]; *cf. infra* note 44 (referring to a twenty-million number).

15 Josh Chin, *Cyber Sleuths Track Hacker to China's Military*, WALL ST. J. (Sept. 23, 2015, 5:00 PM), http://www.wsj.com/articles/cyber-sleuths-track-hacker-to-chinas-military-1443042030. This assertion is not to suggest that the United States does not engage in cyber surveillance internally or externally. *See* Charlie Savage et al., *Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at Border*, N.Y. TIMES (June 4, 2015), http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-

Very personal websites such as Ashley Madison—the purpose of which was to assist adults in finding a partner with whom to commit adultery—were hacked in 2015. This led to the disclosure of details from 32 million accounts and the loss of human capital, in addition to financial capital, as some customers of that website committed suicide as a result of the data breach of which Ashley Madison had been forewarned.[16] The Internal Revenue Service ("IRS") admitted breaches to its system, leading to the disruption of information of approximately 300,000 people.

Simply put, cybersecurity is not a public sector issue or a private sector issue. The federal government should not be putting businesses such as Target through costly investigations while at the same time leaving the nation's power grid vulnerable, and exposing millions of people's personal information—stored by state-sponsored government entities such as UCLA's medical system and the IRS—to data breaches.[17] Even software technology companies have been hacked in the past year, as Apple, Inc. became victim in mid-September 2015.[18] To attempt to combat the various forms of cyber-rattling that have been occurring, a number of discussions have taken place offering a variety of proposals, including this Symposium.

However, one hugely important sector of the U.S. economy that appears to be ignored in all of this discussion is the plight of risk management relative to cybersecurity for the entrepreneur. For purposes of this Article, "entrepreneur" means a startup enterprise or the founder of a startup entity for which the end-goal is that the entity scale to the point of an initial public offering ("IPO") under U.S. securities regulations or an acquisition of the business. This Article considers the risks and costs and policy arguments relative to attempting to run a lean—non-cybersecurity—startup, while simultaneously attempting to disrupt industries and compete with existing rivals in the public, private, and government sectors that have proven

---

spying-at-us-border.html [http://perma.cc/4LQC-FZNL].

16 *See, e.g.*, Laurie Segall, *Pastor Outed on Ashley Madison Commits Suicide*, CNN MONEY (Sept. 8, 2015, 7:10 PM), http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/index.html [http://perma.cc/CVC4-5QAA]; *see also* Chris Isidore & David Goldman, *Ashley Madison Hackers Post Millions of Customer Names*, CNN MONEY (Aug. 18, 2015, 12:39 AM), http://money.cnn.com/2015/08/18/technology/ashley-madison-data-dump/index.html?iid=EL [http://perma.cc/2ZCZ-VAYM] (stating that a month prior to the data release, the hackers, calling themselves the "Impact Team," indicated they would hack and release the information obtained unless the website ceased operations).

17 *IRS Breach Bigger than Thought*, CNBC (Aug. 17, 2015, 2:07 PM), http://video.cnbc.com/gallery/?video=3000407838.

18 Yang Jie & Josh Chin, *Apple iOS Breach No Mere 'Mistaken Experiment,' Chinese Experts Say*, WALL ST. J.: CHINA REAL TIME (Sept. 21, 2015, 8:55 PM), http://blogs.wsj.com/chinarealtime/2015/09/21/prank-or-hack-apple-china-breach-in-eye-of-beholder/.

incapable of protecting themselves or their respective customer bases, despite employing costly protective measures.

The Article first briefly provides an historical framework—including contextualizing recent events—regarding cybersecurity. Next, the Article discusses what options are available to businesses, due to the many recent breaches and failures of government to defend against cyber hacking and cyber terror, and then bifurcates the options available to established businesses and startup entrepreneurial businesses. Third, the Article discusses existing material cyberlaws, regulations, and executive orders, as well as laws proposed by President Obama in early 2015. Fourth, the Article uses those existing and proposed rules to examine the pros and cons of applying a public-private partnership to combat cyberthreats versus employing a purely market-based solution.

Finally, the Article argues, and underpins with policy proscriptions, that due to the huge differences between established businesses and entrepreneurial startups, their legal responsibilities should be placed under the rubric of a sliding scale of fiduciary duties of care relative to personally identifiable information ("PII") and cyberattack mitigation, based on a business's size, scale, and duration since formation. This Part also proposes that each state mandate corporations, limited liability companies, and other owner liability-shielded entities require a risk management committee of its board of directors or governing body. The Article concludes that, due to the many moving parts that exist in this area, the private sector should lead the way in cyber protection, including self-policing and certifying. Solely foreign governmental attacks on domestic U.S. private or governmental cyber-hacking entities require a federal mandate on businesses, rather than cyber hackers, that impact U.S. citizens, businesses, and financial capital.

I. BACKGROUND ON CYBERSECURITY AND CYBER LAW

A. Lack of Meaningful Historical Guidance

Given that the majority of examples of cyber-hacking described in this Article's introduction occurred after the *Chapman Law Review*'s announcement of this Symposium, one can reasonably understand how quickly the field of cybersecurity is moving relative to other areas of law and policy. For example, the initial federal statute concerning computer crimes occurred

in 1984.[19] Less than three years old, 2013's *Internet and Online Law*,[20] a practice guide, already seems dated relative to its awareness or discussion of the existing and looming cybersecurity threat. Although that text contains a robust section entitled "Privacy, Data Protection and Related Issues,"[21] none of the numerous statutes, regulations, rules, and common laws mentioned in the text are able to prevent any material cybersecurity matters or materially affect a business' cybersecurity attempts.

Another text, *Technology Innovation Law and Practice Cases and Materials*,[22] while again providing robust discussion on other areas of law and technology, is essentially silent on cybersecurity and cybercrime.[23] Subsequent cases have been largely ineffective to prevent or deter cybercrime.[24] Worse, during several cybercrimes

---

19 Act of Oct. 12, 1984, Pub. L. No. 98–473, § 2102(a), 98 Stat. 1837, 2190 (codified as amended at 18 U.S.C. 1030 (2012)); *see also* United States v. Morris, 928 F.2d 504, 507 (2d Cir. 1991).

20 KENT D. STUCKEY, INTERNET AND ONLINE LAW (2013); *cf.* CLIFFORD ENNICO, ADVISING EBUSINESSES §§ 11:1–11:15 (2011–2012 ed.) (stating essentially same).

21 *See* STUCKEY, *supra* note 20, §§ 5.01–5.03 (describing the many acts affecting privacy rights online including: (a) the Mail Privacy Statute; (b) Electronic Communications Privacy Act and Stored Communications Act; (c) the Communications Assistance for Law Enforcement Act, Computer Fraud and Abuse Act; (d) Federal Trade Commission Act; (e) Children's Online Privacy Protection Act ("COPPA"); (f) USA Patriot Act; (g) Health Insurance Portability and Accountability Act ("HIPPA"); (h) Graham-Leach-Bliley Act; (i) Common Law Invasion of Privacy Torts; (j) Fair Credit Reporting Act; (k) Fair and Accurate Credit Transactions Act; (k) State Laws and Requirements Imposed on States by the Federal Government; (l) the Stored Communications Provisions of the Electronic Communications Privacy Act; and (m) general descriptions of consumer privacy, identity theft, and the "tension" between public and "hyper-public" information).

22 THEODORE M. HAGELIN, TECHNOLOGY INNOVATION LAW AND PRACTICE CASES AND MATERIALS (2011).

23 *See id.*

24 *See, e.g.*, United States v. Nosal, 676 F.3d 854, 859–60 (9th Cir. 2012) (interpreting the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and stating that "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved"). *But cf.* United States v. John, 597 F.3d 263, 270–73 (5th Cir. 2010) (stating that employees may exceed permissible use of employer data of customer information); United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010) (holding that a government employee of the Social Security Administration exceeded permissible access under the law when obtaining personally identifiable information regarding romantic and former romantic interests of the government employee); People v. Harris, 945 N.Y.S.2d 505, 511–13 (Crim. Ct. 2012) (using the Stored Communications Act to quash a subpoena to obtain information regarding a Twitter account and worrying that an overbroad interpretation of the Stored Communications Act would lead to "litigation by hypothetical," which "becomes particularly risky in the face of ever-evolving and ever-more-complicated technology"). Regardless, the penalties against the wrongdoers under this regulatory scheme do little to protect personally identifiable information, consumers, and customers in any material way, and as this Article's introduction suggested, these cases, even when a violation may exist, appear to do little to dissuade large-scale cybercrime.

or related criminal cases, jurors have inappropriately used social media in contravention of court orders or rules.[25]

Further, according to Verizon's 2015 *Data Breach Investigations Report*, the *New York Times* employed the term "data breach" in 700 articles in the year 2014, up from fewer than 125 articles just one year earlier.[26] Additionally, Verizon reported that 2014 became the year that the data breach was of the "cyber" variety.[27] Moreover, these articles described nearly 80,000 cybersecurity incidents, with more than 2000 confirmed breaches, affecting 700 million compromised records and costing $400 million in financial losses in 2014.[28] While the top three affected industries in 2014 were the same as in previous years of Verizon's studies since 2008—Public, Information, and Financial Services—Section C of this Part describes a broader set of industries that have become increasingly relevant during 2015,[29] because of (1) Moore's Law, (2) Verizon's conclusion that mobile app problems were not a problem as of year-end 2014,[30] and (3) although "anything that leads to the discovery of an incident is worthwhile . . . in most cases, context is key."[31]

B. Paucity of Case Law and Academic Writing on the Matter

In conducting initial research for this Article in the late Spring of 2015, I conducted a Lexis database search using the term "cybersecurity" and located only ninety-five cases—underscoring the current importance of the case law cited earlier[32]—and fewer than two dozen relevant law journal articles.[33] I believe it is safe for me to assert at this time that technology and human action in this arena are well ahead of meaningful protective legal and policy instruments. For a current example—albeit in a slightly different arena of business disruption—that illustrates technology outpacing the extant legal regime, one need simply review Uber's and Lyft's business models versus traditional taxi cabs.[34]

---

25 *See, e.g.*, United States v. Fumo, 655 F.3d 288, 298 (3d Cir. 2011); Commonwealth v. Werner, 967 N.E.2d 159, 167–69 (Mass. App. Ct. 2012).

26 VERIZON, *supra* note 9, at 1.

27 *Id.*

28 *Id.*

29 *Id.* at 3.

30 *Id.* at 18–19 (stating that FireEye, Inc.—discussed *infra* note 89 and accompanying text—indicated that under 0.03% of smartphones per week had malicious code infections based on 1400 EnPublic Apps, and Kindsight Security Labs' biannual report indicated a rate of 0.68%); *see also Motive Security Labs Malware Reports*, ALCATEL LUCENT, www.alcatel-lucent.com/solutions/malware-reports [http://perma.cc/7B5M-NDFP].

31 VERIZON, *supra* note 9, at 11.

32 *See supra* notes 19, 24–25 and accompanying text.

33 Screen capture on file with author.

34 *See, e.g.*, Andrei Hagiu, *Work 3.0: Redefining Jobs and Companies in the Uber Age*, HARV. BUS. SCH. (Sept. 29, 2015), http://hbswk.hbs.edu/item/work-3-0-redefining-jobs-and-

C. Industry Examples of Real Consequences Beyond the Consumer Phase

1. Recent Concurring Black Swan Events Across Industries

During 2015, society witnessed black swan cybersecurity events, such as simultaneous cyber outages to major components of U.S. industry. For example, first, on July 8, 2015, at approximately 10:00 a.m., one of the nation's largest airlines, UAL/Continental grounded its flights due to cyber problems, with the company's former CEO describing UAL as "100% dependent on IT."[35] Second, at approximately 11:32 a.m. on the same day, the New York Stock Exchange's ("NYSE's") computer infrastructure failed, leading to the longest suspension of trading (and the cancelling of all prior trades) since at least the so-called "flash-crash" of 2009.[36] Third, during this time on the same day, the financial media websites of the *Wall Street Journal* and *ZeroHedge* also failed.[37]

The confluence of these events led not only to spikes in the share prices of cybersecurity firms once share trading resumed,[38] but also to two Justice Department officials commenting on the matter, President Obama being briefed on the issue and subsequently issuing a statement, the involvement of the Federal Bureau of Investigation ("FBI"), and a statement from the Department of Homeland Security ("DHS").[39] Eerily, on the eve

---

companies-in-the-uber-age [http://perma.cc/3YMX-5DHU].

35 *UAL 100% Dependent on IT: Former Continental CEO,* CNBC (July 8, 2015, 10:11 AM), http://video.cnbc.com/gallery/?video=3000395071; *United Flights Grounded Due to Computer Issue,* CNBC (July 8, 2015, 9:51 AM), http://video.cnbc.com/gallery/?video=3000395056.

36 *UAL 100% Dependent on IT: Former Continental CEO*, *supra* note 35; *United Flights Grounded Due to Computer Issue*, *supra* note 35.

37 *See, e.g.*, Tyler Durden, *And Now the Wall Street Journal Is Down*, ZEROHEDGE (July 8, 2015, 11:50 AM), http://www.zerohedge.com/news/2015-07-08/wall-street-journal-down [http://perma.cc/3RU3-6XJB]; *see also* Kaja Whitehouse, *WSJ, Barrons Hacked: CEO Warns of Wider Plot*, USA TODAY (Oct. 9, 2015, 5:06 PM), http://www.usatoday.com/story/money/2015/10/09/barrons-hacked-ceo-warns-wider-plot/73663568/ [http://perma.cc/3KJB-REWG] (indicating that the *Wall Street Journal* announced in October 2015 that the business has been hacked multiple times since at least 2012).

38 *See, e.g.*, *FactorShares Trust PureFunds ISE Cyber Security ETF*, MARKETWATCH (July 8, 2015), http://www.marketwatch.com/investing/fund/HACK/historical?siteid=mktw&date=July%208%2C%202015&userName=&password=&remChk=on&returnUrl=&persist=&x=15&y=12 [http://perma.cc/K4JM-VV46] (rising more than 1.7% for a basket of cybersecurity stocks on more than double the average daily trading volume for the stock); *see also CyberArk Software Ltd.*, MARKETWATCH (July 8, 2015), http://www.marketwatch.com/investing/stock/CYBR/historical?siteid=mktw&date=July%208%2C%202015&userName=&password=&remChk=on&returnUrl=&persist=&x=0&y=0 [http://perma.cc/7ASB-HKUT] (rising more than 8.8% in intra-day trading for cybersecurity firm CyberArk discussed *infra*).

39 *See, e.g.*, *FBI: Monitoring Situation at NYSE*, CNBC (July 8, 2015, 12:39 PM), http://video.cnbc.com/gallery/?video=3000395115; *Homeland Security: No Nefarious Actor*

of this non-harmonic convergence, a mysterious tweet predicted the occurrence of the highly improbable event of the NYSE's shutdown.[40]

However, a meaningful question remains as to how much of a black swan event this instance in July 2015 was.[41] Only a month earlier, in June 2015, former FBI agent Austin Berglas—who in 2009 created the New York branch of the FBI's cybercrime unit—described a hypothetical scenario in which the NASDAQ market, the New York subway system, and Con Edison (New York City's largest gas and electric company) all simultaneously went offline.[42] Con Edison is part of the public-private U.S. power grid, which, according to representatives of the federal government, contains vulnerabilities that could cost approximately $1 trillion to secure.[43]

2. Public Sector: U.S. Government, Cybersecurity, and Cyberterrorism

Moving from the private to the public sector, as discussed earlier in this Article, the U.S. government was subjected to a material cybersecurity breach in late 2014. The size and scope of this breach are still unknown, but it is believed to have affected approximately 20 million people in the United States,[44] and the

---

in United and NYSE Issues, CNBC (July 8, 2015, 1:25 PM), http://video.cnbc.com/gallery/?video=3000395165; *No Indications United and NYSE Glitches Related,* CNBC (July 8, 2015, 12:02 PM), http://video.cnbc.com/gallery/?video=3000395110; *White House: President Briefed on NYSE Halt*, CNBC (July 8, 2015, 1:36 PM), http://video.cnbc.com/gallery/?video=3000395167.

40 *See, e.g.*, Jesse Byrnes, *Anonymous Issued Cryptic Tweet on Eve of NYSE Suspension*, HILL (July 8, 2015, 1:55 PM), http://thehill.com/policy/finance/247225-anonymous-issued-cryptic-tweet-on-eve-of-nyse-suspension [http://perma.cc/6XXR-V4NJ]. For more information regarding the group known as "Anonymous," see *infra* note 70.

41 *See, e.g.*, Edward Helmore, *The New Sage of Wall Street*, GUARDIAN (Sept. 27, 2008, 7:01 PM), http://www.theguardian.com/books/2008/sep/28/businessandfinance.philosophy [http://perma.cc/4AMW-EHC5] ("['Black swan event'] refers to the medieval belief that all swans were white, hence black swan was a metaphor for something that could not exist, a metaphor that shifted into a perceived impossibility that came to pass when black swans were discovered in the 17th century."). *See generally* NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE (2010); Bill Conerly, *Uncertainty and Risk Management: What to Do About Black Swans?*, FORBES (Feb. 20, 2013, 5:34 PM), http://www.forbes.com/sites/billconerly/2013/02/20/uncertainty-and-risk-management-what-to-do-about-black-swans/.

42 Basak, *supra* note12.

43 *See Protecting US Power Grid from Hack Attack*, CNBC (June 30, 2015, 8:43 AM), http://video.cnbc.com/gallery/?video=3000392902 (showing Elizabeth Sherwood-Randall, Deputy Secretary of Energy, discussing federal attempts to protect the nation's power from cybersecurity threats); *see also* Ben DiPietro, *Attack on U.S. Electrical Grid Could Cost $1 Trillion*, WALL ST. J. (July 8, 2015, 10:44 AM), http://blogs.wsj.com/riskandcompliance/2015/07/08/attack-on-u-s-electrical-grid-could-cost-1-trillion/.

44 *See, e.g.*, Matt Spetalnick & Michael Martina, *Obama Announces 'Understanding' with China's Xi on Cyber Theft but Remains Wary*, REUTERS (Sept. 26, 2015, 8:19 AM), http://www.reuters.com/article/2015/09/26/us-usa-china-idUSKCN0RO2HQ20150926

IRS cybersecurity breach is apparently larger than first thought,[45] including the government workers mentioned earlier in this Article. Further, when Chinese President Xi Jinping visited the United States in September 2015, cybersecurity threats—arguably cyberterrorism—became a meaningful topic of discussion between Jinping and President Barack Obama.[46]

3. Technology Sector: Apps and Snapchat

Even the software industry can get hacked. In September 2015, Apple's iOS app store was hacked by malware.[47] A code named XCodeGhost—rather than the intended-to-be-used-code called XCode—fooled app developers into injecting malware-infected code into the apps they were creating.[48] This malware could steal users' logins or send false prompts. Apple did not indicate how many apps or users were affected by that cyber breach.[49] Many of the infected apps were located in the China app store.[50]

Through 2014, Symantec has identified more than 1 million apps "that are classified as malware,"[51] including crypto-ransomware.[52]

Another technology company to suffer a cyberhack includes the popular picture posting platform, Snapchat.[53]

[http://perma.cc/K2SK-KF5S] (suggesting that government-to-government cyberspying "could include the massive hack of the federal government's personnel office this year that compromised the data of more than 20 million people"); *see also* Jackie Northam, *Obama Meets with China's President Amid 'Enormous Strain' Between Nations*, NPR (Sept. 24, 2015, 7:35 AM) http://www.npr.org/2015/09/24/443053658/obama-meets-with-chinas-president-amid-enormous-strain-between-nations [http://perma.cc/5KL2-NWLL] ("[T]his two-day visit by President Xi Jinping comes during a particularly turbulent time in U.S.-China relations.").

45 *See, e.g.*, *IRS Breach Bigger than Thought*, CNBC (Aug. 17, 2015, 2:07 PM), http://video.cnbc.com/gallery/?video=3000407838 (estimating over 330,000 taxpayers having their PII breached from the IRS).

46 *See, e.g.*, Spetalnick & Martina, *supra* note 44 (indicating, inter alia, the discussion occurred amid "growing U.S. complaints about Chinese hacking of government and corporate databases, and the suspicion in Washington that Beijing is sometimes behind it").

47 Josh Chin, *Malware Creeps into Apple Apps*, WALL ST. J., Sept. 21, 2015, at B1.

48 *Hack Attack on Apple's iOS App Store*, CNBC (Sept. 21, 2015, 9:00 AM), http://video.cnbc.com/gallery/?video=3000422910.

49 *Id.*

50 *Id. But see generally Anti-theft Protection for iOS (Apple) Wireless Handsets*, CTIA, http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data/anti-theft-protection-for-ios-apple-wireless-handsets [http://perma.cc/6HMT-A5KU] (last updated June 2015) (representing, respectively, app and cyber protection apps for mobile devices); KNOW MY APP, http://www.knowmyapp.org/ [http://perma.cc/8H3C-7GHH].

51 SYMANTEC, INTERNET SECURITY THREAT REPORT 19 (Apr. 2015) https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf [http://perma.cc/6EXV-KEQE].

52 *Id.* at 25.

53 *See, e.g.*, Byron Tau & Elizabeth Dwoskin, *White House Proposes Consumer*

4. Non-profit and Medical Sector: UCLA Health

UCLA Health, a well-known health services provider that has a number of famous celebrities among its client base due to its geographic location, was breached in the summer of 2015, impacting the PII and medical records of approximately 4.5 million patients.[54] Reviewing cybersecurity in the medical sector, from a legal perspective, some cyber-risk management firms, such as Kroll, described later in Part II, have been able to work with legal counsel to demonstrate to government attorneys that the manner in which data had been saved by the hospital was equivalent to encryption, so the state's attorney general recognized the matter as an exception to state law.[55]

Despite being highly regulated by government administrative agencies, data breaches in the healthcare industry often involve matters of life and death. For example, Gartner, Inc., a technology-research company whose ticker symbol on the NYSE is "IT" (i.e., "information technology"), indicated at the 2015 ITxpo that the Food and Drug Administration ("FDA") recently recommended the removal from commerce of an insulin pump due to the potential of the pump being hackable in hospital networks.[56] Symantec indicated that in addition to insulin pumps, pacemakers also are at risk.[57]

5. The Connected Car: Automobile Sector Cyber Hacking

Cybersecurity issues in the automotive industry can also involve life-and-death situations.[58] In July 2015, "two veteran cybersecurity researchers . . . used a software vulnerability . . . to break into a Jeep Cherokee being driven on the highway, intensifying the debate about the safety of increasingly connected cars and trucks."[59] The Jeep cyberhack affected air conditioning,

---

Cybersecurity Measures, WALL ST. J. (Jan. 12, 2015, 2:08 PM), http://www.wsj.com/articles/white-house-to-propose-consumer-cybersecurity-measures-1421068868.

54 *See, e.g.*, Chad Terhune, *UCLA Health System Data Breach Affects 4.5 Million Patients*, L.A. TIMES (July 17, 2015, 5:51 PM), http://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html [http://perma.cc/RX69-XTVS]. For information regarding the predictable class action lawsuit that followed, see Ortiz v. UCLA Health System, No. BC589327 (Cal. Super. Ct. L.A. Cty. July 29, 2015).

55 *Risk Analysis – University Medical Center*, KROLL, http://www.kroll.com/en-us/intelligence-center/case-studies/cyber-security/risk-analysis-university-medical-center [http://perma.cc/23DC-BT57].

56 Tom Loftus, *Cybersecurity Becomes Life or Death Issue as Companies Add Tech to Consumer Devices*, WALL ST. J. (Oct. 6, 2015, 8:08 PM), http://blogs.wsj.com/cio/2015/10/06/cybersecurity-becomes-life-or-death-issue-as-companies-add-tech-to-consumer-devices/.

57 SYMANTEC, *supra* note 51, at 29.

58 I acknowledge that this Section's title could have referred to the "Internet of Things," rather than the automobile industry. The "Internet of Things" refers to "embedded computing devices with Internet connectivity." *Id.* at 26.

59 Abhirup Roy, *Harman Says Car Hacking Risk Restricted to Fiat Chrysler*,

windshield wipers, and "cut the transmission," leading the car's accelerator to immediately stop functioning.[60]

And in August 2015, researchers at the University of California, San Diego indicated that they successfully cyberhacked a 2013 Chevrolet Corvette.[61] This breach apparently permitted the researchers to send messages to the vehicle that not only operated windshield wipers but also tampered with brakes while the vehicle was driving.[62] As a result, these cyberhacks in the auto space evidence that the accelerators and brakes, among other devices, in automobiles are vulnerable to cybercrime that could have fatal consequences. A recent article posed the question regarding cybersecurity and connected cars, inquiring whether an industry-generated solution "without any [g]overnmental approval is the right strategy."[63]

6. Policy Tensions: Privacy Concerns Versus Cyberterrorism Protection Efforts

Further questioning government-involved solutions is the testimony in June 2015 of a FBI official before Congress indicating that the FBI faced a challenge to "[work] with tech companies 'to build technological solutions to prevent encryption above all else.'"[64] Simply put, this means that the FBI wanted the government to "make tech companies build in ways for law enforcement to access secured content from their products."[65] The FBI official, Michael B. Steinbach, assistant director of the FBI's Counterterrorism Division, also oddly disputed the "back door"

REUTERS (Aug. 4, 2015, 4:32 PM), http://www.reuters.com/article/us-fiat-chrysler-hacking-harman-intl-ind-idUSKCN0Q91TV20150804 [http://perma.cc/7KAF-5TAF]; *see also* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—with Me in It*, WIRED (July 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [http://perma.cc/ZA3D-ZEB3] (recounting the experience of being in a moving car that gets remotely hacked).

60 Greenberg, *supra* note 59.

61 Andy Greenberg, *Hackers Cut a Corvette's Brakes via a Common Car Gadget*, WIRED (Aug. 11, 2015, 7:00 AM), http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/ [http://perma.cc/5WY6-P7LF]; *see also* Pete Bigelow, *Chevy Corvette Is Latest Car Breached by Hackers*, AUTOBLOG (Aug. 11, 2015, 7:20 PM), http://www.autoblog.com/2015/08/11/chevy-corvette-car-hackers/ [http://perma.cc/W43E-ARPK]; Mrlanrat, *Fast and Vulnerable*, YOUTUBE (Aug. 11, 2015), https://www.youtube.com/watch?v=-CH9BvFlrGs (employing a video demonstrating this type of cyberhack of automobiles).

62 Bigelow, *supra* note 61.

63 Giulio Coraggio, *Car Makers Join Forces for Connected Car Cyber Security*, TECHNOLOGY'S LEGAL EDGE (Aug. 27, 2015), http://www.technologyslegaledge.com/2015/08/27/car-makers-join-forces-for-connected-car-cyber-security/ [http://perma.cc/A48D-LK58].

64 Andrea Peterson, *FBI Official: Companies Should Help Us 'Prevent Encryption Above All Else,'* WASH. POST (June 4, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/04/fbi-official-companies-should-help-us-prevent-encryption-above-all-else/ [http://perma.cc/5SCL-ECR8].

65 *Id.*

that software engineers and coders use as access points to enter otherwise secure software.[66]

But this FBI proposal arguably weakens cybersecurity[67] because, for example, hackers could use the same back door as the government, and the proposal conflicts with some existing state law.[68] Further, from a policy perspective, the proposal puts legitimate privacy rights concerns at loggerheads with the legitimate national security concerns described in this Part. Moreover, as the CEO of Axeon, Inc., a company offering cyber insurance, stated: "[N]o CISO wants to create a vulnerability for him or herself by giving out the combination to the back door."[69] Another problem related to the government potentially acting overzealously in its prosecution of cyberhacks is described in the next sub-section.

7. Government and Third-Party Overreaching Responses to a Cybersecurity Breach

The government's and the Massachusetts Institute of Technology's ("MIT's") response to—and arguable cause of—the suicide of twenty-six-year-old hacker Aaron Swartz, appears disappointing.[70] Swartz successfully hacked into MIT's electronic JSTOR academic database to make innocuous academic information publicly available—actions seemingly fitting within MIT's own stated goals for "open education" and support for "hackathons."[71] Yet, despite those goals, Swartz was relentlessly pursued by MIT and government authorities, to the tune of thirteen felony counts and at least fifty years in prison.[72] These acts by government attorneys and MIT ostensibly led Swartz to

---

66 *Id.*

67 *Id.*

68 *See, e.g.*, COMMONWEALTH OF MASS. OFFICE OF CONSUMER AFFAIRS & BUS. REGULATION, A SMALL BUS. GUIDE: FORMULATING A COMPREHENSIVE WRITTEN INFO. SEC. PROGRAM, http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf [http://perma.cc/82KV-LL7E].

69 Christopher P. Skroupa, *The Insurance Industry's Vantage Point on Cyber Security*, FORBES (July 9, 2015, 5:42 PM), http://www.forbes.com/sites/christopherskroupa/2015/07/09/the-insurance-industrys-unique-vantage-point-on-cyber-security/#530e2a1a7f9d (CISO stands for Chief Information Security Officer).

70 Sam Gustin, *Aaron Swartz's Suicide Prompts MIT Soul-Searching*, TIME (Jan. 14, 2013), http://business.time.com/2013/01/14/mit-orders-review-of-aaron-swartz-suicide-as-soul-searching-begins/ [http://perma.cc/NPN9-U9F6]; *see also* Lawrence Lessig, *Why They Mattered: Aaron Swartz*, POLITICO (Dec. 22, 2013), http://www.politico.com/magazine/story/2013/12/aaron-swartz-obituary-101418 [http://perma.cc/X8NJ-CUTB].

71 *Hackathon,* RECLAIM OPEN LEARNING, http://open.media.mit.edu/hackathon/ [http://perma.cc/VV7K-9HEF].

72 Tim Cushing, *US Government Ups Felony Count in JSTOR/Aaron Swartz Case from Four to Thirteen*, TECHDIRT (Sept. 18, 2012, 7:42 AM), https://www.techdirt.com/articles/20120917/17393320412/us-government-ups-felony-count-jstoraaron-swartz-case-four-to-thirteen.shtml [http://perma.cc/4NQB-Q4M4].

the point where Swartz believed that he could no longer live his life. MIT's appalling behavior regarding this cybersecurity matter is telling, not only because the school prides itself on its tradition of hacking and its alleged desire of "open learning,"[73] but also because, according to tenured Harvard Law Professor and law and technology expert, Lawrence Lessig, a friend of the young Swartz, JSTOR declined to pursue any action against Swartz and requested that the government drop its case against Swartz.[74]

Swartz's suicide led to MIT being hacked again by so-called "hacktivists" known only as "Anonymous,"[75] who are discussed later in this Article.[76] I hope that Swartz's hacking legacy remains an important part of big data and cybersecurity discussions, particularly because he came from a university famous for "hacking." However, none of the charges brought against Swartz would have prevented or stopped the events described in this Article. Yet, what I am not observing in the legal, business, or financial media is a rational discussion of the real economic carnage—not the made-up kind that Professor Lessig alleged occurred with Swartz[77]—that can occur from a cybersecurity breach.

8. 401(k)s and Other Defined Contribution Plans, Investment, and Savings Accounts

I accept that, frankly, the loss of some of my customer or personally identifiable information in a data breach that occurs at a retailer such as Target, is not hugely impactful to me. For well over a decade, anyone could go online and purchase my

---

73 *See generally HackMIT 2015*, HACKMIT, https://hackmit.org/ [http://perma.cc/RKW8-655C] (discussing MIT's largest Hackathon); MIT HACKING MEDICINE, http://hackingmedicine.mit.edu/ [http://perma.cc/BC6C-X8C2] (stating "[w]hy we should all hack medicine").

74 *See* Gustin, *supra* note 70; Lawrence Lessig, *Prosecutor as Bully*, LESSIG BLOG V2, http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully [http://perma.cc/GQ6C-ABUT]; Juan Carlos Perez, *Hactivist, Internet Innovator Aaron Swartz Commits Suicide*, PCWORLD (Jan. 12, 2013, 4:47 PM), http://www.pcworld.com/article/2025165/hactivist-internet-innovator-aaron-swartz-commits-suicide.html [http://perma.cc/Z7AP-LJ7T] (indicating Professor Lessig's friendship with Swartz).

75 For more regarding the group Anonymous and hacking, see Gustin, *supra* note 70 and accompanying text.

76 *Anonymous Hactivists Target MIT's Websites over Aaron Swartz Suicide*, TELEGRAPH (Jan. 14, 2013, 11:45 AM), http://www.telegraph.co.uk/technology/news/9800257/Anonymous-hacktivists-target-MIT-websites-over-Aaron-Swartz-suicide.html [http://perma.cc/RNT2-493Q].

77 *See* Lessig, *supra* note 74 ("[A]nyone who says that there is money to be made in a stash of ***ACADEMIC ARTICLES*** is either an idiot or a liar. It was clear what this was not, yet our government continued to push as if it had caught the 9/11 terrorists red-handed. Aaron had literally done nothing in his life 'to make money.'") (emphasis in original).

social security number, residential address, telephone information, and the like. I recognize that my financial liability for unauthorized charges to my credit cards is fifty dollars. An inconvenience, yes, but putting me on the verge of bankruptcy, no. But an example of what may put people on the verge of bankruptcy—or being forced to eat cat food in retirement—occurred in October 2015, as Scottrade, a well-known discount securities broker was hacked.[78] Seemingly, only a matter of time exists before one of the major 401(k) custodians or providers is hacked, which could lead to unauthorized trading or funds disappearing from accounts.

Despite 2014 data indicating that the financial services sector permitted the least amount of malware events per week (an average of 350 per week),[79] in 2014, the largest of the "too big to fail"[80] banks, JPMorganChase & Co.,[81] faced a cyber breach that impacted over 70 million customers. Even if one believes that a life savings stuffed in an account insured by a federal agency, the Federal Deposit Insurance Corporation ("FDIC"), is safe, FDIC insurance applies to bank failures, not necessarily cyberattacks, unless those attacks ultimately lead to a bank failure in which the bank is placed in receivership by the FDIC.[82] Therefore, the retirement and financial security of persons in the United States is vulnerable to a myriad of unknown cyberthreats, with unknown financial consequences, because of unknown, unwritten, or outdated policies that are essentially impossible to keep up with the rapid pace of technological advancement as described by Moore's Law. Simply because trades were reversed on the day of the NYSE's ostensible software failure in July 2015, does not mean that the same result would occur following the next cyber terror attack on the NYSE or on a different securities market.

---

78 Jacob Pramuk, *Scottrade Data Breach Affects up to 4M Customers,"* CNBC (Oct. 2, 2015, 2:57 PM), http://www.cnbc.com/2015/10/02/Scottrade-data-breach-affects-up-to-4m-customers.html [http://perma.cc/PR38-QKX3].

79 VERIZON, *supra* note 9, at 21.

80 *See* David C. Wheelock, *Too Big to Fail: The Pros and Cons of Breaking up Big Banks,* REGIONAL ECONOMIST 10 (Oct. 2012), https://www.stlouisfed.org/~/media/Files/PDFs/publications/pub_assets/pdf/re/2012/d/Too_Big_To_Fail.pdf [http://perma.cc/RD95-XN3F] (indicating that JPMorgan Chase was the largest of the big banks); *see also* Halah Touryalai, *The World's 29 Too Big to Fail Banks, JPMorgan at the Top,* FORBES (Nov. 11, 2013, 4:27 PM), http://www.forbes.com/sites/halahtouryalai/2013/11/11/the-worlds-29-too-big-to-fail-banks-jpmorgan-at-the-top/.

81 For the purposes of full disclosure and disclosing any potential conflicts of interest, I was a JPMorganChase & Co. officer for more than a decade, and the entity is an unsecured creditor of mine on a currently undrawn account.

82 *See, e.g.*, FED. DEPOSIT INS. CORP., YOUR INSURED DEPOSITS (2014), https://www.fdic.gov/deposit/deposits/brochures/Your%20Insured%20Deposits%20-%20English.pdf [http://perma.cc/AFG3-SJ2W]; *see also* Federal Deposit Insurance Act of 1950, Pub. L. No. 81-797, 64 Stat. 873 (codified as amended at 12 U.S.C. § 1811 (2012)).

II. WHAT DO THE ESTABLISHED PRIVATE SECTOR AND GOVERNMENTAL FAILURES TO ADEQUATELY DEFEND AGAINST CYBERCRIME AT THIS NASCENT STAGE MEAN FOR THE ENTREPRENEUR?

This Article has so far demonstrated that, to date, the public and private sectors have not thwarted material cyberattacks against the United States and its established businesses. Yet, e-commerce sales represented more than $3 trillion in 2013,[83] and according to consulting firm McKinsey, from 2004–2009, electronic transactions represented 15% of U.S. gross domestic product ("GDP") growth.[84] To understand what cybersecurity means for the entrepreneurial startup enterprise, however, one must first understand the milieu in which larger, traditional, or established businesses operate in their attempts to manage the risk of cyberattacks. This Part begins by looking at data points of what those established business do in hopes of preventing a cyberattack, then moves to a discussion of several potential solutions available to those businesses, and finally concludes with identifying the issue unique to entrepreneurs that is not practically available to startup enterprises in terms of risk management, leaving a meaningful dilemma in an age when small entrepreneurial enterprises often work to create many mobile apps and Internet platforms.

A. How Larger and Established Businesses Manage Cyber Risk

Although established, large businesses have a plethora of cybersecurity firms from whom the established businesses may purchase defenses against cyberattacks or cyberterrorism,[85] these businesses were the target of approximately 41% of spear-phishing attacks.[86] These options include offerings from newer companies such as CyberArk,[87] Palo Alto Networks,[88]

---

83 *E-stats 2013: Measuring the Electronic Economy*, U.S. CENSUS BUREAU (May 28, 2015), http://www.census.gov/econ/estats/e13-estats.pdf [http://perma.cc/XFP5-QN7H].

84 MCKINSEY GLOBAL INSTITUTE, MCKINSEY & CO., INTERNET MATTERS: THE NET'S SWEEPING IMPACT ON GROWTH, JOBS, AND PROSPERITY 16 (May 2011), http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

85 Any meaningful discussion of natural person cyber protection generally resides beyond this Article's scope.

86 SYMANTEC, *supra* note 51, at 14.

87 *See* Renaissance Capital, *US IPO Pricing Recap: CyberArk Software Pops 85% and Year's Second Largest IPO Trades up*, NASDAQ (Sept. 28, 2014, 1:21 PM), http://www.nasdaq.com/article/us-ipo-pricing-recap-cyberark-software-pops-85-and-years-second-largest-ipo-trades-up-cm396042 [http://perma.cc/C6SD-GDLK]. Israel's CyberArk, although a foreign company, had its initial public offering ("IPO") on the United States' NASDAQ as recently as 2013, and saw its share price more than triple from June 2014 to June 2015. CyberArk—as a foreign cybersecurity company—does, however, raise the issue of allowing foreign corporations to collaborate with the U.S. government on cyberterrorism and cybersecurity and to what extent these collaborative efforts should go,

FireEye,[89] Rapid 7,[90] or established companies such as IBM[91] and Cisco.[92] Further, beyond cyber prevention and cyber clean-up companies, established businesses generally have the ability to obtain cybersecurity insurance.[93] Arca, a prominent exchange traded fund which holds stock of cybersecurity firms and trades under the ticker symbol "HACK" on the NYSE, has performed well relative to the broader markets since the ETF's inception.[94]

Cybersecurity insurance, while new and rare in its current form (it originated in the late-1990s in a different form because of different technological capabilities),[95] is expensive, potentially because of the difficult nature of quantifying risks[96] associated with cybercrime and cyber terror and because few large insurers offer the product.[97] AIG predicts that the cyber-insurance market

---

even with traditional U.S. allies.

88 *See* Palo Alto Networks, Inc., Annual Report (Form 10-K) *passim* (Sept. 18, 2014).

89 *See* FireEye, Inc., Annual Report (Form 10-K) 6 (Mar. 3, 2015). FireEye, Inc. advised on the famed 2013 Sony Breach. Basak, *supra* note 12, at 5.

90 *See* Rapid7, Inc., Amendment No. 1 to Form S-1 (Form S-1/A) 52 (June 26, 2015).

91 *See, e.g.*, *Cyber Security Solutions from IBM*, IBM, http://www-304.ibm.com/industries/publicsector/us/en/contentemplate1/!!/xmlid=148819 [http://perma.cc/UL58-7JUT] (marketing IBM's apparent "Cyber Security Solutions" and "Cyber Security Leadership"). *But see* Alex Barinka, *Five Charts Show Why IBM Is Worst Dow Stock for 2nd Year*, BLOOMBERG BUS. (Dec. 30, 2014, 12:43 PM), http://www.bloomberg.com/news/articles/2014-12-30/five-charts-show-why-ibm-is-worst-dow-performer-for-second-year [http://perma.cc/J4RU-ZGQE]; Kevin Kingsbury, *IBM Is One Week away from Infamy*, WALL ST. J.: MONEYBEAT (Dec. 24, 2014, 9:05 AM), http://blogs.wsj.com/moneybeat/2014/12/24/ibm-is-one-week-away-from-dow-infamy/ [http://perma.cc/G3T6-9HN8] ("IBM is just a week away from some infamy—becoming the first Dow component to be bottom of the barrel in consecutive years since now-departed Bethlehem Steel in 1995 and 1996."); *Heard on the Street: IBM Biggest Dow Loser for Second Year*, POST-BULLETIN (Dec. 31, 2014 4:38 PM), http://www.postbulletin.com/business/heard-on-the-street-ibm-biggest-dow-loser-for-second/article_834834c4-fe05-588e-bf1f-ee577be4c90f.html [http://perma.cc/SMM9-2F6J] (indicating collectively that IBM has been the worst performing Dow Jones Industrial Average component company for two years in a row in 2013 and 2014, a feat not accomplished since the mid-1990s, and IBM's white papers on information technology on IBM's website are typically from the decade ending 2010, with only one white paper in the past three years).

92 *See, e.g.*, *Cybersecurity*, CISCO, http://www.cisco.com/web/strategy/government/defense_cybersecurity.html [http://perma.cc/4PUG-RXDM] (indicating various industry-specific cybersecurity solutions).

93 Basak, *supra* note 12, at 2.

94 PureFunds ISE Cyber Security ETF, Supplement to the Prospectus dated Nov. 7, 2014 and Statement of Additional Information ("SAI") dated November 7, 2014, as supplemented March 24, 2015 (Form 497) (June 18, 2015).

95 Basak, *supra* note 12, at 3.

96 *Id.* ("Most firms are reluctant to offer policies for property damage resulting from hacking because there's almost no data available to determine costs . . . . Insurers have been excluding infrastructure damage caused by cyber-attacks from standard property and general liability policies, said Kevin Kalinich, who leads the cyber-risk team at insurance broker Aon Plc.").

97 *Id.* (indicating that, for example, Zurich Insurance Group, AG and Munich Re are considering offering these products but do not offer the product currently).

as of 2015 is $2 billion in annual premiums but could be $10 billion in annual premiums by 2020.[98]

Currently, coverage limits through AIG are at $100 million each for both property damage and bodily injury caused by a cyberattack.[99] Even if an established business were to pay the premiums for a cyber-insurance policy, these policies do not cover certain important cybersecurity matters, because of a lack of data on risk and cost.[100] To contextualize this lack of actuarial data, insurers currently have fewer than twenty years of data points from which to develop cyber-insurance policies, in comparison to up to one hundred years of data points from which to develop and tweak more typical property or liability insurance.[101]

B. The Financial Elephant in the Room: The Entrepreneurial Cost

Unlike established businesses, entrepreneurial startups are constantly concerned with so-called "runway" (the amount of time the company has before running out of cash),[102] burn rates (how quickly the company spends its cash),[103] and attracting new financial capital to allow the business to continue operating (one can think of this scenario as new equity investment equaling revenue for the entrepreneurial startup, often employing only a few people, typically at below-market cash consideration in return for equity stakes in the startup that have unlimited upside at the point of a successful exit, such as an acquisition or an IPO). And in 2014, small businesses were the target of 34% of spear-phishing attacks, only seven percentage points below those of large businesses,[104] an increase of more than 88% from 2011 levels.[105] Furthermore, according to the website of 2016 presidential candidate, former Florida Governor Jeb Bush, in 2014 "60% of all targeted attacks struck small and medium-sized organizations, *which often have fewer resources to invest in cybersecurity*."[106]

---

98 *Id.*

99 *Id.*

100 *Id.; see also Cyber Risk Assessments*, KROLL, http://www.kroll.com/en-us/cyber-security/data-breach-prevention/cyber-risk-assessments [http://perma.cc/T76A-6NEH] (describing assessing risk from well-known security-in-many-industries-firm, Kroll).

101 Basak, *supra* note 12, at 4.

102 *See, e.g.*, DAVID FEINLEIB, WHY STARTUPS FAIL: AND HOW YOURS CAN SUCCEED 33 (2012).

103 *See, e.g.*, EMERGING COMPANIES GUIDE, A RESOURCE FOR PROFESSIONALS AND ENTREPRENEURS 202–04 (Robert L. Brown & Alan S. Gutterman eds., 2d ed. 2004).

104 SYMANTEC, *supra* note 51, at 14.

105 *Id.* at 70 (indicating spear phishing of small businesses represented 18% of attacks in 2011 but 34% by 2014).

106 *Strengthening Cybersecurity*, JEB!2016 (Sept. 14, 2015), https://jeb2016.com/strengthening-cybersecurity/?lang=en [http://perma.cc/BF7G-G3FZ] (emphasis added).

This Article does not intend to convey that startups lack access to the choices available to established business discussed in Section II.A. Rather, startups often are unable to devote the financial resources necessary to these products because of runway, burn-rate, the pacing and amounts of attracting additional financial capital available to the enterprise, and the unknown costs associated with cybersecurity risk management.[107] The cost of complying with existing and proposed laws, regulations, and orders discussed in Part III is simply impossible for many entrepreneurial startups, whether due to the founders' ignorance of the governing rules or the inability to afford cyberthreat risk compliance, either financially or in terms of focus on growing the business.

As a result, a question exists for the reader throughout Part III, which is, "should entrepreneurial startups be faced with complying with the same regime as established corporations as described in Section II.A?"

III. FEDERAL LAWS, REGULATIONS, AND PROPOSED LEGISLATION

In early 2015, President Obama stated: "[I]n this dizzying age of technology and innovation . . . cyber-criminals . . . can . . . [t]urn your life upside down. It may take you months to get your finances back in order. . . . So this is a direct threat to the economic security of American families and we've got to stop it."[108] Elsewhere, President Obama indicated: "Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property."[109] Understanding some of what the government has proposed and already put in place is also necessary to

---

107 *See* VERIZON, *supra* note 9, at 27–28 ("When budgeting and operating an InfoSec [information security] program, accurately assessing . . . how much it'll cost [is] critically important. A lack of reliable estimates leads to a creative environment for decision making, where underspending, overspending, and useless spending invariably result."). Verizon estimated that the average financial loss from a cyber breach per 1000 records was between $52,000 and $87,000. Given that many angel investors typically provide startup capital to entrepreneurs in chunks of approximately $25,000–$50,000, seed-stage investment can be eliminated by a cyber breach, without even discussing the cost of cyber risk management. Even the predicted cost of only 100 records is over $25,000. *Id.*

108 *Remarks by the President at the Federal Trade Commission*, WHITE HOUSE (Jan. 12, 2015, 12:15 PM), https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission [http://perma.cc/GZT6-RZHQ]; *see also* Tau & Dwoskin, *supra* note 53 ("The proposals came amid the revelation the U.S. Central Command Twitter and YouTube accounts appeared to have been [hacked by Islamic militants], underscoring cybersecurity challenges the U.S. faces. The tweets posted by the hackers purportedly included phone numbers of top military commanders and claimed to provide military scenarios for a [potential] conflict with North Korea and China.").

109 *Foreign Policy Cyber Security*, WHITE HOUSE, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity [http://perma.cc/9JM4-NQ2M].

appreciating the entrepreneurial startup's perspective in terms of cybersecurity and cyberterrorism protection efforts. This Part describes several of those measures, including proposed and existing legislation and recent comments from regulatory agencies.

A. Proposed Legislation

Timed to coincide with the comments quoted in this Part's opening paragraph, at a speech delivered at the Federal Trade Commission ("FTC"), the Obama administration indicated that it would be introducing legislation of varying sorts with the hope of protecting consumers from cyberattacks.[110] These proposals generally aimed at protecting privacy, preventing identity theft, and helping children remain safe in cyberspace. The following day, the President announced additional proposals at DHS.[111]

There, President Obama discussed how the federal government could "work with the private sector to better protect American companies against cyber threats."[112] The President further indicated: "Foreign governments, criminals and hackers probe America's computer networks every single day. We saw that again with the attack at Sony, which actually destroyed data and computer hardware that is going to be very costly for that company to clean up."[113]

These proposals were added to the President's 2013 Executive Order 13636, which—issued exactly two years to the week before the 2015 proposals—concerned cyberthreats, including cyberterrorist threats, to the nation's infrastructure.[114] Yet, as of October 2015, the cybersecurity web page at whitehouse.gov had no updates—text or video—since May 1, 2015, well before the numerous cyberattacks described earlier in this Article.[115]

B. SEC and FINRA

From a business perspective, perhaps the next most relevant guidance comes from the Securities and Exchange Commission

---

110 *Remarks by the President at the Federal Trade Commission*, *supra* note 108.

111 *Remarks by the President at the National Cybersecurity Communications Integration Center*, WHITE HOUSE (Jan. 13, 2015, 3:10 PM), https://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent [http://perma.cc/XP7B-326J].

112 *Id.*

113 *Id.*

114 *Executive Order -- Improving Critical Infrastructure Cybersecurity*, WHITE HOUSE (Jan. 12, 2015), https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [http://perma.cc/U2YE-RD6B].

115 *Foreign Policy Cyber Security*, *supra* note 109.

("SEC") and Financial Industry Regulatory Authority ("FINRA"). In 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") examined approximately fifty broker-dealers ("B/Ds") and fifty registered investment advisers ("RIAs").[116] OCIE's ultimate report indicated that a majority of B/Ds and RIAs examined maintained written information security policies ("WISPs"), nearly half of those firms examined identified industry cybersecurity practices via peer groups or information sharing, and more than 90% of B/Ds and RIAs employed some sort of encryption. These data points resulted from participating firms answering questionnaires, not from any inspection or testing by OCIE or a designated third-party to act on OCIE's behalf.[117]

FINRA's report described what the organization not only viewed as the material cybersecurity risks facing B/Ds but also believed were appropriate risk mitigation tactics, including references to the NIST framework.[118] The report identified risk assessment and oversight of third-party vendors ("vendor management"), consultants, and others, as a material concern for B/Ds.[119] Currently, however, neither B/Ds nor RIAs are under any SEC requirement to maintain cyberthreat insurance or have written policies regarding customer losses in the event of a cyber breach.

C. The SAFETY Act

The so-called "Support Anti-terrorism by Fostering Effective Technologies Act of 2002" ("SAFETY Act")[120] provides, in essence, a shield for certain businesses from tort liability. Specifically, the SAFETY Act provides a safe harbor—in the form of an indemnity—to cybersecurity businesses that fail in their essential function of providing cybersecurity.[121] While this Article focuses on the indemnity provision, as authors Finch and Spiegel

---

116 Office of Compliance Inspections and Examinations, U.S. Securities & Exchange Commission, *Cybersecurity Examination Sweep Summary*, 4 NAT'L EXAM PROGRAM RISK ALERT (Feb. 3, 2015), https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf [http://perma.cc/BKM8-BF6Q].

117 Anthony Zeoli, *Lock It up: SEC & FINRA Weigh in on Cybersecurity Issues* (Feb. 23, 2015, 10:09 PM), http://www.crowdfundinsider.com/2015/02/63237-lock-it-up-sec-finra-weigh-in-on-cybersecurity-issues/ [http://perma.cc/A4MT-UKJE].

118 FIN. INDUS. REGULATORY AUTH., REPORT ON CYBERSECURITY PRACTICES 42–43 (2015). For more on the National Institute of Standards and Technology (NIST), see NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, www.nist.gov [http://perma.cc/E8HW-YKXR].

119 FIN. INDUS. REGULATORY AUTH., *supra* note 118.

120 Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, 6 U.S.C. §§ 441–444 (2012) [hereinafter *SAFETY Act*].

121 After *Citizens United v. Federal Election Commission*, 558 U.S. 310 (2010), if corporations are persons, then the word that attaches to describe corporations is "who," not "that."

asserted: "These liability protections can take the form of jurisdictional defenses, a cap on liability, or a presumption of immediate dismissal of third-party liability claims."[122]

In addition, the SAFETY Act permits the federal government to give a seal of approval to certain entities (very similar to the FTC's COPPA compliance seal, despite negotiable prices and hacks that occurred and despite Target having been COPPA compliant). These entities receive a certification as a "Qualified Anti-Terrorism Technology" or "QATT."[123] The SAFETY Act mandates that all cyberterrorism-related liability claims must be litigated in federal court; punitive damages and pre-judgment interest awards are barred; and compensatory damages are capped at an amount agreed to by both the government and company, with the damage cap equal to a set amount of insurance the company must possess. Further, damages awarded to plaintiffs will be offset by any collateral recoveries they receive (e.g., victim compensation funds, life insurance, etc.).[124]

As Finch and Spiegel asserted: "The only way this presumption of immunity can be overcome is to demonstrate that the application contained information that was submitted through fraud or willful misconduct."[125] Cyberattacks are governed by the SAFETY Act's definition of "terrorism," regardless of the type of product or service in which the business is engaged (i.e., the business does not have to be in the technology space for these protections to apply). However, any client who purchases QATT-approved software from a certified QATT seller is absolved from any liability, so long as an act of terrorism is declared by the Secretary of Homeland Security.[126]

Simply put, the seller of the QATT is the sole look-to for liability, and the DHS painstakingly articulated this fact when

---

122 Brian E. Finch & Leslie H. Spiegel, *Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety* Act, 30 SANTA CLARA HIGH TECH. L.J. 349, 351 (2014).

123 *SAFETY Act*, 6 U.S.C. §§ 441–444 (detailing QATT).

124 *Id.* § 442.

125 Finch & Spiegel, *supra* note 122, at 369 (referencing the regulations implementing the *SAFETY Act* of 2002, 71 Fed. Reg. 33147, 33150 (June 8, 2006) (codified in 6 C.F.R. pt. 25)); *see also* 6 U.S.C. § 444(2)(b).

126 The *SAFETY Act* states:

> There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. . . . Such Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism technology to Federal and non-Federal government customers.

6 U.S.C. § 442(a)(1) (2012).

promulgating the final rule implementing the SAFETY Act.[127] Practically, the SAFETY Act supersedes the existing bankruptcy system and replaces an entire body of law with an explicit government grant to internalize arguably nominal costs for large businesses who can afford to purchase QATT-approved software, raising the question of whether entrepreneurial startups are able to purchase QATT-approved software, and externalizing the tremendous damage that could occur should a cyber-terror attack happen to a given safe-harbored business.

D. Discussion of Policy Prescriptions Generally

Typically, a law journal article identifies a problem and then attempts to propose a unique solution underpinned by a proposed law, rule, regulation, executive order or the like. However, as Scott Kannry, the CEO of Aon Global in the insurance industry—the holder of both a J.D. and M.B.A.—has stated:

> [Saying that the cybersecurity industry is] [f]ailing isn't the right description, although one could easily come to that conclusion given the trend line on events over the past 12 months. I would characterize the industry as one that needs a better approach. To date, most of the focus has been on solutions –firewalls, encryption, antivirus, you name it. The problem is that a cyber security program consists of dozens, if not hundreds of technologies, policies and procedures, none of which is a silver bullet and any of which can be immediately outdated based on the ever evolving risk climate. Imagine if your job was solely focused on putting together a puzzle, but some pieces were missing, others didn't fit together, and every 30 minutes the board changed. Technically, you would fail, but you never really stood a chance![128]

As a result, current cybersecurity policies appear too lax; the question is how the public and private sector should procedurally and substantively build an effective framework.

---

127 Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, 71 Fed. Reg. at 33150–51 ("Congress balanced the need to provide recovery to plaintiffs against the need to ensure adequate deployment of anti-terrorism technologies by creating a cause of action that provides a certain level of recovery against Sellers, while at the same time protecting others in the supply chain."); *see also* 6 C.F.R. § 25.7(d) (2016) ("There shall exist only one cause of action for loss of property, personal injury, or death for performance or non-performance of the Seller's Qualified Anti-Terrorism Technology in relation to an Act of Terrorism. Such cause of action may be brought only against the Seller of the Qualified Anti-Terrorism Technology and may not be brought against the buyers, the buyers' contractors, or downstream users of the Technology, the Seller's suppliers or contractors, or any other person or entity.").

128 Christopher P. Skroupa, *The Insurance Industry's Unique Vantage Point on Cyber Security*, FORBES (July 9, 2015, 5:42 PM), http://www.forbes.com/sites/christopherskroupa/2015/07/09/the-insurance-industrys-unique-vantage-point-on-cyber-security/.

IV. EVIDENCE THAT A PUBLIC-PRIVATE OR PRIVATE MARKET ALTERNATIVE EXISTS

In his January 2015 remarks to DHS, President Obama indicated that "[n]either government, nor the private sector can defend the nation alone. It's going to have to be a shared mission—government and industry working hand-in-hand as partners."[129] This Part explores that option, with an eye toward the entrepreneurial startup.

Yet, as this Article indicated above, many of the available cyber-protection solutions—whether software or insurance, regardless of not only the size of the enterprise offering the cyber protection but also the QATT-approval safe harbor involvement—are simply too expensive for entrepreneurial startups concerned with burn rate, runway, and continuing capital raises while protecting against founder and insider equity dilution.

For example, the sole government resource that appears to exist for small businesses, of which entrepreneurial startups are a flavor, is the Federal Communication Commission's ("FCC's") "Small Biz Cyber Planner 2.0."[130] And version 2.0 was launched three years ago in October 2012, which, going back to Moore's Law,[131] likely means that the Cyber Planner is out of date, despite the FCC's stated goal of providing "an online resource to help small businesses create customized cybersecurity plans."[132] "As larger companies take steps to secure their systems, less secure small businesses are easier targets for cyber criminals."[133]

The planner itself is a fifty-one page booklet (also customizable for a business on the FCC's website, but all information comes directly from the booklet) that includes sections such as (1) inventory your data; (2) keep a record of the data's location, and move the record to more appropriate places when needed; (3) develop a privacy policy; (4) protect data collected on the Internet (stating "you need to make sure any data collected through your website and stored by the third party is sufficiently secure," as if that level of due diligence is necessarily feasible); (5) create layers of security; (6) plan for data loss or theft (threateningly stating "[n]ot only can the loss or theft of data hurt your business, brand and customer confidence,

---

129 Air Force Tech. Sgt. Jake Richmond, *Obama Unveils Next Steps in Cybersecurity Plan*, U.S. DEP'T DEF. (Jan. 13, 2015), http://www.defense.gov/News-Article-View/Article/603919 [http://perma.cc/SXL2-9DR6].

130 *Cyberplanner*, FED. COMM. COMMISSION, https://www.fcc.gov/cyberplanner [http://perma.cc/GRD5-7BYL].

131 *See* Harsha, *supra* note 2.

132 *Cyberplanner*, *supra* note 130.

133 *Id.*

it can also expose you to the often-costly state and federal regulations that cover data protection and privacy. Data loss can also expose businesses to significant litigation risk").[134] Whether entrepreneurs even have the time to read this material is questionable, given that founders must essentially dedicate all of their waking hours to their fledgling businesses. The FCC also provides arguably meaningful guidance to protect mobile wallets, which employ software downloaded to a mobile device to pay for commercial transactions or person-to-person payments.[135] The advice provided in this booklet is of questionable value in functioning as a cyber safeguard.

As a result, entrepreneurial startups face unique challenges when faced with defending their firms from hackers, cybercriminals, cyberterrorists, and others attempting to successfully breach data, big data, or systems, via the Internet or the Internet of Things, negatively affecting the startups, including to the point of the startups' very existences. Part V advances some initial proposals for further discussion and evaluation that would assist the entrepreneurial startup when dealing with the very real threats that face entrepreneurs.

V. PROPOSED INITIAL DISCUSSION POINTS FOR ENTREPRENEURIAL SUCCESS FACING CYBERTHREATS

This Part asserts several proposals that may be both cost efficient and effective for the startup and effective for the startup's consumer base. First, communication and cooperation between the public and private sector are important.[136] Having said that, much of corporate law—beyond securities regulation, taxation, consumer protection, and immigrant worker visas—concerning entrepreneurial startups resides at the state level. From entity formation to the applicable internal affairs doctrine affecting the startup, to terms of use for many apps and web platforms, the end-user must agree to specific state law for applicable law, jurisdiction, and forum. Because of state law's importance, the proposals in this Part reflect suggestions for state-level changes to corporate codes, rather than action on the part of federal agencies.

---

134 *Cyber Security Planning Guide*, FED. COMM. COMMISSION PDS-1–PDS-5, https://transition.fcc.gov/cyber/cyberplanner.pdf [http://perma.cc/ZW8V-4PAQ]; *see also FCC Smartphone Security Checker*, FED. COMM. COMMISSION, https://www.fcc.gov/smartphone-security [http://perma.cc/T8CW-Y6AQ] (last updated Oct. 30, 2015, 12:45 PM).

135 *Mobile Wallet Services Protection*, FED. COMM. COMMISSION, https://www.fcc.gov/guides/mobile-wallet-services-protection [http://perma.cc/T7F6-FCY5] (last updated Nov. 4, 2015, 12:00 AM).

136 *See* Basak, *supra* note 12.

A. Corporate Governance

Ultimately, corporations are governed by a board of directors.[137] Corporate boards have fiduciary duties of care (unless exculpated) and loyalty to the company and shareholders.[138] One proposal is that a part of the duty of care that cannot be exculpated is that each corporation must create a functioning risk management committee, under whose umbrella falls cybersecurity. For public companies, the SEC could take the position that, similar to the Sarbanes-Oxley-mandated requirement of an audit committee expert serving on the audit committee, an IT or risk management expert serve on that committee. I would prefer to see such requirements come from the state-level so that businesses can choose what governance framework works best for them among a variety of cybersecurity fiduciary risk management options. For entrepreneurial startups advised appropriately, the fear of personal liability for breaching the fiduciary of care should be sufficient incentive to create a risk-management committee, without the added need and cost of an IT expert serving on the committee. People tend to respond to incentives, and the incentive of facing unlimited personal liability for a fiduciary duty breach should encourage many entrepreneurial startups to create a risk-management committee.

B. Sliding Scales for Size

To avoid disincentivizing entrepreneurial startups from forming while balancing the need to operate in a riskless manner, a sliding scale for liability could exist. This Article stipulates that little to no logical reason exists for many arbitrary numbers that laws and regulations use relative to requirements and exemptions for corporations, based on either financial or employee pool size. Having said that, this Article does advance that appropriately tailored safe harbors from liability should exist for businesses with an equity capitalization under an inflation-adjusted amount of, hypothetically, $100 million, those entities with fewer than, somewhere near twenty employees, and newly formed entities fewer than approximately thirteen months in age that are non-affiliates of previously existing enterprises.

With the rapid pace that entrepreneurial startups must deploy capital for research and development, alpha testing, beta testing, a focus on obtaining additional capital from angel or

---

137 A discussion of LLCs or the array of other owner-liability-shielded entities is beyond the scope of this Article.

138 *See generally* D. GORDON SMITH & CYNTHIA A. WILLIAMS, BUSINESS ORGANIZATIONS (2d ed. 2004).

venture capital investors (or both), seed stage companies often lack the time and human and financial capital to employ attorneys to advise them of the need for cyber-risk assessments. This Article does not believe that it is effective policy to kill off fledgling businesses that are cyberhacked, because those companies simply lacked the knowledge, the resources, or the time because of their nascent nature. As the businesses grow in size, time of existence, and financial capital, then sliding scales of obligations should begin to fall on the entrepreneurial ventures.

These matters could be self-regulating, for example, by the Venture Capital Association of America or other similar groups affecting the startup ecosystem. What fund manager would want to deploy venture or seed-stage capital to an enterprise that was naked in the face of cyber risk? Couple this self-regulation with tweaking of existing state statutes on fiduciary duties that would require an organization to face risk management of cybersecurity in its evaluation of fiduciary duty exculpation at entity formation, and the private sector can self-regulate for entrepreneurs.

C. Private-Public Partnering of Cyber Insurance for Startups

Protecting startups should not, however, come at the expense of consumers. As a result, affordable and meaningful cyber insurance could be required by states. A need for this insurance exists, as articulated earlier in this Article, but costs are high and insurers lack the actuarial data that they need. State-level, or if absolutely necessary, federal level, cyber-terror or cyberthreat insurance could be mandated and overseen by a government insurance agency, such as the Federal Deposit Insurance Corporation ("FDIC") or Pension Benefit Guaranty Corporation ("PBGC"). While, for example, the PBGC has protected the pensions of millions of Americans since the entities formation under ERISA in the mid-1970s, PBGC is funded by the companies whose pension plans it insures, rather than the taxpaying public, and claimants are paid based on a sliding scale based on financial capital. A similar framework may work well in the case of protecting customers of startup enterprises from financial loss, and the insurance and administration of the insurance may be at a lower cost than currently exists in the marketplace.

CONCLUSION

In mid-October 2015 at the first Democratic Party presidential debate, moderator Anderson Cooper asked: "[w]hat is the greatest national security threat to the United States?"

Out of five candidates—among whom were four senators, two governors, a former secretary of state, and a former secretary of the Navy—only one candidate, attorney, former Navy secretary, and Senator Jim Webb, responded with "cyberthreats." Webb indicated: "Our greatest day-to-day threat is cyber warfare against this country."[139]

Regardless of whether former Senator Webb is correct in his assessment of the single greatest security threat to the United States, cyber terror and cybersecurity are legitimate emerging threats to this nation. And in the face of those threats, this Article has proposed problems and policy solutions specific to protecting this country's citizenry from cyberattacks on businesses, with an emphasis on the specific challenges faced by entrepreneurial startups in that effort that are far different than the challenges faced by established businesses in the hopes of spurring a dialogue at this Symposium that both protects the U.S. populace and remains supportive of ensuring an environment supportive of entrepreneurial startups from ideation to commercialization.

---

139 *CNN Democratic Debate – Full Transcript*, CNN (Oct. 13, 2015, 11:26 PM), http://cnnpressroom.blogs.cnn.com/2015/10/13/cnn-democratic-debate-full-transcript/ [http://perma.cc/66UV-EN6J].

Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System

*Jeff Kosseff**

INTRODUCTION

"Tell me about U.S. cybersecurity law," a British colleague requested at a recent conference. It seemed like an easy question, but it wasn't. I paused for far too long to think about it.

That's because there isn't a single U.S. law that comprehensively addresses cybersecurity. The Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce,"[1] and the Federal Trade Commission ("FTC") uses that law to penalize companies with inadequate data security protections.[2] Every state has a similar law, and most states also have passed laws that require companies to notify customers and regulators after data breaches. But those are narrow, punitive rules that deal with data breaches after the fact and don't really focus on cybersecurity as a whole.

We have a number of statutes that focus on consumer information, including: the Children's Online Privacy Protection Act,[3] which regulates the collection of information from minors under thirteen; the Video Privacy Protection Act,[4] which restricts the sharing of consumers' video viewing information; and the Gramm-Leach-Bliley Act,[5] which governs the disclosure of financial account data. But these statutes regulate *privacy,* not cybersecurity.

The military has released a cyber strategy which is compromised of quite a few cyber-defense missions,[6] but those

---

* Assistant Professor of Cybersecurity Law, U.S. Naval Academy, Annapolis, Maryland. The views expressed in this Article are only those of the author, and not of the Naval Academy or Department of Navy.

1 15 U.S.C. § 45(a)(1) (2012).

2 *See* FED. TRADE COMM'N, 2014 PRIVACY AND DATA SECURITY UPDATE (2014), www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf [http://perma.cc/U73Q-PF9Q].

3 15 U.S.C. §§ 6501–6506.

4 18 U.S.C. § 2710 (2012).

5 15 U.S.C. §§ 6801–6809.

6 *See, e.g., The Department of Defense Cyber Strategy*, U.S. DEP'T DEF., http://

apply only to military operations. The Department of Homeland Security ("DHS") also has a strategy comprised of a number of goals and objectives,[7] but those primarily involve government infrastructure. The National Institute of Standards and Technologies has released helpful guidelines,[8] but those are, of course, only guidelines and do not have the binding force of law.

After pausing for far too long, I said, "We don't really have any cybersecurity laws." What we have, instead, is a patchwork of related laws, including breach notification and privacy statutes, that focus on penalizing companies for inadequate data security. But our legal system lacks a coordinated network of laws that are designed to promote cybersecurity and prevent data breaches from occurring in the first place.

This Article seeks to address this shortfall by articulating a consistent system of laws that would promote cybersecurity. Part I of the Article defines cybersecurity from a legal standpoint, and distinguishes it from concepts such as privacy and data security. Many laws that purport to encourage cybersecurity are, in fact, designed with a focus on protecting privacy or encouraging data security. Unlike privacy and data security, cybersecurity is focused not only on the information, but the entire system and network. For this reason, laws that focus only on privacy and data security may not consider all factors necessary to promote cybersecurity. By clearly defining the term, I hope to provide policymakers with clarity as they develop laws aimed at promoting cybersecurity.

Part II examines the patchwork of state and federal privacy and data security laws that are most commonly associated with cybersecurity, including data breach notification laws and data security requirements. These requirements have been the bedrock of U.S. cybersecurity law, yet they are ineffective at preventing cybersecurity incidents. For instance, companies that have experienced a data breach must devote significant resources to determining whether—and how—to satisfy the various notification requirements. This Article evaluates the efficacy of such a system, based on available data about cybersecurity incidents, and concludes that the current legal system contains a number of gaps that do not adequately address cybersecurity threats.

---

www.defense.gov/News/Special-Reports/0415_Cyber-Strategy [http://perma.cc/S7AT-GT47].

7 *See, e.g.*, DEP'T OF HOMELAND SEC., BLUEPRINT FOR A CYBER FUTURE: THE CYBER SECURITY STRATEGY FOR THE HOMELAND SECURITY ENTERPRISE (2011), www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf [http://perma.cc/GH9Y-V76Z].

8 *See Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH., http://www.nist.gov/cyberframework/ [http://perma.cc/7K8W-J6CF] (last updated Dec. 11, 2015).

Part III of the Article draws from other areas of law to suggest a unitary framework that could provide strong, clear, and adaptable cybersecurity laws and policies. Frist, policymakers should consider centralizing cybersecurity responsibilities within a single federal agency, rather than scattering them among the FTC, fifty state attorneys general offices, and other agencies. Such a structure would allow specialized employees and leaders to shape the nation's cybersecurity defense system. Second, policymakers should reconsider the current system's focus on punitive measures, such as fining companies for failing to adequately notify customers of data breaches. While penalties always will be a necessary component of a cybersecurity law, our laws also should include incentives for companies to invest in costly cybersecurity protections. Among the policies that lawmakers might consider are tax credits for cybersecurity investments, a national cybersecurity insurance program, and a safe harbor from data security lawsuits for companies that adhere to a rigorous set of government-mandated security standards. This Article considers the theories that support including incentives, rather than only penalties, in a policy framework. It will also examine how the government has used such incentives in other areas, and how these incentives might advance cybersecurity goals.

I refer to this concept as "positive cybersecurity law"—policies designed to encourage cybersecurity before a malicious attack occurs. This requires a shift in thinking from our nation's longstanding mindset in which nearly all cybersecurity laws are punitive. While such regulations always play a role in cybersecurity, our system should be a mix of punitive *and* positive law. The unique design of cyberspace—interconnected networks of public and private infrastructure—demands a collaborative, rather than adversarial, relationship between the government and industry. A combination of "carrots" and "sticks" would most effectively encourage investments in cybersecurity.

I. WHAT IS CYBERSECURITY?

A logical starting point for our discussion is a definition of cybersecurity. Although the term is commonly used by the press and policymakers, its precise scope often varies.

In the private sector, cybersecurity often is associated with data breaches. Indeed, a large portion of the cybersecurity industry is dedicated to helping companies prevent data breaches

and remediate the harm after a breach has occurred. Worldwide, the cybersecurity industry was estimated to generate $75.4 billion in 2015.[9] Companies are understandably concerned about the exposure of their customers' and employees' personal information, both because of potential legal liability and damage to their brand. Moreover, data breaches may expose a company's trade secrets or other confidential business information that could lead to significant financial harm to the company. Accordingly, data security is an integral part of the cybersecurity ecosystem.

However, data theft is only one aspect of cybersecurity. Cybersecurity professionals also help companies prevent the destruction or inaccessibility of data. Moreover, cybersecurity involves the *protection* of networks and systems from damage. In other words, cybersecurity aims to safeguard the confidentiality, integrity, *and* accessibility of data (commonly known as the "CIA" triad).[10]

Cybersecurity involves the protection of both private *and* public networks. Too often, policymakers and companies talk about "private-sector cybersecurity" and "public-sector cybersecurity." The open architecture of the Internet makes it futile to focus *only* on private-sector concerns, such as trade secret theft, or *only* on public-sector concerns, such as cyberattacks by other nation-states. For instance, North Korea's hack of Sony in 2014 implicated not only Sony's business interests and assets, but U.S. national security and international relations, leading President Obama to impose sanctions.[11] Similarly, if a cyberattack were to target U.S. government infrastructure, private companies likely would be affected. Accordingly, policymakers must look at cybersecurity in both the private *and* public sectors at the same time.

These goals are best reflected in the National Initiative for Cybersecurity Careers and Studies' ("NICCS")[12] definition of cybersecurity as "[t]he activity or process, ability or capability, or state whereby information and communications systems and the

---

9 Tara Seals, *Cybersecurity Spending to Hit $170Bn by 2020*, INFOSECURITY MAG. (July 13, 2015), http://www.infosecurity-magazine.com/news/cybersecurity-spending-to-hit/ [http://perma.cc/WJQ4-FZ59].

10 *See* Chad Perrin, *The CIA Triad*, TECHREPUBLIC (June 30, 2008, 8:13 AM), www.techrepublic.com/blog/it-security/the-cia-triad/ [http://perma.cc/8923-QKKT].

11 *See* Dan Roberts, *Obama Imposes New Sanctions Against North Korea in Response to Sony Hack*, GUARDIAN (Jan. 2, 2015, 4:08 PM), http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview [http://perma.cc/6WXC-PRGX].

12 NICCS is a resources of cybersecurity information managed by DHS.

information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[13] Under this definition, cybersecurity involves the protection of both data and systems. The definition also does not apply separate standards for public and private systems. The NICCS definition serves as a useful starting point as we determine how to meet the goals of cybersecurity.

Importantly, cybersecurity and privacy are *not* one in the same. The modern legal concept of privacy emerged in Samuel D. Warren and Louis D. Brandeis' 1890 *Harvard Law Review* article, *The Right to Privacy*.[14] They defined privacy as "the right 'to be let alone,'"[15] reasoning that common law right to property "has grown to comprise every form of possession—intangible, as well as tangible."[16] Privacy, therefore, involves individuals' ability to control their personal data. Strong, proactive cybersecurity measures help to promote privacy by reducing the likelihood of unauthorized disclosure. However, there are a number of other avenues in which privacy can be protected, such as by providing individuals with choice about the collection and sharing of their data. Unfortunately, cybersecurity and privacy often are used interchangeably, leading some to the mistaken belief that privacy-focused laws also will promote cybersecurity.

Why does the definition matter? If our goal is to promote cybersecurity, we should have a clear idea of what exactly cybersecurity is. As I will describe in Part II, many of our laws that purport to promote cybersecurity do very little to accomplish that goal. Some areas of cybersecurity could benefit from new laws, but often those areas are entirely unaddressed in the current political debate at the federal and state levels. To assess whether our current laws advance the goals of cybersecurity, using the NICCS definition, we must examine whether they protect systems, networks, and data from damage, unauthorized use or modification, or exploitation.

---

13 *Explore Terms: A Glossary of Common Cybersecurity Terminology*, NAT'L INITIATIVE CYBERSECURITY CAREERS & STUD., www.niccs.us-cert.gov/glossary [http://perma.cc/Z2CL-33K3].

14 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

15 *Id.* at 195 (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT (2d ed. 1888)).

16 *Id.* at 193.

II. THE CURRENT STATE OF CYBERSECURITY LAW

As discussed above, the United States does not have a cohesive cybersecurity legal framework. Instead, it had a patchwork of laws that address some aspects of data security. These laws fail to work together harmoniously, occasionally conflict, and do little to ensure the future security of data, networks, and systems. The current legal system largely is backward-looking, and provides companies and the public sector little guidance as to how to prevent future cybersecurity incidents.

A. Breach Notification Laws

Forty-seven states and the District of Columbia have enacted data breach notification laws since 2002.[17] These laws require companies and government agencies to notify individuals that their personal information has been compromised. The laws vary significantly in scope. For instance, most laws are triggered if the individual's name is compromised, along with a financial account number, Social Security number, or driver's license number. However, some notification laws cover additional categories of information, such as medical data[18] and birth dates.[19] Some states only require notification if the company determines that the disclosure poses a reasonable risk of harm to the individuals,[20] while other states require notification regardless of the actual risk.[21] The required content and form of breach notices also vary by state. Breach notification laws apply to the state's residents, and most companies have customers in all fifty states. Accordingly, if a company experiences a data breach, it must devote significant time and staff to determining the states in which it must notify residents and regulators, as well as the timing, form, and substance of the notification. That time and money could be better spent on measures to mitigate the harm of the breach and to prevent future incidents from occurring.

Furthermore, it is unclear whether the data breach notice fulfills its intended purpose. Individuals are informed of data breaches weeks or months after the initial exposure. By the time that they receive the notice, identity theft and other damage

---

17 *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Oct. 22, 2015), www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [http://perma.cc/U4RK-4DDE].

18 CAL. CIV. CODE §§ 1798.29(g)(1)(D), 1798.82(h)(1)(D) (West 2016).

19 N.D. CENT. CODE § 51-30-01(4)(a)(5) (West 2016).

20 *See, e.g.*, COLO. REV. STAT. § 6-1-716 (West 2016).

21 CIV. § 1798.82.

likely already has occurred. The notices typically direct the individuals to obtain free credit reports, and some companies offer additional identity theft protection services. However, few customers actually use these services when offered.[22] Moreover, the rationale for data breach notification laws is outdated. States began passing data breach notification laws in 2002, when large-scale data breaches were relatively uncommon. The size, number, and scope of data breaches have increased exponentially in recent years. In a 2014 survey of executives, the Ponemon Institute found that 43% experienced a data breach in the past year, up from 33% in a 2013 survey.[23] Individuals should operate under the assumption that their data has been breached; therefore, they would be wise to take precautions such as changing passwords, checking their free annual credit reports, and routinely updating their computer anti-virus software and operating systems. Although data breaches may have been rare a decade ago when the breach notice laws were first enacted, breaches now are commonplace.

Although there is some value in notifying individuals of data breaches, this should not be the primary focus of cybersecurity law. Once a data breach has occurred, much of the harm is inevitable, regardless of whether customers have been notified. It would be far more productive if companies were able to devote all of their time and expertise to forensics: figuring out how the breach occurred, and how to prevent it from occurring again.

Unfortunately, our cybersecurity legal framework focuses heavily on breach notification laws. This is an outdated and increasingly futile exercise that adds unnecessary expense and slows companies' ability to respond to data breaches.

B. FTC Data Security Enforcement and State Data Security Laws

Many people are surprised to learn that the United States does not have a national law that sets specific data security standards. Instead, the FTC uses its general consumer protection regulatory authority to bring enforcement actions against companies that it believes have failed to adequately safeguard personal information. The FTC asserts this authority under section 5 of the Federal Trade Commission Act, which allows the

---

22 *See* Jeff Kosseff, *Notified About a Data Breach? Too Late*, WALL ST. J. (Oct. 9, 2015, 7:04 PM), http://www.wsj.com/articles/notified-about-a-data-breach-too-late-1444345445.

23 Elizabeth Weise, *43% of Companies Had a Data Breach in the Past Year*, USA TODAY (Sept. 24, 2014, 3:33 PM), http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/ [http://perma.cc/U7AN-A2TL].

FTC to prevent companies from using "unfair or deceptive acts or practices in or affecting commerce."[24] Often, the FTC alleges that a company's lax data security practices constitute "unfair" trade practices.

For decades, there has been confusion as to what makes a trade practice "unfair." In 1964, the FTC issued guidance in which it stated that the following factors determine whether a trade practice was unfair:

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers (or competitors or other businessmen).[25]

Over the next two decades, critics questioned whether the FTC is in the best position to determine whether trade practices are "immoral" or "unscrupulous," leading the FTC to gradually change its analysis to focus on the harm and benefits to customers. Congress codified this new approach in 1994, amending the Federal Trade Commission Act to define "unfair" as a practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[26]

The FTC also has alleged that security practices that violate companies' privacy policies constitute deceptive trade practices under the Federal Trade Commission Act. Between 2002 and 2014, the FTC brought more than fifty cases against companies whose security and privacy practices, it claimed, were unfair or deceptive.[27] Typically, companies settle these enforcement actions before they go to court, agreeing to a consent order that, among other things, allows the FTC to closely oversee the companies' data security practices.[28]

---

24 Federal Trade Commission Act § 5(a)(1), 15 U.S.C. § 45(a)(1) (2012).

25 Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964).

26 15 U.S.C. § 45(n).

27 *See* GINA STEVENS, CONG. RESEARCH SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES AUTHORITY 6 (2014).

28 *See* PATRICIA BAILIN, IAPP, STUDY: WHAT FTC ENFORCEMENT ACTIONS TEACH US ABOUT THE FEATURES OF REASONABLE PRIVACY AND DATA SECURITY PRACTICES, https://iapp.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf [http://perma.cc/8VWV-85N7].

Because section 5 of the Federal Trade Commission Act does not explicitly mention data security, some critics have asserted that the FTC lacks jurisdiction to bring data security enforcement actions. Among the most vocal opponents of such actions is Wyndham Worldwide Resorts, which was hacked in 2008 and 2009.[29] After investigating the attacks, the FTC brought an enforcement action against Wyndham, alleging that Wyndham's data security measures were inadequate and, therefore, unfair, and that the company deceived customers by failing to provide the security measures that it guaranteed in its privacy policy.[30] Among the practices that the FTC found most objectionable was the storage of credit card information in clear text, the lack of a requirement for complex passwords on Wyndham's computer systems, and Wyndham's failure to use firewalls and other common data security solutions.[31]

Unlike most companies that face an FTC data security enforcement action, Wyndham did not settle with the FTC. Instead, the FTC brought a civil action against Wyndham in the U.S. District Court for the District of New Jersey.[32] Wyndham moved to dismiss the case, arguing that the Federal Trade Commission Act does not give the FTC the authority to regulate data security.[33] Wyndham noted that Congress has passed statutes that provide the FTC with the authority to regulate cybersecurity in particular areas, including financial institutions, websites that collect information from children under thirteen, and credit agencies. Accordingly, Wyndham argued, such "tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field."[34] The district court rejected this argument, and on appeal, the U.S. Court of Appeals for the Third Circuit agreed. The court reasoned that all of those tailored laws served different purposes than the general Federal Trade Commission Act, and therefore, "none of the recent privacy legislation was 'inexplicable' if the FTC already had some authority to regulate corporate cybersecurity through § 45(a)."[35] The Third Circuit also rejected Wyndham's argument that the FTC's numerous attempts to convince Congress to enact laws that provide it with specific data

---

29 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).
30 *Id.*
31 *Id.* at 241.
32 *Id.* at 242.
33 *Id.*
34 *Id.* at 247.
35 *Id.* at 248.

protection powers demonstrates that section 5 does not provide it with such authority.

Wyndham also argued that the FTC failed to provide clear data security standards with "ascertainable certainty,"[36] in violation of the Due Process Clause. The court also rejected this argument, concluding that Wyndham was not entitled to ascertainable certainty. Instead, the court concluded, "the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute."[37] Wyndham, the court wrote, is "only entitled to notice of the meaning of the statute and not to the agency's interpretation of the statute."[38]

The *Wyndham* case is important because it demonstrates two primary flaws with the FTC's data security enforcement. First, *Wyndham* raised valid questions about whether section 5 of the Federal Trade Commission Act provides the FTC with authority to regulate data security. The Third Circuit is the only federal appellate court to rule on the issue, so there is a very real chance that another circuit would disagree, creating a circuit split that ultimately would be resolved by the U.S. Supreme Court. Second, and more importantly, *Wyndham* demonstrated that the FTC provides little concrete guidance as to what constitutes adequate data security. This is perhaps the most significant shortcoming with the FTC's current data security enforcement system. Even if a company is well-intentioned and attempts to comply with all applicable data security laws, it has no guarantee that the FTC would believe that its efforts are adequate. What kinds of data should be encrypted in transit and at rest? What level of encryption should a company use? How often should companies require employees to reset passwords? How long should passwords be? Should a company use two-factor authentication for remote access? What about in-office access? How often should companies provide cybersecurity training to employees? Should a company design an incident response plan? These are just some of the many questions that companies have on a routine basis. Binding, concrete guidance on these issues would be incredibly helpful, and likely would increase the overall number of cybersecurity measures that companies put in place. If a company knows that a cybersecurity safeguard will help to satisfy regulators' expectations, the investments in that safeguard will be easier to justify.

---

36 *Id.* at 253–54.
37 *Id.* at 255.
38 *Id.*

Approximately a dozen states have supplemented the FTC's general data security enforcement with laws that impose data security requirements on companies that process the data of the state's residents.[39] However, most of these laws simply require a company to develop "reasonable" security, providing no more certainty than the FTC. The two exceptions are Nevada, which requires compliance with payment card industry data security standards, and Massachusetts, which requires companies to develop detailed data security plans in writing.[40] However, these state-level laws do little to address the significant uncertainty that arises due to the lack of nationwide, concrete standards for data security. Furthermore, if other states follow their lead and enact their own specific data security regulations, companies would be forced to apply a number of different data security standards, based on the state in which the individual lives. Why should, say, the personal data of a Massachusetts resident receive more protection than the data of a New Hampshire resident? Cybersecurity simply is not an area where state-level regulation is effective.

III. A POSITIVE, UNITARY FRAMEWORK

Now that we have a better idea of the concepts that are involved in cybersecurity and the shortcomings of the current legal framework, we can begin to create a legal framework that provides companies with the certainty necessary to invest heavily in cybersecurity.

Cyberspace, by its very architecture, is a network of both private-sector and public-sector infrastructure. Unlike traditional regulatory areas, such as food safety, where the government is more than an overseer of the private sector, the government is a partner *with* the private sector. The government developed the initial infrastructure of the Internet, and the private sector invested billions of dollars to build that initial infrastructure into the transformative force that it is today. Accordingly, unlike other areas, in which traditional top-down regulation is effective, cybersecurity requires a different mindset. Cybersecurity requires a continuation of the partnership between the government and companies. Indeed, an insecure Internet harms the private sector by slowing the growth and progress of the

---

39 Hogan Lovells, *Outlook for State Data Security Laws: More than Breach Notification*, IAPP (Dec. 16, 2014), https://iapp.org/news/a/outlook-for-state-data-security-laws-more-than-breach-notification [http://perma.cc/2VX5-FJJ3].

40 *Id.*

Internet; it is in the best interests of every company to work with the government for a more secure cyberspace.

In line with that collaborative mindset, below are four suggested starting points for building such a legal framework. I note that I do not address whether Congress should immunize companies from liability arising from sharing cyberthreat information with the federal government. Such proposals are subject to significant debate among policymakers, companies, and privacy advocates. The goal of this Article is to highlight policies that have not received as much public attention and debate.

A. Create a Safe Harbor for Responsible Cybersecurity

As I argued in the previous section, the FTC's current data security enforcement provides little certainty for well-intentioned companies that would like to comply with all legal requirements. Ideally, the FTC would issue specific regulations that set minimum standards such as password lengths, firewall capabilities, and categories of data that require encryption in transit and at rest.

A likely response to such a proposal is that every data security incident involves unique circumstances, and therefore, it is impossible to provide minimum standards that apply in all circumstances. For instance, costly firewalls may be more necessary for companies that handle sensitive information, such as health records, and may be more affordable for larger companies than for smaller companies. Moreover, larger companies are more likely to be able to afford dedicated information security staff.

Point taken. It would be difficult to proscribe nationwide, minimum data security standards for all companies. Such rules could lead to unreasonable penalties for small companies, or those that do not typically process significant amounts of personal information and, therefore, are not in a position to make significant investments.

Instead of setting a national minimum cybersecurity standard, Congress should pass a law that directs the FTC to develop cybersecurity criteria for a national safe harbor program. If a company demonstrates, through an annual independent audit, that it has satisfied all of those safe harbor criteria, then it cannot be the subject of a regulatory action or lawsuit—at either the federal or state level—arising from a data breach or another cybersecurity incident, unless the regulator or plaintiff can demonstrate that the breach was due to the company's intentional actions or gross negligence.

A safe harbor program would provide companies with significant incentive to make costly investments in cybersecurity hardware, software, and staff. Although companies would not be required to make these investments, doing so would provide them with reasonable certainty that they would be protected from lawsuits and regulatory actions.

In fact, this would not be the first technology-related safe harbor. The Digital Millennium Copyright Act ("DMCA") addresses concerns about online copyright piracy by granting Internet service providers and websites with immunity for copyright infringement claims arising from their users' actions, contingent upon the providers removing the infringing content upon receiving notice.[41] The DMCA safe harbor affords service providers with a significant incentive to remove infringing content.

Critics likely would argue that the safe harbor would unfairly shield companies from being held responsible for data breaches that are caused by their inadequate security. Such criticism would fail for two reasons. First, companies still could face regulatory actions and lawsuits if they are found to have been grossly negligent. The safe harbor would not provide an absolute shield; rather, it would provide companies with qualified protection in exchange for upfront investments in cybersecurity. Even if a company has qualified for the safe harbor, significant lapses could lead to its being held responsible in court or before a regulatory agency.

Second, the statute should direct the FTC to set very high standards for companies to qualify for the safe harbor. These should not be the minimum necessary safeguards for cybersecurity; instead, the safe harbor should only reward companies that invest in and implement the best of the best cybersecurity safeguards, as determined by the FTC. The safe harbor requirements should be designed to be difficult to achieve; qualified protection from lawsuits and regulatory actions is incredibly valuable, and companies should be required to meet a very high bar before receiving that protection.

The failure of a number of technology-related laws is that they do not quickly adapt to new changes in technology. For instance, Congress took years to update the Video Privacy Protection Act, which restricts the disclosure of video rental information, to address online streaming video services such as

---

41 17 U.S.C. § 512 (2012).

Netflix.[42] Congress often takes years to pass Legislation; by the time that a technology-related bill has been enacted, there is a good chance that it will be outdated. For that reason, the FTC—and not Congress—should set specific safe harbor requirements in regulations, and routinely update those requirements. The FTC is better positioned than Congress to set these requirements because it has more technical expertise, and promulgating regulations typically takes less time than passing a new statute.

B. Create a Nationwide Breach Notification Standard

As described in Part II of this Article, I question the utility of data breach notifications. Complying with the specific notification rules of forty-seven states and the District of Columbia is time-consuming, and there is no demonstrable evidence that notifications actually mitigate the harm caused by data breaches. However, eliminating breach notifications altogether likely would face significant opposition from privacy advocacy groups. Politically, such a change likely would be a non-starter.

As a compromise, Congress should pass a national data breach notification law that preempts the state notification laws. By creating a single standard, companies would no longer be forced to analyze the dozens of different procedures and definitions in the state laws. Individuals still would receive notice of significant breaches, but the process would be far less time-consuming for companies, allowing them to focus their time and resources on preventing further damage from the breach.

The specific requirements of a national data breach notification law likely would be subject to intense debate and negotiation among companies and privacy advocates. Below are the key elements that a national breach notification law should address:

Risk of harm: Some state breach notification laws only require companies to notify individuals if they determine that there is a reasonable likelihood that the breach will lead to harm, such as identity theft. Other state laws require notice in all circumstances, even if there is no risk of harm. Ideally, a national breach notice law would only require companies to notify individuals if there is some risk of identity theft or other harm. If there truly is not a risk of harm, it would be counterproductive to notify and unnecessarily scare customers. Moreover, if customers

---

42 Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112–258, 126 Stat. 2414 (codified at 18 U.S.C. § 2710(b)(2)).

receive too many breach notices, they will be less likely to take the notices seriously.

Definition of "personal information": Similarly, the federal law should only apply to breaches of sensitive categories of personal information. Social Security numbers, unencrypted credit card numbers, and other information that could be used in identity theft should fall within the scope of the law. However, breaches that only disclose a name or email address likely do not present significant risk.

Minimum number of affected individuals: A small breach, involving only a few individuals, should not trigger a nationwide breach notification. The federal breach law should only apply if a minimum number of people—such as 500 or 1000—are affected.

Encryption: Like every state breach notice law, the federal law should not apply if the information was encrypted.

Length of time: Companies should be required to notify individuals of data breaches only after the companies have had an opportunity to investigate the incident and fully remediate the harm. A company's first priority should be preventing further breaches or damage.

C. Provide Tax Incentives for Cybersecurity

Very little public debate about cybersecurity has focused on the use of tax incentives to promote investments. That should change. The federal tax code offers tax incentives for education, wind energy, electric vehicles, and other areas that the government has determined to be a priority for investment.[43] Yet the tax code does not provide a penny in tax incentives for investments in cybersecurity.

This is partly due to the nascence of the cybersecurity field. The federal tax code received its last comprehensive overhaul in 1986, decades before cybersecurity emerged as a common term and serious challenge. However, the failure also is due to fiscal concerns. In response to an Executive Order directing departments to analyze potential cybersecurity policies, the Treasury Department wrote that tax incentives for cybersecurity "would come at the expense of foregone revenue for the government or reallocation of existing fiscal obligations," and recommended against further consideration of tax incentives.[44]

---

43 *See generally Credits and Deductions*, IRS, https://www.irs.gov/Credits-&-Deductions [http://perma.cc/K9DP-PNCE] (last updated Feb. 1, 2016).

44 *See* TREASURY DEP'T, SUMMARY REPORT TO THE PRESIDENT ON CYBERSECURITY

The Treasury Department is correct that, in the short term, tax incentives may result in a reduction in revenues to the federal government. However, such a view is short-sighted. If structured properly, tax incentives could dramatically increase companies' investments in cybersecurity safeguards, preventing costly data breaches and stimulating economic growth. Indeed, a report by the Atlantic Council estimates that an insecure Internet would reduce global economic net benefit by $90 trillion; a fully secure Internet would lead to a net gain of $190 trillion.[45]

Cybersecurity tax incentives could be structured in a number of different ways. The government could provide companies with a tax credit for investments in qualified cybersecurity expenditures up to a certain annual amount. The challenge for policymakers will be agreement on which cybersecurity investments qualify for the tax credit. An effective program would broadly include hardware, software, services, and staffing that help to promote the confidentiality, integrity, and accessibility of systems, networks, and data, consistent with the definition of "cybersecurity" in Part I of this Article. Policymakers also would need to determine the maximum size of cybersecurity tax credits. A $50,000 annual tax credit may provide a significant incentive for a small business to invest in cybersecurity, but that credit would be a rounding error for the budget of a Fortune 500 company. Accordingly, the maximum tax credit could be tied to an objective measure of a company's size, such as its annual revenues or number of employees.

Alternatively, the federal government could provide a tax credit that encourages investments in cybersecurity companies. This could be modeled after a Maryland program that provides a 33% tax credit for investments of up to $250,000 in certain cybersecurity businesses.[46] Such a program, at the national level, likely would lead to an increase in cybersecurity innovation.

D. Offer National Cybersecurity Insurance

After a data breach, companies often are surprised to learn that their general commercial insurance policies may not cover

---

INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636 (2013).

45 *Atlantic Council / Zurich Insurance Report Finds the Global Benefits of Cyber Connectivity Expected to Outweigh Costs by $160 Trillion Through 2030*, ATLANTIC COUNCIL (Sept. 9, 2015), http://www.atlanticcouncil.org/news/press-releases/atlantic-council-zurich-insurance-report-finds-the-global-benefits-of-cyber-connectivity-expected-to-outweigh-costs-by-160-trillion-through-2030 [http://perma.cc/RE9P-KESC].

46 *See Cybersecurity Investment Incentive Tax Credit (CIITC)*, MD. DEP'T COM., http://commerce.maryland.gov/fund/programs-for-businesses/cyber-tax-credit [http://perma.cc/QHP9-VX4B].

the expenses involved with remediation and defending against legal claims.[47] Some insurers have developed cybersecurity insurance policies that specifically insure companies for certain cybersecurity events. So far, the policies have received lukewarm reviews from companies and the cybersecurity community due to the cost and the number of exclusions that apply if companies have not implemented adequate safeguards.[48] DHS has conducted workshops and issued reports on the "nascent" cybersecurity insurance market, and insurers told DHS that their cybersecurity offerings are limited due to "a lack of actuarial data; aggregation concerns; and the unknowable nature of all potential cyber threat vectors."[49] These problems have placed cybersecurity insurance out of reach for many companies. In a 2015 survey of small businesses, Endurance International Group found that although 81% of small business owners are concerned about cybersecurity, only 5% of the small businesses have purchased cybersecurity insurance.[50]

This coverage gap provides an opportunity for policymakers to give companies more protection from catastrophic data breaches, while at the same time encouraging companies to invest in cybersecurity safeguards. The solution is a modified version of the National Flood Insurance Program ("NFIP"). Congress enacted the NFIP in 1968 to address concerns about building homes on rivers and other floodplains. NFIP flood insurance is available to property owners in communities that have adopted minimum floodplain management regulations that help to minimize the likelihood that a building would be

---

47 *See* Paul F. Roberts, *Cyber Insurance: Only Fools Rush in*, ITWORLD (Oct. 27, 2014), http://www.itworld.com/article/2839393/cyber-insurance-only-fools-rush-in.html [http://perma.cc/LUH2-PN6P] ("Insurers have responded by writing exclusions into [commercial general liability] and other nuts and bolts commercial policies, like so-called E&O (errors and omissions) and D&O (directors and officers) liability policies. Those exclusions carve out cyber claims and push them into new, specialized insurance products.").

48 *Don't Waste Your Money on Cyber Breach Insurance*, INFORMATIONWEEK (Sept. 26, 2012), http://www.darkreading.com/dont-waste-your-money-on-cyber-breach-insurance/d/d-id/1138422 [http://perma.cc/7GMW-BFDR] ("If line-of-business and legal leaders unilaterally decide to get a breach policy without input from IT, they may miss exclusions in the policy that require a higher level of controls than what the organization currently has in place.").

49 DEP'T OF HOMELAND SEC., INSURANCE INDUSTRY WORKING SESSION READOUT REPORT (2014).

50 *New Survey Finds a Vast Majority of U.S. Small Business Owners Believe Cybersecurity Is a Concern and Lawmakers Should Do More To Combat Cyber-Attacks*, ENDURANCE INT'L GRP. (May 4, 2015), http://www.prnewswire.com/news-releases/new-survey-finds-a-vast-majority-of-us-small-business-owners-believe-cybersecurity-is-a-concern-and-lawmakers-should-do-more-to-combat-cyber-attacks-300076543.html [http://perma.cc/39R5-94F6].

damaged or destroyed in a flood.[51] The Federal Emergency Management Agency administers the NFIP and promulgates regulations that set the minimum safeguards for local communities that wish to participate in the program. As of 2014, 5.35 million NFIP policies are in force.[52] In 2005, when Hurricane Katrina hit the southern states, the NFIP paid $17.8 billion in loss dollars.[53]

NFIP serves as a roadmap for the solution to the cybersecurity insurance problem. The government could create a cybersecurity insurance program, structured similarly to the NFIP. A government agency with experience in cybersecurity, such as DHS, would administer the insurance program and promulgate minimum cybersecurity safeguards that a company must implement to qualify for the insurance. If implemented properly, the program would help businesses mitigate risk, while encouraging companies to invest in cybersecurity infrastructure and services. Such a program would not only benefit businesses, but it would be a net win for the American public, as the cybersecurity safeguards would result in fewer cybersecurity incidents.

CONCLUSION

Some of the proposals in this Article, such as the national data breach notification standard, have been discussed for many years but have not gained significant traction.[54] Other proposals, such as the safe harbor and insurance program, have not been discussed significantly, and may come out of left field for many policymakers. This is because our cybersecurity debate has focused too long on punitive measures rather than collaboration between the private and public sectors.

Our cybersecurity policy is built on decades-old infrastructure that does not account for the unique, public-private nature of cyberspace. Regulating companies into oblivion is not the most effective way to optimize investments in cybersecurity. Instead,

---

51 *See* FED. EMERGENCY MGMT. AGENCY, FEMA 496, JOINING THE NATIONAL FLOOD INSURANCE PROGRAM (2005), http://www.floods.org/ace-files/documentlibrary/State_Local%20Resources%20and%20Tools/3.6_FEMA_496_JoiningNFIP.pdf [http://perma.cc/AYP6-U4SM].

52 *Total Policies in Force by Calendar Year,* FEMA, https://www.fema.gov/total-policies-force-calendar-year [http://perma.cc/94SH-HN94] (last updated Nov. 19, 2015).

53 *Loss Dollars Paid by Calendar Year,* FEMA, https://www.fema.gov/loss-dollars-paid-calendar-year [http://perma.cc/XH76-BGJH] (last updated Nov. 19, 2015).

54 *See* Jeff Kosseff, *Analysis of White House Data Breach Notification Bill*, INSIDEPRIVACY (Jan. 15, 2015), http://www.insideprivacy.com/uncategorized/analysis-of-white-house-data-breach-notification-bill/ [http://perma.cc/7FKA-9YXC].

we need a legal framework that encourages companies to work with the government to invest in cybersecurity. Such a change will benefit not only the companies, but society as a whole, helping to secure individuals' personal information.

Cybersecurity: Executive Orders, Legislation, Cyberattacks, and Hot Topics

Kelly Russo and Harvey Rishikof***

INTRODUCTION

For all actors—government, business, and individual—cybersecurity has evolved significantly over the last fifteen years due to the rise of the Internet and the need for the free flow of information.[1] Due to statutory divisions, we refer to cybersecurity as cybercrime, cyberespionage, and cyberwar. However, the evolution of security regulations can be examined through four periods, beginning with pre-9/11 and progressing through the cyber era of today.

As the Internet expanded during the 1990s, it forced industry to focus on connecting systems and expanding the flow of information, while the law, the Telecommunications Act of 1996, left the network largely unregulated.[2] Some legislative attempts were made, but most failed. During this period, threats usually came from low-budget, mischievous hackers, rather than criminals or nations. From the perspective of the U.S. government, terrorism and related security issues were almost exclusively issues dealt with overseas; it was an age of innocence.

After 9/11, a series of security-related laws and regulations were passed as attempts were made to lock down cyberspace. The Department of Homeland Security, Department of Justice, and Department of Defense began a nascent regulatory framework to strengthen security. The focus was "centered primarily on the

---

* Kelly Russo is an attorney with the Cybersecurity Legal Task Force at the American Bar Association in Washington D.C. She graduated from Wake Forest University, (B.A. 2012 cum) (J.D. 2015). While in law school, Ms. Russo served as the Marshal on the Moot Court Board, and was an Elite 8 Finalist at the Regional Jessup International Law Competition.

** Harvey Rishikof, American Bar Association Chair, Advisory Standing Committee on Law and National Security, is former legal counsel to the Deputy Director of the FBI, former Administrative Assistant to the Chief Justice of the United States, and former Dean of Roger Williams University School of Law. The opinions and views expressed in this Article are his own and do not reflect the opinions or views of any entity of the U.S. government.

1 CROWELL & MORING, REGULATORY FORECAST 2016, at 8–9 (2016), https://www.crowell.com/files/Regulatory-Forecast-2016-Crowell-Moring.pdf [http://perma.cc/S2GX-G2NK].

2 *Id.*

16 'critical infrastructure' sectors vital to the U.S., such as energy, chemicals, communications, financial services, and the defense industrial base."[3] Almost exclusively, regulators focused on the security of physical spaces; however, some regulations were created to defend information systems from hackers disrupting critical operations. The legislation passed during this era included the USA Patriot Act of 2001, which permitted the use of more extensive investigative tools, harsher penalties, and intra-governmental information sharing. In 2001, the Department of Homeland Security ("DHS") was created. In 2002, the Federal Information Security Management Act of 2002 established a cybersecurity framework for federal data systems. Then, in 2004, the Intelligence Reform and Terrorism Prevention Act of 2004, among other things, created the Director of National Intelligence.[4]

In response to these developments, the ABA Cybersecurity Legal Task Force was created in 2012 under Former ABA President Laurel Bellows. It was established to examine ways to help lawyers protect their practices and their clients' confidential information and intellectual property during cyber events, as well as position the ABA to contribute to national dialogue about cyber issues.[5] It is tasked with addressing the tough questions about the appropriate role and responsibility of lawyers in cyber-related incidents and to examine ways that lawyers and businesses can protect their practices and their clients' confidential information and intellectual property.[6] It is composed of representatives of ABA entities having an interest in the cyber domain as well as leaders in the private and public sectors responsible for cybersecurity.[7]

The Mission Statement for the Task Force was clear:

> [to] identify and compile resources within the ABA that pertain to cybersecurity, and will focus and coordinate that ABA's legal and policy analyses and assessments of proposals relating to cybersecurity. . . . (1) Facilitate collaboration and information exchange among constituent ABA entities and with relevant public and private organizations; (2) Serve as a clearinghouse among ABA entities regarding cybersecurity activities, policy proposals, advocacy, publications and resources; (3) Study and analyze executive and legislative branch cybersecurity proposals; (4) Identify cyber-related issues for appropriate action by the ABA, including filling gaps in

---

3 *Id.*

4 *Id.*

5 *See generally* JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK (2013).

6 *Id.*

7 *Id.*

> policy, encouraging ABA entities to develop new policy as appropriate, and sharing best practices with members and their firms; and (5) Advise and assist ABA Governmental Affairs Office on cybersecurity advocacy and responses to government actions.[8]

During the next period, regulations were focused more on protecting data, as data breaches affected a broad range of organizations, from corporations to the U.S. Office of Personnel Management. Regulators questioned the government's role in ensuring cybersecurity and protecting private information. Information sharing between the public and private sector increasingly became the zone to ensure cybersecurity. Data theft in the last few years was perpetrated by criminals, spies, nations, terrorists, and "hactivists," and "creating common, overarching standards for security, reporting, and response has proven to be a

---

8 *About the Task Force*, A.B.A., http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity/aboutcyber.html [http://perma.cc/87ZK-G7UC]. The Task Force was quite productive establishing principles, writing reports, and passing resolutions. Their Resolution of November of 2012 was comprised of the following five principles:

> (1) Public-private frameworks are essential to successfully protect United States ' assets, infrastructure, and economic interests from cybersecurity attacks; (2) Robust information sharing and collaboration between government agencies and private industry are necessary to manage global cyber risks; (3) Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements; (4) Privacy and civil liberties must remain a priority when developing cybersecurity law and policy; (5) Training, education, and workforce development of government and corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful.

A.B.A. CYBERSECURITY LEGAL TASK FORCE, REPORT TO THE BOARD OF GOVERNORS 1 (2012), http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf [http://perma.cc/Y9V8-NQ9A]; *see also* A.B.A. CYBERSECURITY LEGAL TASK FORCE, REPORT AND RESOLUTION 118 1 (2013), http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf [http://perma.cc/947M-FK7R] (containing a Resolution that condemns "intrusions into computer systems and networks utilized by lawyers and law firms" and urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions); A.B.A. CYBERSECURITY LEGAL TASK FORCE, REPORT TO HOUSE OF DELEGATES ON RESOLUTION 109 2 (2014), http://www.americanbar.org/content/dam/aba/events/law_national_security/2014annualmeeting/ABA%20-%20Cyber%20Resolution%20109%20Final.authcheckdam.pdf [http://perma.cc/DA4X-SKGX] ("This Resolution addresses cybersecurity issues that are critical to the national and economic security of the United States (U.S.). It encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected."); A.B.A. CYBERSECURITY LEGAL TASK FORCE, REPORT TO THE HOUSE OF DELEGATES ON RESOLUTION 116 1 (2015), http://www.americanbar.org/content/dam/aba/images/law_national_security/Aug-2015-Cyber-Res.pdf [http://perma.cc/EXE7-TYXF] ("It urges the federal, state, local, tribal, and territorial legislatures and government agencies to provide the funding necessary to develop, implement, and maintain appropriate cybersecurity programs for the courts and to train court personnel on methods to counter threats and protect judicial information systems from cyber intrusions or data breaches.").

challenge . . . ."[9] This period was marked by tensions between the need for openness and creativity and the role of security and safety. The Department of Defense implemented the Defense Federal Acquisition Regulation Supplement Safeguard Rule in 2013 requiring defense contractors to implement IT security controls. In 2014, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity was released, outlining the elements of a comprehensive cybersecurity program.[10] Then, in 2015, President Obama issued an executive order that allowed the administration to impose sanctions on those that threaten U.S. infrastructure,[11] and finally the Cybersecurity Information Sharing Act of 2015 was passed to improve information sharing between the government and private sector.[12]

As we begin the year 2016, "data and information sharing will likely be woven more deeply into daily life."[13] Regulators will need to address the issue of privacy and the right to control information. Businesses and the government will be called on to implement security measures for a growing cyberworld. One of the most difficult challenges will be regulating global business as we attempt to navigate international efforts to ensure worldwide security. In this period, security measures will focus less on reacting to events and more on preventative measures. It will be all about finding the balance between privacy and security as we merge big data with small data.[14] So how has the executive branch been navigating this balance thus far?

I. EXECUTIVE ORDERS REGARDING CYBERSECURITY

A. President Clinton

President Clinton signed the first executive order, Executive Order 13035, pertaining to the cyber sector on February 11, 1997.[15] This order established the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet.[16] The committee consisted of twenty-five or fewer non-federal members appointed

---

9 CROWELL & MORING, *supra* note 1, at 9.

10 CROWELL & MORING, *supra* note 1.

11 *Id.*

12 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).

13 CROWELL & MORING, *supra* note 1.

14 Small data refers to personal information belonging to an individual. Big data refers to information associated with corporations or government entities.

15 Exec. Order No. 13035, 62 Fed. Reg. 7131 (Feb. 14, 1997), http://www.gpo.gov/fdsys/pkg/FR-1997-02-14/pdf/97-3992.pdf [http://perma.cc/D5WB-R4GJ].

16 *Id.*

by the President. The purpose of this committee was to provide the National Science and Technology Council with guidance and information regarding "high-performance computing and communications, Information Technology, and the Next Generation Internet."[17] This included an independent assessment of progress in designing and implementing the Next Generation Internet Initiative and the High-Performance Computing and Communications Program. The order stated that the Department of Defense would provide the financial and administrative support to the committee.[18]

Building on this framework, President Clinton also signed Executive Order 13133 on August 5, 1999, establishing the Working Group on Unlawful Conduct on the Internet, to report on the extent to which existing federal law offered an adequate basis for "effective investigation and prosecution of unlawful conduct that involves the use of the Internet."[19] The Order also sought information and recommendations regarding new technological tools that might be necessary for effective investigation and prosecution of unlawful Internet use, as well as the availability of new or existing tools to educate the population and prevent unlawful conduct involving the Internet.[20] The first attempts to organize the federal space met much resistance.

B. President Bush

President George W. Bush began with signing Executive Order 13231 on October 16, 2001, entitled "Critical Infrastructure Protection in the Information Age," with the purpose of encouraging "continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems."[21] The order established the "President's Critical Infrastructure Protection Board," to recommend policies and programs to "provide security and continuity to national security information systems."[22] In doing so, the Board would consult and coordinate with the private sector, as well as state and local governments, to ensure that systems were established and maintained with the capacity to share threat warning, analysis,

---

17 *Id.*

18 *Id.*

19 Exec. Order No. 13133, 64 Fed. Reg. 43895 (Aug. 5, 1999), http://www.gpo.gov/fdsys/pkg/FR-1999-08-11/pdf/99-20924.pdf [http://perma.cc/W458-2QGZ].

20 *Id.*

21 Exec. Order No. 13231, 3 C.F.R. § 13231 (2002), http://fas.org/irp/offdocs/eo/eo-13231.htm [http://perma.cc/QAA4-ZF6T].

22 *Id.*

and recovery information. Again, there was much resistance from both inside and outside of government.[23]

C. President Obama

Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," was signed by President Obama on October 7, 2011, in the wake of the WikiLeaks exposés.[24] It encouraged reforms to improve the security of cyber networks that house sensitive information.[25] It established multiple interagency groups to collaborate on security initiatives and put the burden of ensuring classified network security on "all agencies that operate or access classified computer networks."[26] The Order also recognized the importance of information sharing and established the Senior Information Sharing and Safeguarding Steering Committee as well as the Classified Information Sharing and Safeguarding Office, to ensure safe sharing of information.[27] Executive Order 13587 assigned the Secretary of Defense and the Director of the National Security Agency to serve as the Executive Agent for Safeguarding Classified Information on Computer Networks.[28] It also created a government-wide Insider Threat Task Force to detect, deter, and mitigate cyberthreats.[29]

President Obama's Executive Order 13636, entitled "Improving Critical Infrastructure Cybersecurity," was signed on February 12, 2013, to "improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."[30] The Order mandated the development of a "technology-neutral voluntary cybersecurity framework," in addition to promoting the adoption of cybersecurity practices and timely cyberthreat sharing.[31] It also directed the incorporation of privacy and civil liberties protections and the exploration of using existing regulations and policies to promote cybersecurity.[32] The Executive Order instructed the National Institute for Standards and Technology to collaborate with the private sector to establish best

---

23 *Id.*

24 *See* Exec. Order No. 13587, 3 C.F.R. § 13587 (2011), https://www.gpo.gov/fdsys/pkg/CFR-2012-title3-vol1/pdf/CFR-2012-title3-vol1-eo13587.pdf [http://perma.cc/6XPH-AYRJ].

25 *Id.*

26 *Id.*

27 *Id.*

28 *Id.*

29 *Id.*

30 Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013), https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf [http://perma.cc/55CS-QW22].

31 *Id.*

32 *Id.*

practices and create a cybersecurity framework.[33] It also directed DHS to promote the implementation of the framework.[34]

President Obama, seeing the need, signed Executive Order 13691, entitled "Promoting Private Sector Cybersecurity Information Sharing," on February 13, 2015.[35] The Order presented a framework for enhanced information sharing with the purpose of encouraging private sector companies to work together and work with the federal government to identify cyberthreats.[36] The Order first "encourage[d] the voluntary formation of [organizations engaged in the sharing of information related to cybersecurity], to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organization to partner with the Federal Government on a voluntary basis."[37] The Order instructed DHS to create a non-profit organization to establish voluntary standards for the information sharing and analysis organizations ("ISAOs") and authorized the Department to enter into information sharing agreements with ISAOs.[38] Privacy concerns were also addressed, as the Order instructed private sector ISAOs to abide by voluntary standards of privacy protections when information sharing.[39]

To grant the presidency more tools, President Obama signed Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," on April 1, 2015.[40] This Executive Order regarded the recent cyberthreats as a national security emergency.[41] It authorized the Secretary of the Treasury, in collaboration with the Attorney General and Secretary of State, to impose sanctions on those engaged in cyber-enabled activities that "are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States" and have the purpose or effect of "harming . . . entities in a critical infrastructure sector"

---

33 *Id.*

34 *Id.*

35 Exec. Order No. 13691, 80 Fed. Reg. 9349 (Feb. 20, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf [http://perma.cc/TH2R-P6C4].

36 *Id.*

37 *Id.*

38 *Id.*

39 *Fact Sheet: Executive Order Promoting Private Sector Cybersecurity Information Sharing*, WHITE HOUSE (Feb. 12, 2015), https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform [http://perma.cc/7DTG-4UJW].

40 Exec. Order No. 13694, 80 Fed. Reg. 18077 (Apr. 1, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-04-02/pdf/2015-07788.pdf [http://perma.cc/738U-S6TZ].

41 *Id.*

with "significant disruption to the availability of a computer or network," or "causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain."[42] The Executive Order also authorized the imposition of sanctions on those who knowingly receive or use trade secrets stolen by cyber-enabled activities (or provide material support) for financial gain when the theft threatens national security, foreign policy, or the financial stability of the country.[43]

As one can see, the executive orders increasingly engaged the federal bureaucracy and searched for ways to engage the private sector.

II. CURRENT PENDING LEGISLATION

But one key to the puzzle remained: the need for legislation. Executive power alone would not be sufficient. The following bills on cybersecurity pending in the 114th Congress were attempts to solve the issues. While several bills were proposed, those discussed below are the most comprehensive and the only then-pending cyber legislation with significant bipartisan support.

On Friday, December 18, 2015, lawmakers merged the first three information sharing cyber bills mentioned below into an omnibus spending plan, which was signed by President Obama. The Cybersecurity Act of 2015 includes an iteration of the Cybersecurity Information Sharing Act ("CISA"), which includes components from both the Protecting Cyber Networks Act ("PCNA") and the National Cybersecurity Protection Advancement Act ("NCPAA").[44]

A. Protecting Cyber Networks Act, H.R. 1560

This bill was sponsored by Republican Devin Nunes from California and was introduced on March 24, 2015. It was passed 307-116 in the House on April 22, 2015 and was received in the Senate on April 27, 2015.[45] The bill's purpose was to encourage businesses to share information regarding cybersecurity risks by providing them protection from liability.[46] Under the PCNA, the

---

42 *Id.*

43 *Id.*

44 Andrew Blake, *CISA Cyber Bill Squeezed into Omnibus Spending Plan*, WASH. TIMES (Dec. 16, 2015), http://www.washingtontimes.com/news/2015/dec/16/cisa-cyber-bill-squeezed-omnibus-spending-plan/ [http://perma.cc/A7FG-YQNK].

45 *H.R. 1560 - Protecting Cyber Networks Act*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/1560/actions [http://perma.cc/SE8Q-DEK6].

46 *See id.*; Chris Preimesberger, *House Finally Passes Cyber-Networks Protection Act*, EWEEK (Apr. 22, 2015), http://www.eweek.com/security/house-finally-passes-cyber-networks-protection-act.html [http://perma.cc/PC4E-WED9].

cyber information would be shared with civilian agencies, rather than DHS (as is the case with the NCPAA discussed below). The bill would require that businesses, prior to sharing information regarding a cybersecurity threat, "take reasonable efforts to remove personal information identifying individuals related to the threat."[47] Additionally, the bill required the Privacy and Civil Liberties Oversight Board to address Congress and the President every two years with regard to the sufficiency of procedures to address privacy concerns.[48]

The PCNA lists authorized uses of the information shared including: "cybersecurity, preventing death or serious bodily harm, preventing the exploitation of minors, preventing and prosecuting violent felonies, fraud and identity theft, and espionage and the theft of trade secrets."[49] Conversely, the NCPAA, discussed below, allows shared information to be used only for cybersecurity purposes.[50]

While the NCPAA empowers DHS's National Cybersecurity and Communications Integration Center ("NCCIC") to serve as the main hub for public and private-sector information sharing, the PCNA does not designate a hub, but rather gives the President the power to establish a government hub or hubs with which the private sector can share information while explicitly prohibiting information sharing with the Department of Defense.[51]

Critics of the bill argue that it does not include strong enough liability protections for non-federal entities.[52] The PCNA states, "[n]o cause of action shall lie or be maintained in any court against any non-federal entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure if such sharing or receipt is conducted in good faith."[53] This "good faith" standard is regarded as a lower standard (than "willful misconduct," for example) of proof and opens businesses up to a greater risk of litigation.[54]

Critics also attacked the bill's privacy protections, arguing that the bill would give companies the ability to share data with

---

47 Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015).

48 *Id.* § 107.

49 David Inserra & Riley Walters, *House Cyber Information Sharing Bills: Right Approach but Require Fixes,* HERITAGE FOUND. (Apr. 10, 2015), http://www.heritage.org/research/reports/2015/04/house-cyber-information-sharing-bills-right-approach-but-require-fixes [http://perma.cc/85GH-HNEH].

50 *Id.*

51 David Eppstein, Cyber Bills Compared (Dec. 17, 2015) (unpublished working paper) (on file with author); *see also* H.R. 1560 § 103.

52 Inserra & Walters, *supra* note 49.

53 H.R. 1560 § 106(b).

54 *Id.*

intelligence agencies, allowing them to ignore laws like the Privacy Act of 1974 and the Electronic Communication Privacy Act of 1986.[55] However, proponents of the bill argued that there are strong privacy protections because the bill limits the categories of sharable information to only the listed cyberthreat indicators and requires two scrubs of personal information from the shared information: one by the private sector business and one by the government.[56]

B. National Cybersecurity Protection Advancement Act, H.R. 1731

This bill was sponsored by Republican Michael McCaul from Texas and was introduced on April 13, 2015.[57] The House Homeland Security Committee passed it nearly unanimously.[58] It was designed to provide liability protections to those businesses who voluntarily share data regarding cyberthreat indicators and defensive measures with one another and with DHS's NCCIC. The bill would grant liability for private businesses to perform network awareness sweeps of their own data systems and would permit the NCCIC to share information concerning cybersecurity threats with private businesses, in addition to other non-federal bodies.[59] Without these liability protections, businesses sharing information pursuant to this bill could expose themselves to class actions or regulatory enforcement actions.[60]

The NCPAA included several provisions limiting the privacy threat of information sharing, such as a prohibition on federal use of shared data to engage in surveillance for the purpose of tracking persons' individually identifiable information.[61] The bill also required DHS to create and review annually privacy policies and processes that direct the "receipt, retention, use, and disclosure" of information shared with NCCIC in accordance with the bill.[62] Another privacy protection in the NCPAA would require private businesses to remove all personal information

---

55 Andy Greenberg, *Privacy Critics Go 0-2 with Congress' Cybersecurity Bills*, WIRED (Mar. 26, 2015, 4:16 PM), http://www.wired.com/2015/03/privacy-critics-go-0-2-congress-cybersecurity-bills/ [http://perma.cc/DJ35-NY9A].

56 *H.R. 1560*, Legislative Digests, HOUSE REPUBLICANS (Apr. 22, 2015), http://www.gop.gov/bill/h-r-1560-the-protecting-cyber-networks-act/ [http://perma.cc/643H-35KM].

57 National Cybersecurity Protection Advancement Act, H.R. 1731, 114th Cong. (2015).

58 *Id.*

59 H.R. 1731 - National Cybersecurity Protection Advancement Act of 2015, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/1731 [http://perma.cc/82MJ-RBRU].

60 Daniel Farris & Lindsay Kessler, *House Passes the National Cybersecurity Protection Advancement Act*, JDSUPRA BUS. ADVISOR (Apr. 25, 2015), http://www.jdsupra.com/legalnews/house-passes-the-national-cybersecurity-69958/.

61 H.R. 1731 § 3.

62 *Id.*

that is not related to the cyberthreat before sharing the information with the NCCIC or private bodies.[63] The NCCIC would then be required to conduct a second screening in order to ensure that there is no personal information unrelated to the cyberthreat before sharing the information with other government or private groups.[64]

This bill was viewed by technology, telecommunications, and infrastructure businesses as "a critical compliment to the PCNA."[65] It also was viewed as favorably expansive, allowing the NCCIC to include tribal governments, information sharing and analysis groups, and the private sector, in addition to expanding the NCCIC's functions to include global cybersecurity measures with international partners.[66] Its liability protection had been given positive reviews as well. The NCPAA states that a "non-federal entity . . . shall not be liable in any civil or criminal action brought under this subsection unless such non-federal entity engaged in willful misconduct or gross negligence with respect to sharing or conduct and such gross negligence or willful misconduct proximately caused the injury."[67] The standard of "willful misconduct or gross negligence" is a strong standard and protects businesses, and thus incentivizes the sharing of cyber information.[68]

While the liability provisions of the NCPAA were strong and widely praised, critics suggested that the bill could be improved by broadening the authorized uses of the shared information, as the NCPAA restricts the government use to just "cybersecurity purposes."[69] Critics suggested allowing the government's use of properly shared information as long as *one* significant use is for cybersecurity purposes, pointing to the authorized uses in the PCNA as a model.[70]

C. Cybersecurity Information Sharing Act of 2015, S. 754

Republican Senator Richard Burr from North Carolina sponsored this bill. It is the Senate counterpart to the PCNA and was introduced on March 17, 2015, and passed 74-21 in the Senate on October 27, 2015.[71] CISA would provide liability

---

63 *Id.*
64 *Id.*
65 Farris & Kessler, *supra* note 60.
66 *Id.*
67 H.R. 1731.
68 Inserra & Walters, *supra* note 50.
69 *Id.*
70 *Id.*
71 Cybersecurity Information Sharing Act, S. 754, 114th Cong. (2015); *S.754 – Cybersecurity Information Sharing Act of 2015*, CONGRESS.GOV, https://www.congress.gov/

protections to companies of the private sector that share information about security breaches or vulnerabilities with particular government entities. Like the PCNA, CISA would authorize voluntary sharing of information between the government and private companies through a portal established by DHS.[72] Also similar to PCNA, CISA would protect information shared against disclosure under the Freedom of Information Act and similar state laws.[73] Both the PCNA and the CISA would also provide protection from private suits and would codify Federal Trade Commission and Department of Justice policy that cybersecurity information sharing does not encroach upon antitrust laws.[74]

Critics of the CISA, including major technology companies, like Apple, Twitter, and Reddit, argued that the bill has major privacy and Internet security concerns. First, they argue that CISA would allow surveillance of Internet users and does not include adequate privacy protections of personal information. Second, it does not include any recourse for consumers if their personal information were to be improperly shared with the federal government. Third, the liability protections in the bill would discourage businesses from improving their own security measures.[75]

All three of these information sharing bills contain a federal preemption clause, meaning they would supersede any state statutes or provisions of state law that regulate an activity expressly authorized under one of these bills. This could limit states' ability to combat cyberthreats, which are sometimes arguably better equipped to collaborate with the private sector to prevent cyberthreats.

D. Cybersecurity Act of 2015

The Cybersecurity Act of 2015, which is Division N of the most recent omnibus spending bill, was passed by Congress and signed by President Obama on December 18, 2015.[76] The Act

---

bill/114th-congress/senate-bill/754 [http://perma.cc/L7HQ-VKN7].

72 Eppstein, *supra* note 51; *see also Summaries for the Cybersecurity Information Sharing Act of 2015,* GOVTRACK.US, https://www.govtrack.us/congress/bills/114/s754/summary [http://perma.cc/G3LD-7R2L].

73 Greg Nojeim & Jadzia Butler, *Guide to Cybersecurity Information Sharing Act Amendments*, CTR. FOR DEMOCRACY & TECH. (Oct. 23, 2015), https://cdt.org/blog/guide-to-cybersecurity-information-sharing-act-amendments/ [http://perma.cc/HP74-PRZC].

74 David Navetta & Utsav Mathur, *Sharing Cyber Threat Information: A Legal Perspective,* ISSA 29 (Jan. 2015), http://www.dataprotectionreport.com/wp-content/uploads/sites/489/2015/01/Sharing-Cyber-Threat-Information_ISSAS0115.pdf [http://perma.cc/U5PQ-5BMK]; *see also* Eppstein, *supra* note 51.

75 *See Summaries for the Cybersecurity Information Sharing Act of 2015, supra* note 72.

76 Cybersecurity Act of 2015, Pub. L. No. 114-113, 129 Stat. 2936.

establishes a voluntary cybersecurity information sharing procedure that encourages public and private entities to share cyberthreat information with one another.[77] Despite the outpour of divided reactions from various supporters and critics, the Act is meant to serve as a piece of compromise legislation, as provisions of both the PCNA and NCPAA influence it. However, it does not include language from the two pieces of pending legislation discussed below.[78]

Under the Act, the federal government is instructed to establish procedures for sharing classified and unclassified cyberthreat indicators and defensive measures with the private sector.[79] The Act's key information sharing provision states, "[a] non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure."[80] The private sector may only share data that falls within the Act's definitions of "cyber threat indicator" or "defensive measure." The Act defines a cyberthreat indicator as "information that is necessary to describe or identify [a cyberthreat]."[81] A defensive measure is "an action, device, procedure, signature, technique, or other measure" that "detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[82] Additionally, before sharing any information, the private sector entity must remove information that it "knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual."[83]

The Act tasks DHS with the job of creating a mechanism by which the government can receive cyberthreat indicators and defensive measures from the private sector. In real time, DHS must then share the information with the appropriate federal entities, including the Office of the Director of National Intelligence and the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury.[84] It also allows the President to designate other federal entities (in addition to DHS)

---

77 *Id.*

78 *See generally* David J. Bender, *Congress Passes the Cybersecurity Act of 2015*, NAT'L L. REV. (Dec. 20, 2015), http://www.natlawreview.com/article/congress-passes-cyber security-act-2015 [http://perma.cc/ATZ5-TRUN].

79 Cybersecurity Act of 2015 § 103, 129 Stat. at 2940–41.

80 *Id.* § 104(c)(1), 129 Stat. at 2942.

81 *Id.* § 102(6), 129 Stat. at 2938.

82 *Id.* § 102(7), 129 Stat. at 2938.

83 *Id.* § 104(d)(2)(A), 129 Stat. at 2943.

84 *Id.* § 102(3), 129 Stat. at 2937; *see also id.* § 105(a)(3)(A), 129 Stat. at 2945.

to develop an information sharing process, excluding the Department of Defense.[85]

The Act provides several privacy protections for those entities that choose to participate in information sharing. First, it limits the government's use of the shared information to use only for a "cybersecurity purpose," meaning "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[86] Second, the Act prevents federal agencies from disseminating the shared information, which the Act exempts from disclosure under the Freedom of Information Act.[87] Third, the private sector is immune from liability for sharing or receiving cyberthreat indicators or defensive measures.[88]

There have been varying degrees of support and opposition in response to the passing of the Cybersecurity Act. Supporters of information sharing believe that the increase in information sharing will improve the overall cybersecurity of our country. They argue that the Act has ample privacy protections and is voluntary. Critics call the Act a "surveillance bill" that encroaches upon privacy rights, and Section 104 of the Act, the key provision relating to Internet surveillance, has become a popular topic of discussion.[89] Section 104 allows network operators to take three steps only "for cybersecurity purposes." Network operators can (1) monitor, (2) operate defensive measures, and (3) share information. Additionally, with written consent, a network operator can allow an outside entity to monitor its network and operate defensive measures.[90] Those that oppose Section 104 argue that it gives a network operator too much power with little to no guidance or limitations. For example, the Act allows monitoring for "cybersecurity purposes," which is arguably broad and unclear.[91]

---

85 *Id.* § 105(c)(2)(B), 129 Stat. at 2948.

86 *Id.* § 102(4), 129 Stat. at 2937.

87 *Id.* § 105(d)(3), 129 Stat. at 2950.

88 *Id.* § 106(a)–(b), 129 Stat. at 2951–52.

89 *See* Tom Risen, *Obama Signs Cybersecurity Law in Spending Package*, U.S. NEWS & WORLD REP. (Dec. 18, 2015, 5:49 PM), http://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package [http://perma.cc/97TL-5CQM].

90 *Id.* § 104, 129 Stat. at 2940–43.

91 Orin Kerr, *How Does the Cybersecurity Act of 2015 Change the Internet Surveillance Laws?*, WASH. POST (Dec. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/ [http://perma.cc/5LYK-BWQD].

E. Bills Not Incorporated into the Act of 2015

1. Data Security and Breach Notification Act of 2015

Not incorporated into the Cybersecurity Information Sharing Act of 2015 were two pieces of pending legislation dealing with state power and resources. On December 9, 2015, the House Financial Services Committee approved the Data Security Act of 2015 by a 46-9 vote. This act would supplant 47 state laws with a single national statute, requiring minimum-security protections at businesses in the private sector and establishing a national requirement for data breach notification. The private sector is generally in favor of a single law because it will provide a uniform standard to comply with, as opposed to various state laws. The legislation "identifies security controls organizations should adopt, including those involving access controls and restrictions, use of encryption of sensitive information and monitoring systems. The bill also directs businesses to require their third-party service providers to implement appropriate safeguards for sensitive information."[92]

The Data Security Act would allow businesses in different sectors to adopt security procedures that would work best with their specific needs. Regulatory enforcement would occur among several different agencies, including the Federal Trade Commission, the Comptroller of the Currency, the Federal Reserve System, and the Securities and Exchange Commission, among others. Business entities covered by the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act would be exempt from the Data Security Act.[93]

Critics of the legislation, including Democratic Representative Denny Heck from Washington, believe it takes the power to regulate security among insurers away from states' insurance commissioners, whom Heck contends work smoothly together. The legislation would also usurp laws in twelve states that call for businesses in their jurisdiction to adopt particular IT security procedures.[94] Massachusetts Assistant Attorney General Sara Cable testified before Congress earlier this year and contended that preempting state laws "represents a significant retraction of existing protections for consumers at a time when such protections are imperative. Minimum data security standards are

---

92 Eric Chabrow, *House Panel OK's National Breach Notification Bill*, GOV INFO SECURITY (Dec. 9, 2015), http://www.govinfosecurity.com/house-panel-oks-national-breach-notification-bill-a-8734 [http://perma.cc/QN57-KDUJ].

93 *Id.*

94 *Id.*

important and necessary, but the proposed standards leave consumers' data vulnerable."[95] This led Democrat Maxine Waters of California to present an amendment that would allow states to provide more stringent security requirements. However, the panel struck down the amendment on a voice vote, as Massachusetts was the only state that had stronger data security requirements than those presented in the Data Security Act.[96]

Critics also believe that this one-size-fits-all approach to cybersecurity will not be effective. Jennifer Safavian, an executive vice president at the Retail Industry Leaders Association, stated in a letter sent to the Committee's leaders that "[h]aphazardly slapping rules that were written 15 years ago for the financial industry on retailers, restaurants and thousands of small businesses is not the kind of data security legislation that will safeguard our economy."[97]

Privacy advocates, as well as consumer protection organizations, argue that the legislation would weaken consumer protections by stifling new and/or developing state laws that extend data security and breach notification protections to online account login systems. They argue that the bill would also abolish all opportunities of redress for consumers.[98] In a December 7, 2015 letter to the Committee's leaders, seventeen privacy and protection groups wrote: "If this bill were to pass, state attorneys general would be limited to seeking civil penalties and injunctive relief, even in cases where consumers suffer extensive harm as a result of a breach of highly sensitive information."[99]

2. State and Local Cyber Protection Act of 2015, H.R. 3869

On December 10, 2015, the House unanimously passed a bill that would provide state and local government with federal funds to battle cybercrime.[100] The bill's sponsor is Republican Representative Will Hurd from Texas. He is a former CIA officer who focused on cybersecurity and now chairs the House Oversight Subcommittee on Information Technology. Hurd stated, "[l]ocal governments often do not have access to the technical capabilities and training required to address highly

---

95 *Id.*

96 *Id.*

97 *Id.* (quoting Jennifer Safavian).

98 *Id.*

99 *Id.* (quoting letter from privacy and consumer protection groups).

100 *H.R.3869 – State and Local Cyber Protection Act of 2015*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/3869/actions?q=%7B%22search%22%3A%5B%22%5C%22hr3869%5C%22%22%5D%7D&resultIndex=1 [http://perma.cc/H8LG-EYUH].

exploitable cybersecurity vulnerabilities."[101] The bill amends the Homeland Security Act of 2002 to require the NCCIC, DHS's cyber group, to assist state and local governments with technical and strategic training to enhance their cyber defense.[102] The NCCIC is tasked with aiding state and local governments with identifying vulnerabilities in their systems, providing guidelines and information related to information security, conducting trainings on cybersecurity, and providing technical assistance with regard to implementing security systems.[103] The bill is now awaiting further action in the Senate.[104]

III. CYBERATTACK HOT TOPICS LEFT OPEN

Although the Cybersecurity Act of 2015 is a sound first step, there are a number of issues that still need to be resolved. With the evolution of technology, ensuring sound cyber protections and preventing attacks has become increasingly important and increasingly difficult. Even the federal government is having difficulties enlisting the tech industry to help fight terrorism. While the tech community is willing to help, it is reluctant to reveal private information and data to the government for fear of user distrust and the misuse of sensitive information. White House representatives traveled to Silicon Valley in early January 2016 in an effort to convince tech companies of the importance of working with the government to keep our country safe. Needless to say, there was push back. A chief security officer at the tech company Twistlock pleaded with the "Obama administration to consider alternative forms of intelligence gathering now that encryption technology has become so common."[105] There is a "Washington" v. "Silicon Valley" divide concerning how best to deal with cybersecurity.

Nevertheless, the tech community is willing to work with the government as long as proper protections are in place. After the meeting, Facebook noted that tech companies and the government were "united in [their] goal to keep terrorists and terror-promoting material off the Internet."[106] This strained

---

101 Katie Bo Williams, *House Unanimously Passes Bill Boosting Resources to Fight Cybercrime*, HILL (Dec. 10, 2015, 6:06 PM), http://thehill.com/policy/cybersecurity/ 262870-house-unanimously-passes-dhs-cyber-bill [http://perma.cc/8MMR-W244].

102 State and Local Cyber Protection Act of 2015, H.R. 3869, 114th Cong. § 2.

103 *Id.*

104 Williams, *supra* note 101.

105 W.J. Hennigan & Paresh Dave Tracey Lien, *White House Presses Silicon Valley to Aid in Terrorism Fight*, SEATTLE TIMES (Jan. 9, 2016, 3:49 PM), http://www.seattle times.com/nation-world/white-house-presses-silicon-valley-to-aid-in-terrorism-fight/ [http://perma.cc/L24N-U4C3].

106 *Id.*

safety/privacy conversation between White House representatives and Silicon Valley tech experts serves as an example of the many complications involved in cybersecurity. While terrorism is one worry associated with the ever-evolving cyberworld, the following issues of privacy, encryption, liability, and cyber insurance are at the forefront of concerns and debates.

A. Privacy: Who Owns the Information?

While there are many benefits to increasing data, connectivity, and other cyberservices, the developments in the cyberworld pose difficult challenges to ensuring privacy of sensitive information. Julie Brill of the U.S. Federal Trade Commission ("FTC") is one of the leaders in analyzing privacy and data security issues. In her recent speech at the Washington Governor Jay Inslee's Cyber Security and Privacy Summit, Brill stressed, "[c]onsumers want to know – and should be able easily to find out – what information companies are collecting, where they're sending it, and how they're using it. This kind of information is important to consumers' decisions about whether to use digital products and services in the first place."[107] She also mentioned the work the FTC has done to protect the privacy interests of consumers. For example, the FTC has brought actions against companies for inappropriately collecting private information from mobile devices and for revealing confidential health and other sensitive information.[108] In addition to the work of the FTC, other federal regulators, as well as state governments have enhanced privacy protections for consumers, but there is much more work to be done.[109]

One of the most widely discussed privacy issues with regard to cybersecurity centers around cyber information sharing between private entities and the government. Privacy and civil liberties groups cite many issues surrounding companies' duty to remove personally identifiable information ("PII") before sharing with the government. Critics are also skeptical about what the government does with this information when it is received and whether or not it is safely stored.[110] This debate is at the heart of the intersection of small and big data.

---

107 Julie Brill, U.S. Fed. Trade Comm'r, Privacy and Data Security in the Age of Big Data and the Internet of Things 1, 7 (Jan. 5, 2016) (transcript can be found at https://www.ftc.gov/system/files/documents/public_statements/904973/160107wagovprivacysummit.pdf [http://perma.cc/5D9X-WAQH]).

108 *Id.* at 3.

109 *Id.* at 4.

110 *See* Tal Kopan, *Obama to Sign Cybersecurity Bill as Privacy Advocates Fume*, CNN (Dec. 18, 2015, 1:51 PM), http://www.cnn.com/2015/12/18/politics/cybersecurity-house-senate-omnibus/ [http://perma.cc/5VXU-DS6K].

Privacy and civil liberties groups claim privacy concerns as the reason for their opposition towards the new cybersecurity bill signed by President Obama on December 18, 2015. They argue that the definition of acceptable information to share is too broad and the burden placed on companies to erase PII is not strict enough.[111] Nonetheless, the final version of the cybersecurity bill "compels entities to remove information they 'know' is extraneous personal information."[112] This is a higher standard than previous versions of the bill that used "reasonably believe" instead.[113]

Furthermore, DHS is sponsoring the nonprofit group Mitre Corporation's development of the Structured Threat Information eXpression ("STIX"). This would provide a "common language and mechanism for quickly analyzing, sharing, and receiving cyber threat information."[114] The adoption of a common sharing scheme would improve privacy, as there would be clearer guidelines as to what vulnerable information is shared and what is not.

Privacy issues also arise in the context of data breach reporting after a cyberattack has occurred. While there is no federal data breach statute, almost all of the states have data breach notification laws. Most state breach notification statutes are similar, however some do vary in several ways including: what constitutes a breach, what data is considered PII, and when a notification should be filed.[115] Most states agree on the general definition of PII—the attachment of certain information connected to someone's first and last name. However, states have not uniformly agreed upon what constitutes PII. For example, some states do not consider medical information, health insurance information, and email addresses to be PII.[116]

As the Internet and data sharing defy borders, privacy concerns do not affect the U.S. in isolation. The European Union's new data privacy law and the newly passed U.S. Cybersecurity Act set the tone for a pending U.S.-EU data sharing agreement to replace the Safe Harbor, which expedited

---

111 Tal Kopan, *Obama to Sign Cybersecurity Bill as Privacy Advocates Fume,* CNN (Dec. 18, 2015, 1:51 PM), http://www.cnn.com/2015/12/18/politics/cybersecurity-house-senate-omnibus/index.html [http://perma.cc/6DJ8-2YTM].

112 *Id.*

113 *Id.*

114 David Inserra & Paul Rosenzweig, *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace,* BACKGROUNDER, Apr. 1, 2014, at 6, http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace [http://perma.cc/EU29-SVTW]

115 JUDITH MILLER ET AL., A PLAYBOOK FOR CYBER EVENTS 39 (2d ed. 2014).

116 *Id.* at 39–40.

the transfer of data between businesses and international networks. The EU's new data privacy regulations have been deemed more burdensome for U.S. companies and aim to protect the consumer. This could affect U.S. companies operating in the EU if they are held to the new standards. In the coming months, we will see how the EU-U.S. negotiations play out and how that will affect international privacy concerns.[117]

B. Encryption: How Is Access to Be Granted to Information?

Encrypting data alters readable information into unreadable information except to authorized readers. This prevents anyone who steals data from reading it, rendering the stolen data worthless to cybercriminals. In addition to protecting data, companies encrypt data because it may exempt a company from particular regulatory requirements, such as some state data breach notification statutes. Some downsides to encryption include the time and effort it takes to encrypt all data, the cost, and the potential for slowed operating performance. While encryption/decryption occurs automatically for authorized readers, the process can require significant computing power and memory that can slow computer systems and affect productivity within the company. Therefore, it is most common for companies to encrypt some, but not all data.[118]

It is important to note that encryption does not fully protect a company, as encryption only protects data and not the security of networks and systems. Furthermore, companies must securely store and protect decryption keys/algorithms that could get in the hands of cybercriminals.[119]

Lawmakers have considered the argument in favor of strong encryption requirements as a means of protecting data from cyberattacks, as well as the argument against encryption by those who argue that it could hamper law enforcement efforts, as communication via encryption could allow terrorist and other criminals to avoid surveillance.[120] The problem with providing law enforcement "back door" access is that cybercriminals could easily misuse it, or sophisticated cybercriminals could communicate via unsanctioned encrypted data that does not

---

117 Stephen Dockery, *EU Data Law Shows Way Forward for Next Safe Harbor Agreement*, WALL ST. J. (Dec. 18, 2015, 3:25 PM), http://blogs.wsj.com/riskandcompliance/2015/12/18/eu-data-law-shows-way-forward-for-next-safe-harbor-agreement/.

118 JUDITH MILLER ET AL., *supra* note 115, at 12–13.

119 *Id.* at 14.

120 Joe Uchill, *Both Sides of Data Encryption Debate Face Off in Congress*, CHRISTIAN SCIENCE MONITOR (Apr. 30, 2015), http://www.csmonitor.com/World/Passcode/2015/0430/Both-sides-of-data-encryption-debate-face-off-in-Congress [http://perma.cc/YJ6P-M24J].

contain a back door, and thus, would prevent law enforcement from accessing the data.

In his article, "Be Careful What You Wish For: Device Hacking and the Law," cybersecurity expert Benjamin Wittes theoretically discusses the legal implications of allowing the government to bypass encryption systems, as opposed to requiring decryption. This would occur through the "exploitation of existing vulnerabilities to accomplish legally authorized wiretapping."[121] Wittes warns that allowing the government to bypass encryption systems would deprive the private sector of key legal protections. The scope of the information hacked would have no limit. It would also be unclear as to whether the carrier would be required to assist the government in installing the malware. He believes that in the context of a lawsuit, courts would ask whether the government's request for technical assistance is "unduly burdensome for companies," which has not been clearly defined. All in all, Wittes believes that lawful hacking would lead to the "government's commandeering companies into compromising their users' devices."[122]

This debate has its roots in the Communications Assistance to Law Enforcement Act of 1994, when telephone companies were required to assent to lawful wiretaps. As noted by the recent Harvard Berkman Center report, *Don't Panic: Making Progress on the "Going Dark" Debate*, the world of the Internet of Things has changed the playing field for encryption, and that is not that easy to achieve as world wide web standards and key elements of communication such as metadata and weak software provide many avenues for the state. As before, there is much debate over the ground truth concerning technical issues and the implications for the market and policy.[123]

Apple is now litigating the scope of the technical assistance language in the Wiretap Act, which requires carriers to assist government agents in lawful wiretaps. One potential public policy impact of requiring Apple to push government malware is that it could lead to a serious lack of trust in Apple and other service providers. Wittes believes that the case will likely turn on how difficult it would be for a company like Apple to

---

121 Benjamin Wittes, *Be Careful What You Wish for: Device Hacking and the Law*, LAWFARE (Jan. 6, 2016, 3:14 PM), https://www.lawfareblog.com/be-careful-what-you-wish-device-hacking-and-law [http://perma.cc/Y8MC-M9HT].

122 *Id.*

123 Matt Olsen et al., *Forward* to BERKMAN CENTER, DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE (2016).

unobtrusively send malware to its users. He mentions that it may also turn on who writes the malware.[124]

Despite the lawsuits, media attention, and airtime the topic of encryption has received at both the Republican and Democratic presidential debates, at this point there is no strong legislative push to give law enforcement access to encrypted data.[125]

C. Liability: Who Will Pay for Information Violations?

One of the most prevalent topics with regard to liability is information-sharing relevant to liability protections. In order to encourage businesses to share cyberthreat information with the government and other private sector companies, there must be liability protections to shield companies from lawsuits surrounding the shared data. The U.S. Department of Justice and the Federal Trade Commission jointly issued a Policy Statement in April 2014 acknowledging that antitrust laws do not attach liability to cybersecurity information sharing "as long as the sharing does not encroach on competitively sensitive information related to price, cost or output."[126] The agencies reasoned that the type of information shared in cyber information sharing is typically "very technical in nature and very different from the sharing of competitively sensitive information."[127] The White House agreed and President Obama stressed the importance of information sharing in Executive Order 13636.[128] Currently, companies are shielded from liability when sharing "cyber threat indicators," arguably a narrow liability protection.

Liability concerns for breached companies also involve private suits. It varies from state to state whether private actions can be brought against breached companies. Some do not allow any private suits, while others allow suits to recover damages. Suits are brought by clients, customers, vendors, and other business associates of the breached company. Courts are split on whether the data must be misused before a plaintiff can sue.[129] The new legislation affords some indemnification if the information is shared with DHS, but it is unclear what potential liability awaits from other regulatory agencies such as the FTC or the SEC.[130]

---

124 Wittes, *supra* note 121.

125 Matthew Mcdonald, *Making Sense of the Encryption Debate*, PHYS.ORG (Dec. 22, 2015), http://phys.org/news/2015-12-encryption-debate.html [http://perma.cc/C6GB-L685].

126 Navetta & Mathur, *supra* note 74.

127 *Id.*

128 *Id.*

129 MILLER ET AL., *supra* note 115, at 40.

130 Cybersecurity Act of 2015 § 106(a)–(b), Pub. L. No. 114-113, 129 Stat. 2936, 2951–52.

D. Cyber Insurance: How Will Risk over Information Be Allocated?

There are many expenses that a company may incur from a cyberattack. The expenses may involve: notification of clients, government agencies, credit monitoring services, forensic costs involved in the investigation, and legal costs surrounding claims or suits, as well as business interruption or the payment of judgments or settlements. The average cost of a cyberattack was $7.2 million in March 2011 and has likely risen since then. The majority of cost comes from the time and resources expended surrounding notification requirements.[131]

While resilient security systems may prevent most cyberattacks, there are some cyber intrusions that cannot be prevented, such as a zero-day attack.[132] In order to protect one's company from incurring the exorbitant costs that follow unpreventable breaches, cyber insurance has become more and more common. There are several types of insurance with varying degrees of protection. It is important to understand all the exclusions and gaps in coverage. Oftentimes multiple plans are necessary in order to have adequate protection. Insurance services organization commercial property policies may cover losses as a result of a virus, but oftentimes the policy requires the data to have been destroyed or corrupted.[133] General liability insurance covers only physical injury, in addition to liability as a result of publication of private material.[134] Professional liability insurance is limited by the term "professional services" or by exclusions.[135] Policies like the surety and fidelity computer crime policy oftentimes do not cover losses resulting from theft of private information, indirect consequential loss, and potential income.[136]

Cyber liability insurance is often offered as a stand-alone insurance policy with combined third-party liability and first-party coverage. It is designed to cover insureds that transmit and store private consumer data.[137] It is extremely important to review the coverage one's company has in place before an attack occurs in order to ensure adequate coverage. At this time, cyber liability insurance coverage can include: data breach/privacy crisis management (i.e. investigation, data notification, legal costs etc.), media liability (i.e. defacement of

---

131 RHODES & POLLEY, *supra* note 5, at 192–93.

132 *See What is a Zero-Day Vulnerability*, PC TOOLS, http://www.pctools.com/security-news/zero-day-vulnerability/ [http://perma.cc/T73X-HAMX].

133 *See* RHODES & POLLEY, *supra* note 5, at 192–93.

134 *Id.* at 193.

135 *Id.*

136 *Id.* at 192–93.

137 *Id.* at 194.

website and intellectual property rights infringement), extortion liability (i.e. losses due to threat of extortion), and network security (i.e. damages due to denial of access, costs related to theft of third-party data).[138] One advantage from a system perspective is that as insurance coverage expands, more elements of the private sector will enhance coverage to meet policy requirements.

CONCLUSION

Cybersecurity is hard because it requires the forging of the "geek-wonk" bridge. It involves the blending of technical and policy cultures. Moreover, to engage society in this arena, we have four large social hammers—legislation, insurance premiums, tax policy, and lawsuits. Increasingly we are seeing movement in each of these policy areas. In short, both carrots and sticks are being deployed against corporate America.

But our adversaries are not resting. The recently released report from the Defense Security Service provides a snapshot into the current state of the world's cybersecurity situation, detailing specific regions and industries at risk.[139] The report states that in the last year there has been an eight percent increase in reported foreign collection attempts to obtain sensitive or classified data in the U.S. cleared industrial base.[140] East Asia and the Pacific was the top collector region and the threat level from this region was labeled "critical."[141] The electronics sector topped the list as the most targeted sector, while the commercial sector remained the top collector affiliation.[142] Academic solicitation was reported as the top method of operation.[143] In order to prevent these threats and enhance national and global cybersecurity, the government and the private sector must balance security and privacy interests through a concise set of agreed-upon standards and approaches necessary to build worldwide cybersecurity. Waiting is no longer an option.

---

138 Sarb Sembhi, *An Introduction to Cyber Liability Insurance Cover*, COMPUTER WEEKLY (July 29, 2013), http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover [http://perma.cc/C92D-CJPL].

139 DEF. SEC. SERV., 2015 TARGETING U.S. TECHNOLOGIES: A TREND ANALYSIS OF CLEARED INDUSTRY REPORTING 10 (2014), http://www.dss.mil/documents/ci/2015_DSS_Trend_Report.pdf [http://perma.cc/M68R-DUNG].

140 *Id.*

141 *Id.*

142 *Id.*

143 *Id.* at 12.

Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk

*Scott J. Shackelford**

INTRODUCTION

Days after one of the largest data breaches in U.S. government history, in which the private information of more than twenty-two million current and former federal government employees was compromised,[1] hackers claiming an affiliation with Anonymous crashed several Canadian government websites.[2] Also in mid-2015, myriad firms including Blue Cross Blue Shield were targeted,[3] as was German Chancellor Angela Merkel;[4] even sports teams seem to be entering the fray with the FBI probing the St. Louis Cardinals baseball team about

* Assistant Professor of Business Law and Ethics, Indiana University; Edward Teller National Fellow, Stanford University Hoover Institution; Senior Fellow, Center for Applied Cybersecurity Research. An earlier version of this research was published as *Gauging a Global Cybersecurity Market Failure: The Use of National Cybersecurity Strategies to Mitigate the Economic Impact of Cyber Attacks*, *in* ECONOMICS OF NATIONAL CYBER SECURITY STRATEGIES (NATO Cooperative Cyber Defence Centre of Excellence, Pascal Brangetto ed., 2015). The author recently published an article discussing critical infrastructure protection, cybercrime, and cybersecurity governance practices across thirty-four nations. *See* Scott J. Shackelford & Andraz Kastelic, *Toward a State-Centric Cyber Peace?: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 895 (2015).

1 *See, e.g.*, Ryan Evans, *Why the Latest Government Hack is Worse than the Snowden Affair*, WASH. POST (June 17, 2015), http://www.washingtonpost.com/opinions/hitting-an-agency-where-it-hurts/2015/06/17/ffca6c6a-1512-11e5-9ddc-e3353542100c_story.html [http://perma.cc/3NSF-3GA8] ("[T]he United States' rivals and enemies may have the leverage they need to induce or coerce government employees and contractors into providing classified information."); Mike Levine & Jack Date, *22 Million Affected by OPM Hack, Officials Say*, ABC NEWS (July 9, 2015, 3:17 PM), http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731 [http://perma.cc/ZXJ6-M738].

2 *See Canada Government Websites Taken Down in Cyber Attack*, GUARDIAN (June 18, 2015), http://www.theguardian.com/technology/2015/jun/18/canada-government-websites-taken-down-in-cyber-attack [http://perma.cc/5QE3-6DD5].

3 *See* Scott Dance, *Cyberattack Affects 1.1 Million CareFirst Customers*, BALT. SUN (May 20, 2015, 10:03 PM), http://www.baltimoresun.com/health/bs-bz-carefirst-data-breach-20150520-story.html [http://perma.cc/DCV7-6AUQ].

4 *See Computer in Merkel's Office Hit by Cyber Attack: Report*, YAHOO! NEWS (June 14, 2015, 4:16 AM), http://news.yahoo.com/computer-merkels-office-hit-cyberattack-report-034919582.html [http://perma.cc/Z4RJ-YRCJ].

allegedly hacking into competitors' databases.[5] These events highlight both the tumultuous nature and diverse array of cyberthreats facing the public and private sectors around the world. Some have gone so far to argue that we are facing a market failure when it comes to effective, proactive cybersecurity management in which costs are not being effectively internalized to punish either bad actors or laggards.[6] A similar argument could be made looking at an array of national governments that run the gambit in terms of their efforts to enhance national cybersecurity. Are we then facing a global cybersecurity market failure? And if so, what can realistically be done about it to better protect intellectual property and civil rights and liberties in the digital age?

These are questions admittedly far too large and complex to comprehensively tackle in this Article, or indeed in a stand-alone volume. However, it is possible to lay a foundation for analysis that helps to break some new ground in the literature while assessing cybersecurity best practices from the public and private sectors that can cross-pollinate to help promote a global culture of cybersecurity. In particular, this Article analyzes State involvement in cybersecurity, including those policies aimed at mitigating cyberthreats targeting intellectual property that fall below the armed attack threshold—namely cybercrime and espionage—by analyzing thirty-four national cybersecurity strategies across the dimensions of economic espionage, intellectual property theft, and civil rights and liberties.[7] Although the focus is on national cybersecurity strategies, related domestic follow-up initiatives are also considered, including "voluntary" bottom-up initiatives being pursued by leading cyber powers like the United States and Germany, such as the U.S. National Institute for Standards and Technology ("NIST") Cybersecurity Framework.[8] The vital role of the private

---

5 *See Cardinals Sin: FBI Probes St. Louis Cardinals over Alleged Cyberattack*, AL JAZEERA (June 16, 2015, 1:37 PM), http://america.aljazeera.com/articles/2015/6/16/fbi-reportedly-probes-cardinals-over-cyberattack.html [http://perma.cc/5XV3-3KWP].

6 *See* Robert Beeres & Myriame Bollen, *An Economic Analysis of Cyber Attacks*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES 147, 153 (Paul Ducheine et al. eds., 2012) (discussing cybersecurity as a public good and, thus, we could define it as "the goods, services, measures and techniques [that aim] to enhance the feeling of being secure in cyberspace").

7 *See* Helen Stacy, Professor, Stanford Univ., International Humanitarian Law Issues, Remarks at the Meeting of the Committee on Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare (Apr. 11, 2007).

8 *See NIST's Voluntary Cybersecurity Framework May Be Regarded as de Facto Mandatory*, HOMELAND SECURITY NEWS WIRE (Mar. 3, 2014), http://www.homelandsecuritynewswire.com/dr20140303-nist-s-voluntary-cybersecurity-framework-may-be-regarded-as-de-facto-mandatory [http://perma.cc/39DQ-DN4W] (reporting on the extent to which NIST Framework recommendations are becoming more mandatory).

sector to help identify and instill cybersecurity best practices is also considered as part of a polycentric approach to fostering cyber peace.[9]

I. ASSESSING THE CYBERTHREAT LANDSCAPE

Analyzing the cost of cyberattacks globally or to any one particular nation is a difficult matter, made more so by the lack of verifiable data and a common vocabulary. Consider the figure often heard that more than $1 trillion has been lost to cybercriminals, which has been attacked for, among other reasons, the methodological problems associated with extrapolating global trends from limited (and sometimes unrepresentative) survey data.[10] Indeed, calculating the costs of attacks is also challenging for firms themselves, especially because of questions over the impact of a data breach on brand reputation, the price of downtime,[11] legal liability, and costs associated with a "competitor's access to confidential or proprietary information."[12] As a representative from TechAmerica, an advocacy group for the U.S. technology industry, wrote in late 2010, such "calculations are incomplete estimates at best, and sorely understated at worst."[13] Even as more jurisdictions move toward a more robust disclosure regime, problems continue; for example, even though the U.S. Securities and Exchange Commission has required that firms disclose "material" cyberattacks leading to financial losses since 2011,[14] still a

---

9 For more on this topic, see generally SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

10 Sheldon Whitehouse, U.S. Senator for R.I., Cyber Threats (July 27, 2010) (transcript available at http://www.whitehouse.senate.gov/news/speeches/sheldon-speaks-in-senate-on-cyber-threats [http://perma.cc/32CA-R8Z9]); *see also* Peter Maass & Megha Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012, 11:12 AM), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion [http://perma.cc/7BGN-QQSH] (critiquing McAfee and other estimates on which the $1 trillion figure was based).

11 *See, e.g.*, Katherine O'Callaghan et al., *Managing Unplanned IT Outages*, CIO (Jan. 24, 2010, 10:00 PM), http://www.cio.co.nz/article/468694/managing_unplanned_it_outages/ [http://perma.cc/4LEY-RNJ7].

12 Huseyin Cavusoglu, *Economics of IT Security Management*, *in* ECONOMICS OF INFORMATION SECURITY 71, 74 (L. Jean Camp & Stephen Lewis eds., 2004).

13 TechAmerica, Comments on Cybersecurity, Innovation and the Internet Economy 3–4 (Sept. 20, 2010), http://www.nist.gov/itl/upload/TechAmerica_Cybersecurity-NOI-Comments_9-20-10.pdf [http://perma.cc/UW8Z-BT3K].

14 U.S. SEC. & EXCH. COMM'N, DIV. OF CORP. FIN., CF DISCLOSURE GUIDANCE: TOPIC NO. 2 CYBERSECURITY (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [http://perma.cc/MM2Y-MTLZ]; *see also* Joel Bronstein, *The Balance Between Informing Investors and Protecting Companies: A Look at the Division of Corporation Finance's Recent Guidelines on Cybersecurity Disclosure Requirements*, 13 N.C. J.L. & TECH. 257, 271 (2012) (citing TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976), which defined "material" as "a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having

minority of publicly traded firms are offering data and even fewer are volunteering that it has had a significant financial impact on their operations.[15] As a result, some have gone so far as to argue that financial information about cybercrime reflects only "approximate guesses."[16] That is a difficult starting point, needless to say, for policymakers and managers alike.[17] Yet, that is the state of play at present. Thus, with those caveats, this Part provides some background on the cyber threat facing the global economy through the lens of three leading cyber powers—the United States, Germany, and China.

A. Global Losses to Cyberattacks

The true economic impact of cyberattacks is unknown, but contested estimates range from $400 billion to more than $2 trillion (which is a figure larger than estimates for the global illegal drugs market),[18] though in truth, no one really knows for sure how big of a problem cyberattacks are for the reasons stated above.[19] For example, cyberattacks are often broken down into four main categories: cyber terrorism, warfare, crime, and espionage.[20] But motivations can overlap and targets abound in

---

significantly altered the 'total mix' of information made available").

15 *See* Chris Strohm, Eric Engleman & David Michaels, *Cyberattacks Abound Yet Companies Tell SEC Losses Are Few*, BLOOMBERG BUS. (Apr. 3, 2013, 6:00 PM), http://www.bloomberg.com/news/articles/2013-04-04/cyberattacks-abound-yet-companies-tell-sec-losses-are-few [http://perma.cc/3D4E-GWJ8]; *cf.* Andrew Collins, *SEC Increases Scrutiny on Cyberattacks*, SUSTAINABILITY ACCT. STANDARDS BOARD (July 14, 2014), http://www.sasb.org/sec-increases-scrutiny-cyberattack-disclosures/ [http://perma.cc/859R-BP98] ("[T]he SEC has opened investigations of multiple companies, focusing on data security processes and disclosure on breaches (or lack of) to investors.").

16 Robert Richardson, *2007 CSI Computer Crime and Security Survey*, COMPUTER SECURITY INST. 3, http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf [http://perma.cc/T55H-N5UE].

17 Ross Anderson et al., *Measuring the Cost of Cybercrime*, *in* THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY 265, 266 (Rainer Böhme ed., 2013), http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf [http://perma.cc/45NS-92ZP].

18 *See, e.g.*, CTR. STRATEGIC INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME 2 (2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf [http://perma.cc/4Z6H-G4G2] [hereinafter CSIS]; *see also* Brian Taylor, *Cyberattacks Fallout Could Cost the Global Economy $3 Trillion by 2020*, TECHREPUBLIC (Feb. 20, 2014, 10:38 AM), http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/ [http://perma.cc/4ULX-UWQD].

19 *See, e.g.*, *U.S. Cybercrime Losses Double*, HOMELAND SECURITY NEWS WIRE (Mar. 16, 2010), http://homelandsecuritynewswire.com/us-cybercrime-losses-double [http://perma.cc/F2UP-7J7M]; *see also* U.N. OFF. ON DRUGS & CRIME, WORLD DRUG REPORT 127 (2005), http://www.unodc.org/pdf/WDR_2005/volume_1_web.pdf [http://perma.cc/H7XG-SYY3] (estimating the "[s]ize of the global illicit drug market in 2003" at more than $320 billion); Robert Vamosi, *The Myth of That $1 Trillion Cybercrime Figure*, SECURITY WK. (Aug. 3, 2012), http://www.securityweek.com/myth-1-trillion-cybercrime-figure [http://perma.cc/NC6R-W2XM].

20 *See, e.g.*, SCOTT CHARNEY, RETHINKING THE CYBER THREAT: A FRAMEWORK AND PATH FORWARD 5 (2009), http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=062754cc-be0e-4bab-a181-077447f66877.

cyberspace; how should one classify a state-sponsored cyberattack involving a criminal organization to conduct economic espionage, for example? Such ambiguity means that some estimates count trade secrets losses as cybercrime, while others as espionage, which is meaningful given the different legal avenues to pursue under each scenario. In many ways, describing a cyberattack, then, is in the eye of the beholder. Needless to say, though, cyberattacks are a large and growing problem for nations, firms, and ultimately, individuals around the world. The G20 nations were estimated to have lost $200 billion to cyberattacks in 2014 alone,[21] though it is also telling that a cohesive strategy has yet to emerge from this forum—comprising some 85% of the global economy—to get a better handle on the problem.[22] The elite cyber powers, though, are not fairing much better.

B. Impact on the Leading Cyber Powers

There is not yet a consensus on the identity of the leading global cyber powers. According to Booz Allen—a consultancy—for example, the top three contenders are the United Kingdom, United States, and Australia, in that order.[23] China is ranked thirteenth.[24] However, in terms of a "cyber footprint," the United States, Germany, and China are, in some ways, in a league of their own because of their leading technical industries and vulnerability to cyberattacks—the United States and Germany were the second and third most targeted nations as of June 19, 2015, according to the cybersecurity firm Kaspersky Labs.[25] Thus, each of these nations will be briefly discussed in turn to provide some context for discussion.

1. The United States

The United States is frequently described as being the nation with the greatest susceptibility to cyberattacks due to both the high number of insufficient networks and the presence of valuable—in some cases world-leading—trade secrets.[26] The

---

21 *See* Pierluigi Paganini, *McAfee Report on the Global Cost of Cybercrime*, SECURITY AFF. (June 10, 2014), http://securityaffairs.co/wordpress/25635/cyber-crime/mcafee-report-global-cost-cybercrime.html [http://perma.cc/38MN-FUH9].

22 *See id.*

23 *See* ECONOMIST INTELLIGENCE UNIT, BOOZ ALLEN HAMILTON, CYBER POWER INDEX: FINDINGS AND METHODOLOGY 4 (2015), http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf [http://perma.cc/T82L-Y25P].

24 *Id.*

25 *See Cyberthreat Real-Time Map*, KASPERSKY LAB, http://cybermap.kaspersky.com/ (last visited Mar. 26, 2016).

26 *See, e.g.*, Sharone Tobias, *2014: The Year in Cyberattacks*, NEWSWEEK (Dec. 31, 2014, 12:28 PM), http://www.newsweek.com/2014-year-cyber-attacks-295876.

impact of these attacks on the U.S. economy is large, some say enormous—more than 40 million U.S. citizens were victims of cyberattacks in 2014 according to one McAfee survey.[27] Likewise, a report by the U.S. Cyber Consequences Unit estimates losses from a major attack on U.S. critical infrastructure at roughly $700 billion.[28] Yet, despite the amount of current and potential loss, the U.S. government has been relatively slow at developing a comprehensive cybersecurity policy. In the face of congressional inaction, President Obama issued an executive order that, among other things, expanded public-private information sharing and established the NIST Framework comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure.[29] This Framework is important since, even though its critics argue that it helps to solidify a reactive stance to the nation's cybersecurity challenges,[30] it is spurring the development of a standard of cybersecurity care in the United States and beyond.[31] Whether it is enough to help protect the intellectual property of U.S. firms or the civil rights and liberties of U.S. citizens, though, remains to be seen.

2. Germany

According to Booz Allen, Germany "is one of only five countries (the others being the United Kingdom, the United States, France, and Japan) to have a comprehensive national cyber plan and a comprehensive cybersecurity plan" which is "a key to its success."[32] The impact of cyberattacks on the German economy has been severe, as it has for the United States and China, with a total loss for all three nations coming in at $200 billion.[33] Within Europe, Germany and the Netherlands

---

27 *See* CSIS, *supra* note 18, at 3.

28 *See* JAYSON M. SPADE, CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY 26 (Jeffrey L. Caton ed., 2012) (citing EUGENE E. HABIGER, CYBERWARFARE AND CYBERTERRORISM: THE NEED FOR A NEW U.S. STRATEGIC APPROACH 15–17 (2010)).

29 *See* NAT'L INST. OF STANDARDS AND TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK 1 (2013), http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf [http://perma.cc/QK8T-NY7U] [hereinafter NIST CYBERSECURITY FRAMEWORK].

30 Taylor Armerding, *NIST's Finalized Cybersecurity Framework Receives Mixed Reviews*, CSO (Jan. 31, 2014, 7:00 AM), http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html [http://perma.cc/4MNM-V9E9].

31 *See, e.g.*, Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 310 (2015).

32 ECONOMIST INTELLIGENCE UNIT, *supra* note 23, at 3.

33 *See* Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and Espionage Costs $445 Billion Annually*, WASH. POST (June 9, 2014), http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html [http://perma.cc/5XC3-3LFP].

particularly stand out for their losses to cybercriminals.[34] In sum, by some estimates Germany is losing approximately 1.6% of its GDP to cyberattacks annually.[35] Yet the German response to such cyber insecurity has been impressive. In particular, the federal government approved the German Cybersecurity Strategy (*Cyber-Sicherheitsstrategie für Deutschland*) in February 2011. The "[s]trategy recognizes cyberspace as an essential domain for the German state, economy, and society, and emphasizes the protection of critical infrastructure as a core cybersecurity policy priority."[36] Germany has also been active in identifying and spreading cybersecurity best practices in a similar vein as the NIST Framework. The Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, or "BSI") first released its IT Baseline Protection (*IT-Grundschutz*) in 1994.[37] This set of BSI standards contains recommendations for cybersecurity and has been adopted by German corporations and international stakeholders; some of the standards are now available in English, Swedish, and Estonian. In summary, Germany's comprehensive approach to cybersecurity policymaking stands in contrast to both the United States and China and has earned top marks for being the most robust cybersecurity legal environment in the world.[38]

3. China

Although much of the attention, especially in the Western press, has been paid to Chinese cyberattackers targeting the trade secrets of advanced firms, including those based in the United States and Germany, China is also a leading victim of cyberattacks; it is the second largest economy in the world with the most Internet users of any nation on Earth—some 640 million as of June 2015—more than double the number of U.S. citizens online.[39] Yet, as with the United States, China's cybersecurity strategy remains fragmented, even as its

---

34 *See* CSIS, *supra* note 18, at 9.

35 *See id.*

36 Scott J. Shackelford, Scott Russell & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Private Sector* (Chi. J. Int'l L. Research Paper No. 15-64, 2015) (representing the first publication of portions of these case studies); *see also Cyber-Sicherheitsstrategie für Deutschland*, FED. MINISTRY INTERIOR (2015), http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/cybersicherheitsstrategie_node.html [http://perma.cc/8AWD-JME5].

37 *See* Carsten Schulz, *BSI Offers Free IT Baseline Protection Manual, Solicits Comments*, IEEE COMPUTER SECURITY (1997), http://www.ieee-security.org/Cipher/Newsbriefs/1997/971004.bsiITmanual.html [http://perma.cc/CJG4-R6EN].

38 *See* ECONOMIST INTELLIGENCE UNIT, *supra* note 23, at 5.

39 *See Internet Users by Country (2014)*, INTERNET LIVE STATS, http://www.internetlivestats.com/internet-users-by-country/ [http://perma.cc/8Q7WG-CVCL].

development and implementation has recently garnered political support of high-ranking senior government officials.[40] Among the actions taken in China's current cybersecurity strategy are enhanced critical infrastructure protections "addressing China's dependency on foreign technology as a security issue, the promotion of Chinese cryptography standards, the build-up of broadband infrastructure, next-generation mobile technology, and e-government services."[41] Civil liberties and, until relatively recently, intellectual property protection have not been priorities for the Chinese government.[42] Indeed, China's official government position remains that "[p]roperly guiding Internet opinion is a major measure for protecting Internet information security."[43] Yet even with this broad scope of state-centric regulation, as compared to the more bottom-up NIST Framework and BSI Standards, China's efforts have been criticized as lacking effective enforcement or being otherwise misguided,[44] which may help explain China's lower cyber power rating relative to the United States or Germany.[45]

C. Summary

Although the onus is on the cyber powers in many ways to be norm entrepreneurs and enhance global cybersecurity, there is no island in cyberspace. Nations around the world have a role to play in combating this global collective action problem. Yet as we

---

40 *See China Must Evolve from a Large Internet Nation to a Powerful Internet Nation*, XINHUANET (Feb. 27, 2014, 8:43 PM), http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm [http://perma.cc/4DZ8-TEYQ].

41 Shackelford, Russell & Kuehn, *supra* note 36, at 20; *see also* Hauke Johannes Gierow, *Cyber Security in China: New Political Leadership Focuses on Boosting National Security*, 20 MERCATOR INST. CHINA STUD.: CHINA MONITOR, Dec. 9, 2014, at 1, 2, http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf [http://perma.cc/Z2LX-7V24]. China is far from alone in seeking to protect its domestic industry in the name of enhancing cybersecurity. *See* Karen Kornbluh, *Beyond Borders: Fighting Data Protectionism*, 34 DEMOCRACY J. (2014), http://democracyjournal.org/magazine/34/beyond-borders-fighting-data-protectionism/?page=all [http://perma.cc/GW49-59RD]; Scott J. Shackelford, *How to Enhance Cybersecurity and Create American Jobs*, HUFFINGTON POST (July 16, 2012, 2:09 PM), http://www.huffingtonpost.com/scott-j-shackelford/how-to-enhance-cybersecurity_b_1673860.html [http://perma.cc/WUB3-C6E4].

42 *See China to Further Strengthen Intellectual Property Rights Protection*, CHINA BRIEFING (Mar. 26, 2013), http://www.china-briefing.com/news/2013/03/26/china-to-further-strengthen-intellectual-property-rights-protection.html [http://perma.cc/G2F2-PLJE].

43 Chris Buckley & Lucy Hornby, *China Defends Censorship After Google Threat*, REUTERS (Jan. 14, 2010, 9:02 AM), http://www.reuters.com/article/2010/01/14/us-china-usa-google-idUSTRE60C1TR20100114 [http://perma.cc/2G8E-7VUD].

44 *See* Bethany Allen-Ebrahimian, *The 'Chilling Effect' of China's New Cybersecurity Regime*, FOREIGN POL'Y (July 10, 2015), http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/ [http://perma.cc/TJD7-3TZX].

45 For more background on the comparative regulation of critical infrastructure, see generally Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

will see in Part II, the extent to which developed and developing nations alike are meeting this burden runs the gambit, opening the door for other potentially more innovative stakeholders, including the private sector.

II. THE BIRTH AND EVOLUTION OF NATIONAL CYBERSECURITY STRATEGIES

Those, such as Judge Frank Easterbrook, who advocate "that efficiency is the desired outcome" of the law and that the free "market is the most desirable route to such efficiency," believe that regulation displaces competition and can even "defeat the market altogether."[46] However, some regulatory room is left even among free-market proponents to correct market imperfections.[47] The question then is which, if any, of the cyber powers, or other developed and developing nations, have gotten this cybersecurity regulatory balance right? Although a global analysis of cybersecurity regulation is beyond the scope of this Article, the focus here is on national cybersecurity strategies as a guide for better understanding the national strategic focus of these nations to guide the development of twenty-first century cyberspace. In all, thirty-four nations are investigated particularly as their policies relate to the economic impact of cyberattacks—including espionage mitigation and intellectual property protection—along with associated privacy and civil liberties issues.[48] First, though, a few notes are offered on methodology, as well as on the birth and evolution of national cybersecurity strategies, to provide a framework for discussion.

A. A Note on Methodology

The affirmative choice was made to conduct this targeted survey so as to analyze the thirty-four ("G34") published national cybersecurity strategies representing those nations with cybersecurity strategies in place and available in English as of

---

46 ANDREW D. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 165–66 (2007) (internal quotation marks omitted).

47 *Id.* at 166. *But see* Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, 3 HARV. NAT'L SECURITY J. 39, 82 (2011) (making the case against there being a cybersecurity market failure); Eli Dourado, *Is There a Cybersecurity Market Failure?* (George Mason Univ. Mercatus Ctr., Working Paper No. 12–05, 2012) (arguing that market failures are not so common in the cybersecurity realm).

48 For more background on methodology and other related issues, such as cybercrime, critical infrastructure protection, and governance, see Scott J. Shackelford & Andraz Kastelic, *Toward A State-Centric Cyber Peace?: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 895 (2015) (representing a comparative study of national cybersecurity strategies focusing on critical infrastructure protection, cybercrime, and governance).

September 2014.[49] These data were amassed from the European Union and NATO; all of the information is publicly available.[50] Documentation of key findings is included in Appendices A and B. It should also be noted that the following study only analyzes the instances in which certain key phrases were used in the national cybersecurity strategies, such a "trade secrets." More nuanced and methodologically sophisticated work is needed to unpack and compare these findings in greater detail.

B. Birth and Evolution of National Cybersecurity Strategies

In general, it could be said that national cybersecurity strategies stem from at least three needs. First, cybersecurity requires flexible adaptations beyond traditional security theory transposed to cyberspace. Volumes of unstructured data, inhumanly short time scales, and difficulties in attribution, among other challenges, mean that simplistic institutional models based on one-sided liability schemes, the arbitrary separation of public and private interests, or a focus solely on malevolent actors as the source of risk, are likely to do more harm than good due to adverse selection and moral hazard. Second, a cybersecurity strategy is a political act; it creates expectations and raises awareness among businesses and civil society. However, when addressing cybersecurity, governments need to answer the question of whether the competitive market can effectively enhance cybersecurity without regulatory interference, or whether policymakers must intervene to address market failures. Cybersecurity is structured in layers with incidents ranging from "people may die" to "people may lose trust in e-commerce" that require adapted answers and the involvement of many actors, thus rendering governance of cybersecurity difficult, as shown by the ambiguity in many of the cybersecurity strategies surveyed. Third, trust and "fair" governance must be strengthened such as by promoting impartiality, reflexivity, and proximity; cybersecurity may be

---

49 It should be noted that three additional nations—Belgium, Luxembourg, and Romania—also had strategies in place at this time, but they were not available in English as of this writing. We used Google Translate to help identify some of the relevant passages for other researchers, but kept those data out of our primary analysis to help ensure consistency. The countries analyzed are: Armenia, Australia, Austria, Canada, Colombia, Czech Republic, Estonia, Finland, France, Germany, Hungary, India, Italy, Japan, Latvia, Lithuania, Macedonia, Malaysia, Netherlands, New Zealand, Nigeria, Norway, Poland, Qatar, Romania, Russia, Slovakia, South Africa, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

50 *See National Cyber Security Strategies in the World*, ENISA, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world [http://perma.cc/2FGK-T7CG]; *Strategies and Policies*, NATO CCDCOE, https://www.ccdcoe.org/strategies-policies.html [http://perma.cc/527M-R94W].

seen as a factor impairing the openness of the Internet if incentives are not aligned.

Despite the need for comprehensive, transparent, and robust national cybersecurity strategies, they were relatively slow to get going. For example, the United States in many ways pioneered national cybersecurity, beginning with the creation of the first Cyber Emergency Response Team ("CERT") in 1988.[51] However, it was not the United States, but Russia that enacted among the first of what could be considered national cybersecurity strategies in 2000. Since then, though, the pace has picked up considerably with 2013 being the busiest year studied to date.[52] Still, while many of these new strategies have a great deal in common, they still diverge in myriad aspects including in the related areas of economic espionage, intellectual property protection, and civil rights, as is discussed next.

C. Analysis of National Cybersecurity Strategies

This section briefly reviews the G34 national cybersecurity strategies analyzed across the dimensions of economic espionage, intellectual property protection, and civil rights, with the goal of determining those areas in which practices may be converging, giving rise to opportunities for norm development to help promote cyber peace.

1. Economic Espionage and Intellectual Property Protection

Despite the attention paid to the dangers of economic espionage and trade secrets theft, many nations pay little if any attention to this aspect of the multifaceted cyberthreat in their national cybersecurity strategies. Only Russia's, for example, explicitly uses the term "trade secret." This is surprising given both the importance of trade secrets, comprising much of the value of many leading firms, as well as the substantial (and well-publicized) risk of cyberattackers poaching this invaluable and often hard-won intellectual property.[53] However, eleven nations (32%) did discuss the importance of intellectual property protections more generally,[54] while four nations (12%) referenced

---

51 *See About Us*, U.S. COMPUTER EMERGENCY READINESS TEAM, https://www.us-cert.gov/about-us [http://perma.cc/Q96X-L3LL]; *see also* SHACKELFORD, *supra* note 9, at 3.

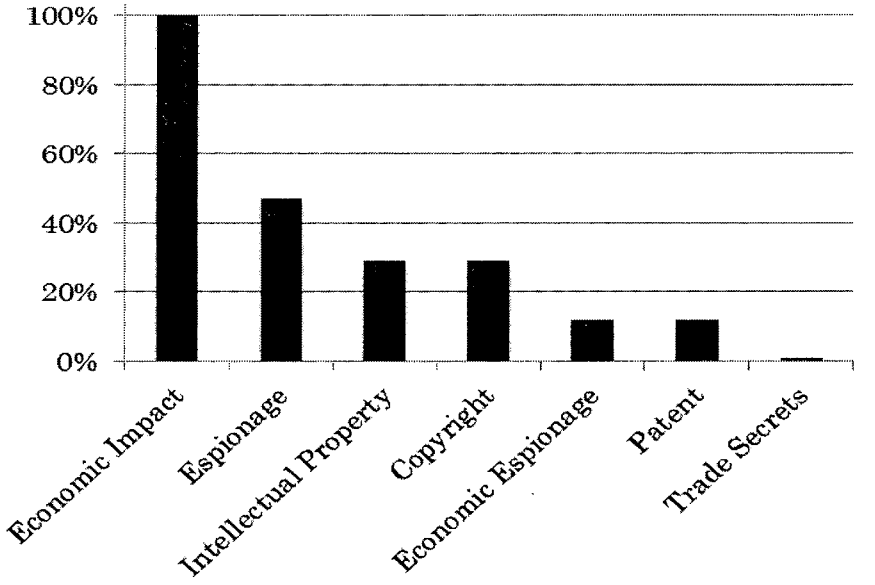
52 For more information on how this timeline breaks down, see Figure 5 in Shackelford & Kastelic, *supra* note 48, at 926.

53 *See, e.g.*, Robert Hackett, *Diplomacy Is Failing to Protect the United States' Trade Secrets*, FORTUNE (May 11, 2015, 1:51 PM), http://fortune.com/2015/05/11/diplomacy-is-failing-to-protect-the-united-states-trade-secrets/ [http://perma.cc/9JHF-M2DQ].

54 *See infra* Appendix A (these nations include: Armenia, Australia, Canada, Estonia, Japan, Malaysia, New Zealand, Qatar, Russia, the United Kingdom, and the United States).

patents.[55] All of the strategies at least mentioned the economic impact of cyberattacks. As for the causes of intellectual property theft, sixteen nations (47%) referenced the threat that espionage poses to the well-being of their national economies (as compared to 68% that discuss cybercrime perhaps owing to the sometimes more opaque nature of espionage).[56] Only four nations (12%) explicitly used the phrase "economic espionage" in their national cybersecurity strategies.[57]

Figure 1: Economic Espionage and Intellectual Property Protection Dimension Summary Chart[58]



2. Civil Rights and Civil Liberties

The difficulty of managing cyberattacks is oftentimes discussed as a balancing act between ensuring privacy and promoting cybersecurity.[59] That is one reason why cybersecurity reform legislation has been so contentious in the U.S. Congress,

55 *See id.* (these nations include: Australia, Italy, New Zealand, and Russia).

56 *See id.* (these nations include: Armenia, Australia, Austria, Canada, France, Germany, Italy, Japan, Netherlands, New Zealand, Norway, Russia, Spain, Switzerland, the United Kingdom, and the United States). For more information on how cybercrime is treated across these strategies, see Shackelford & Kastelic, *supra* note 48, at 916–19.

57 *See infra* Appendix A (these nations include: Japan, Spain, Switzerland, and the United Kingdom).

58 *See id.*

59 *See, e.g.*, Melissa Riofrio, *It's Privacy Versus Cybersecurity as CISPA Bill Arrives in Senate*, PCWORLD (Apr. 25, 2013, 3:00 AM), http://www.pcworld.com/article/2036328/it-s-privacy-versus-cybersecurity-as-cispa-bill-arrives-in-senate.html [http://perma.cc/5YGA-9E9Z].

such as with the Cyber Intelligence Sharing and Protection Act ("CISPA"), which aimed to boost information sharing to better manage cyberattacks; however, concerns arose regarding the type and quantity of personal information being shared.[60] Part of the difficulty arising in the U.S. context is that privacy itself is such a multi-faceted concept, meaning different things to different stakeholders. It encompasses (among much else) freedom of thought, of bodily integrity, solitude, information integrity, and the protection of reputation and personality.[61] Countries around the world strike the balance between the protection of individual privacy and security in varied ways that flex as perceived national emergencies and social trends ebb and flow.[62] This is seen in the national cybersecurity strategies surveyed. For example, twenty-two nations (65%) discussed "privacy" in their national cybersecurity strategies.[63] Such a high percentage may owe to the fact that many nations agree in principle that the individual's right to privacy is a human right recognized in international treaties, including the 1948 Universal Declaration of Human Rights, the 1966 International Covenant on Civil and Political Rights,[64] and a 2013 U.N. General Assembly Resolution that unanimously backed a "right to privacy in the digital age" in the aftermath of former NSA contractor Edward Snowden's revelations.[65] Other areas of agreement between the strategies include seventeen countries (47%) referencing "civil rights,"[66] while seven nations (21%) discuss "civil liberties" broadly.[67] This may be because "civil rights" create "legal actions

60 *See id.*

61 *See generally* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) (advocating a pragmatic approach to conceptualizing privacy).

62 *See* Emanuel Gross, *The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—The Proper Balance*, 37 CORNELL INT'L L.J. 27, 28–30 (2004) (recognizing that national tragedies can cause legal responses that limit privacy in extreme and irrational ways).

63 *See infra* Appendix B (these nations include: Armenia, Australia, Austria, Canada, Czech Republic, Estonia, Finland, Italy, Japan, Lithuania, Macedonia, Netherlands, Nigeria, Norway, Qatar, Russia, Slovakia, Spain, Switzerland, Turkey, the United Kingdom, and the United States).

64 G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at art. 12 (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."); *see also* G.A. Res. 2200 (XXI) A, International Covenant on Civil and Political Rights, U.N. GAOR, 21st Sess., U.N. Doc. A/6456, at art. 17 (Dec. 16, 1966) (reiterating text from Universal Declaration of Human Rights).

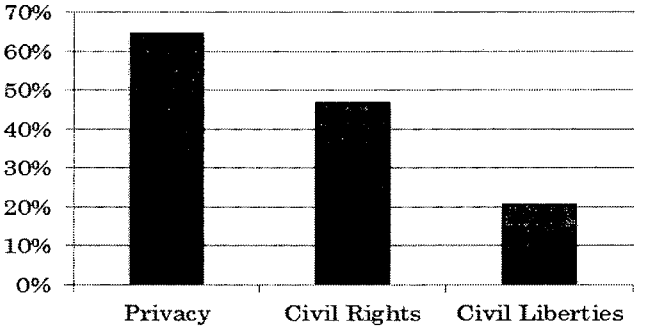
65 *General Assembly Backs Right to Privacy in Digital Age*, U.N. NEWS CTR. (Dec. 19, 2013), http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UtKxrPYjBkU [http://perma.cc/P3CU-JFBH].

66 *See infra* Appendix B (these nations include: Australia, Austria, Estonia, Czech Republic, Germany, Italy, Macedonia, Netherlands, Poland, Russia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States).

67 *See id.* (these nations include: Armenia, Australia, Hungary, Italy, Romania, the United Kingdom, and the United States).

that the government takes to create equal conditions for all people," whereas "civil liberties" refer "to protections against government actions," a perhaps more thorny topic that more nations seem unwilling or unable to tackle in their national cybersecurity strategies.[68] Relatedly, 56% of the G34 discuss information sharing as an integral strategy for managing cyberattacks generally, though not necessarily within the context of civil rights.[69]

Figure 2: Civil Rights and Civil Liberties Dimension Summary Chart[70]



C. Summary

There is a growing consensus that nations bear increasing responsibility for enhancing cybersecurity. Although a growing number of countries seem to be recognizing this fact by enacting national cybersecurity strategies, many are written as broad vision statements rather than comprehensive and concrete frameworks for enhancing national cybersecurity. More nations should emulate norm entrepreneurs such as Saudi Arabia, which has a detailed report of more than 100 pages in length, laying out its cybersecurity posture in great detail. Still, broad vision statements, while important, should be considered as merely one aspect of a global campaign to correct market failures surrounding cybersecurity. Hence, it is vital to focus not only on nations but also on other stakeholders, including the private sector, as part of a polycentric strategy to manage cyberattacks. In that perspective, businesses play a vital role in promoting cyber peace, such as by identifying and spreading cybersecurity best practices.

---

68 *Civil Rights vs. Civil Liberties*, STAN. J. CIV. RTS. & CIV. LIBERTIES (Oct. 18, 2013), https://journals.law.stanford.edu/stanford-journal-civil-rights-and-civil-liberties-sjcrcl/online/civil-rights-vs-civil-liberties [http://perma.cc/UU7H-W79G].

69 For more information on how information sharing is treated across these strategies, see Shackelford & Kastelic, *supra* note 48, at 913.

70 *See infra* Appendix B.

III. THE IMPORTANCE OF PRIVATE-SECTOR PARTNERSHIPS IN ENHANCING GLOBAL CYBERSECURITY

Space constraints prohibit a thorough rendering of the importance of active private-sector engagement to help create a global culture of cybersecurity.[71] However, two areas are briefly considered to help enrich the discussion. First is the necessity of investing in proactive cybersecurity best practices rather than relying on a reactive stance. Second is the NIST Framework, which is examined as an arguably successful mechanism for fostering public-private cooperation to enhance national cybersecurity.

A. Proactive Cybersecurity Best Practices

Proactive does not mean "hack back," which runs afoul of a wide array of national cybercrime laws including the U.S. Computer Fraud and Abuse Act.[72] Instead, the proactive cybersecurity movement includes technological best practices ranging from real-time analytics to cybersecurity audits promoting built-in resilience,[73] and may be considered to be a response to the more reactive stance of an array of companies.[74] Market leaders such as Microsoft and Google have helped to popularize such tactics as advanced threat intelligence sharing, enabling security companies to reasonably predict access attempts by malicious actors rather than guard against already known malicious traffic. Such an approach represents an opportunity for firms to create broad, collective defense partnerships; however, with whom and how intelligence is shared will impact both the success of those partnerships and how private-sector security actors shape evolving polycentric governance structures discussed in Part IV.[75] Likewise, many of

---

71 For more on this topic, see SHACKELFORD, *supra* note 9, at 3.

72 *See* 18 U.S.C. § 1030 (2012).

73 *See, e.g., Hackback? Claptrap!—An Active Defense Continuum for the Private Sector*, RSA CONF. (Feb. 27, 2014), http://www.rsaconference.com/events/us14/agenda/sessions/1146/hackback-claptrap-an-active-defense-continuum-for [http://perma.cc/PM3S-EF2Z] ("[A]ctive defense should be viewed as a diverse set of techniques along a spectrum of varying risk and legality."); *see also* Orla Cox, *Proactive Cybersecurity – Taking Control Away from Attackers*, SYMANTEC CONNECT (Apr. 2, 2014), http://www.symantec.com/connect/blogs/proactive-cybersecurity-taking-control-away-attackers [http://perma.cc/35TW-R37E]; Michael A. Davis, *4 Steps for Proactive Cybersecurity*, INFO. WK. (Jan. 18, 2013, 12:25 PM), http://www.informationweek.com/government/cybersecurity/4-steps-for-proactive-cyber security/d/d-id/1108270 [http://perma.cc/G4L7-BLTF].

74 For more on this topic, see SCOTT DYNES, INFORMATION SECURITY INVESTMENT CASE STUDY: THE MANUFACTURING SECTOR (2006), http://www.tuck.dartmouth.edu/cds-uploads/research-projects/pdf/InfoSecManufacturing.pdf [http://perma.cc/9QG5-SZ24].

75 For more background on the proactive cybersecurity movement, see Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721 (2015).

these same companies are involved in the race for better encryption to help safeguard their customers' data from unwanted intrusions in the wake of former NSA contractor Edward Snowden's leaks.[76] This is pitting Silicon Valley against the law enforcement community, fearing that in the name of protecting civil rights, national security may be compromised.[77] At the national level, industry collaboration is impacting the ways in which cybersecurity is being conceptualized and regulated, as was seen with the development of the NIST Framework introduced above.[78]

B. Case Study: NIST Framework

The difficulty of forming effective cybersecurity regulatory interventions is high, as is the cost if things go wrong. Hence, in part to avoid the regulatory confusion, more jurisdictions are moving toward bottom-up approaches to mitigate cyber risk. One such approach is the NIST Framework; first announced as an executive order in February 2013, the Framework version 1.0, *Framework for Improving Critical Infrastructure Cybersecurity*, was released in February 2014.[79] The NIST Framework harmonizes consensus standards and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk.[80] Yet the Framework also has its detractors. Some, for example, have cautioned that the Framework does not go far enough in terms of its scope, influence, or impact.[81] One of the main questions surrounding the NIST Framework is how "voluntary" it will actually turn out to be—as well as how

---

76 *See, e.g.*, Alan Rusbridger & Ewen MacAskill, *Edward Snowden Urges Professionals to Encrypt Client Communications*, GUARDIAN (July 17, 2014, 12:14 PM), http://www.theguardian.com/world/2014/jul/17/edward-snowden-professionals-encrypt-client-communications-nsa-spy [http://perma.cc/5HUZ-F6CS].

77 *See* Dina Temple-Raston, *FBI Director Brings Silicon Valley Encryption Fight to Capitol Hill*, NPR (July 8, 2015, 6:34 PM), http://www.npr.org/2015/07/08/421225069/fbi-director-brings-silicon-valley-encryption-fight-to-capitol-hill [http://perma.cc/WH9Y-AW58].

78 *See supra* Section I.B.1.

79 NIST CYBERSECURITY FRAMEWORK, *supra* note 29, at 1.

80 Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,739, 11,741 (Feb. 12, 2013).

81 *See, e.g.*, Tony Romm, *Cybersecurity Still in Slow Lane*, POLITICO (Feb. 9, 2014, 10:40 PM), http://www.politico.com/story/2014/02/cybersecurity-in-slow-lane-one-year-after-obama-order-103307.html?hp=f1 [http://perma.cc/8ZT4-K572] ("Nearly a year after President Barack Obama issued an executive order to improve the cybersecurity of the nation's vital assets, the administration doesn't have much to show: The government is about to produce only some basic standards, with little incentive for the private sector to participate."); *see also* Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR (Feb. 13, 2013), http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts [http://perma.cc/5TET-5DK6].

voluntary it should be—questions that turn in part on the extent to which a market failure is occurring in the global cybersecurity arena.[82] Yet, the NIST Framework is already having an impact, both in the U.S. context, in terms of identifying and reinforcing industry best practices, and beyond.[83] Indeed, already some private-sector clients are receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[84] This could arguably be an instance, then, of cybersecurity regulation occurring from the bottom-up, with this Framework helping to identify best practices and punish market participants that fail to follow them—which may help to better safeguard both intellectual property and civil rights both in the United States and beyond as part of a polycentric approach to fostering cyber peace.

IV. A POLYCENTRIC END GAME? ASSESSING THE PROSPECTS FOR CYBER PEACE

No nation is an island in cyberspace, even if some may wish they were.[85] Thus, a multifaceted, multi-stakeholder approach to global cybersecurity policymaking is required, which may be considered a polycentric undertaking. This final part discusses the literature on polycentric governance as a vehicle to promoting cyber peace and, in so doing, helping safeguard both privacy and intellectual property.

A. Introducing Polycentric Governance

The field of polycentric governance has been built up over some decades by the work of an array of eminent scholars led by Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom. This multi-level, multi-purpose, multi-functional, and multi-sectoral model[86] that challenges orthodoxy by demonstrating the benefits

---

82 *See, e.g.*, *NIST's Voluntary Cybersecurity Framework May Be Regarded as de Facto Mandatory*, *supra* note 8 (stating that experts have warned that many of the recommendations in the framework "may be used by courts, regulators, and even consumers to hold institutions accountable for failures that could have been prevented if the cybersecurity framework had been fully implemented by the respective institution").

83 *See EU Eying NIST Framework with 'Great Interest,'* INSIDE CYBERSECURITY, http://insidecybersecurity.com/daily-news/official-eu-eying-nist-framework-great-interest (last visited Mar. 26, 2016).

84 John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, PIVOTPOINT SECURITY (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework [http://perma.cc/48UL-8CHB].

85 *See, e.g.*, *10 Most Censored Countries*, COMMITTEE TO PROTECT JOURNALISTS, https://cpj.org/2015/04/10-most-censored-countries.php [http://perma.cc/L6YN-D2LL].

86 Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop*, 39 POL'Y STUD. J. 163, 171–72 (2011), http://php.indiana.edu/~mcginnis/iad_guide.pdf [http://perma.cc/769K-K32S] (defining polycentricity as "a system of

of self-organization, networking regulations "at multiple scales,"[87] and examining the extent to which national and private control can in some cases coexist with communal management, as may be seen in the success of the Internet Engineering Task Force ("IETF").[88] It also posits that, due to the existence of free riders in a multipolar world, "a single governmental unit" is often incapable of managing "global collective action problems,"[89] such as cyberattacks. Instead, a polycentric approach recognizes that diverse organizations working at multiple governance scales from companies to national governments to bilateral and regional alliances can create policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[90]

Although much of the fieldwork comprising polycentric governance was conducted in the domestic context, such as involving the governance of marine fisheries or commonly held pastures, the notion has more recently been applied to a range of global collective action problems, including climate change and cyberattacks.[91] The notion even seems to be diffusing beyond academia. The likes of the President of Estonia, Toomas Ilves, and the head of the Internet Corporation for Assigned Names and Numbers ("ICANN"), Fadi Chehadé, have used the term "polycentric" to describe an end game for Internet governance.[92] Such a model feeds off both public- and private-sector

governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes").

87 Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08–6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1 [http://perma.cc/BF4K-B534].

88 The IETF is responsible for managing the communications side of the Internet through voluntary mechanisms for fostering multi-stakeholder collaboration. For more background on IETF and the extent to which it may be considered a successful polycentric undertaking, see Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119 (2014).

89 Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change* 35 (World Bank, Policy Research Working Paper No. 5095, 2009), http://www.iadb.org/intal/intalcdi/pe/2009/04268.pdf [http://perma.cc/N2BF-VSUE].

90 Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 9 PERSP. POL. 7, 9 (2011); *cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").

91 *See* Ostrom, *supra* note 89; *see also* SHACKELFORD, *supra* note 9.

92 *See* Nancy Scola, *ICANN Chief: "The Whole World is Watching" the U.S.'s Net Neutrality Debate*, WASH. POST (Oct. 7, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/07/internet-operations-chief-snowden-disclosures-make-my-job-easier/ [http://perma.cc/2BQB-H479].

experimentation in which actors can learn about what works, and does not work, in the field of cybersecurity management without risking top-down governance structures crowding out such bottom-up innovative efforts. According to Professor Ron Diebert and Masashi Crete-Nishihata, "states learn from and imitate" one another, and "[t]he most intense forms of imitation and learning occur around national security issues because of the high stakes and urgency involved."[93] Due to the common perception on the part of many policymakers that cyber risk is "escalating out of control," an opportunity exists to engage in a constructive, polycentric dialogue on norm building to promote cyber peace.[94]

B. Toward Cyber Peace

The International Telecommunication Union ("ITU"), a U.N. agency specializing in information and communication technologies, pioneered some of the early work in the field by defining "cyber peace" in part as "a universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence . . . ."[95] Although certainly desirable, such an outcome is politically and technically unlikely, at least in the near term.[96] That is why cyber peace is defined here not as the absence of conflict, a state of affairs that may be called negative cyber peace.[97] Rather, it is the construction of a network

---

93 Ronald J. Deibert & Masashi Crete-Nishihata, *Global Governance and the Spread of Cyberspace Controls*, 18 GLOBAL GOVERNANCE 339, 350 (2012).

94 James Andrew Lewis, *Confidence-Building and International Agreement in Cybersecurity*, *in* DISARMAMENT FORUM: CONFRONTING CYBERCONFLICT 51, 51–53 (Kerstin Vignard, Ross McRae & Jason Powers eds., 2011). Though norms do not bind states like a treaty, Lewis notes that "[n]on-proliferation provides many examples of non-binding norms that exercise a powerful influence on state behavior." *Id.* at 53. This position has also been supported by other scholars. *See, e.g.*, Roger Hurwitz, *An Augmented Summary of the Harvard, MIT and U. of Toronto Cyber Norms Workshop* 5 (2012), http://citizenlab.org/cybernorms/augmented-summary.pdf ("At the very least, acceptance of a norm by a state puts the state's reputation at risk. If it fails to follow the norm, other states which accept that norm, will typically demand an explanation or account, rather than ignoring the violation or dismissing it as self-interested behavior.").

95 Henning Wegener, *Cyber Peace*, *in* THE QUEST FOR CYBER PEACE 77, 82 (Int'l Telecomm. Union & Permanent Monitoring Panel on Info. Sec., 2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf [http://perma.cc/Y2PC-FPGQ]. For more on the topic of cyber peace generally, see SHACKELFORD, *supra* note 9.

96 To its credit, though, the ITU report recognizes this fact, and that the concept of cyber peace should be broad and malleable given an ever-changing political climate and cyber threat landscape. Henning Wegener, *supra* note 95, at 78 ("The definition [of cyber peace] cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.").

97 The notion of negative peace has been applied in diverse contexts, including civil rights. *See, e.g.*, Martin Luther King, *Non-violence and Racial Justice*, CHRISTIAN CENTURY, Feb. 6, 1957, at 118, 119 ("True peace is not merely the absence of some negative force—tension, confusion or war; it is the presence of some positive force—justice, good will and brotherhood.").

of multi-level regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to enhance cybersecurity due diligence. Working together through polycentric partnerships, we can mitigate the risk of cyberwar by laying the groundwork for a positive cyber peace that respects human rights including privacy, spreads Internet access along with best practices to help safeguard valuable intellectual property, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[98]

CONCLUSION

This Article has assessed the extent to which national cybersecurity strategies are addressing the economic impact of cyberthreats as part of a larger discussion on the appropriate role for the State in regulating cybersecurity, particularly in the fields of protecting intellectual property and civil rights and liberties. Overall, we have found that, although more nations are publishing national cybersecurity strategies that discuss common concerns such as cybercrime, only a minority discuss the importance of protecting intellectual property generally, and far fewer trade secrets in particular. Likewise, though privacy is discussed by a supermajority of nations in their cybersecurity strategies, fewer discuss civil rights, and even less engage with civil liberties protections. Consequently, it may prove fruitful to look beyond national cybersecurity policymaking if progress is to be made toward enhancing global cybersecurity such as by engaging with the private-sector to help instill an array of proactive best practices, such as that which may now be occurring under the guise of the NIST Framework, which

98 *See* Johan Galtung, *Peace, Positive and Negative*, *in* THE ENCYCLOPEDIA OF PEACE PSYCHOLOGY 760, 760–62 (Daniel J. Christie ed., 2011) (comparing the concepts of negative and positive peace). Definitions of positive peace vary depending on context, but the overarching issue in the cybersecurity space is the need to address structural problems in all forms, including the root causes of cyber insecurity, such as economic and political inequities and legal ambiguities, as well as working to build a culture of peace. *Id.* "The goal is to build a structure based on reciprocity, equal rights, benefits, and dignity . . . and a culture of peace, confirming and stimulating an equitable economy and an equal polity." *Id.* at 761; *see also A Declaration on A Culture of Peace*, UNESCO, A/Res/53/243, www.unesco.org/cpp/uk/declarations/2000.htm [http://perma.cc/22DW-GBQX] (offering a discussion of the prerequisites for creating a culture of peace including education, multi-stakeholder collaboration, and the "promotion of the rights of everyone to freedom of expression, opinion and information").

includes a set of privacy best practices.[99] Over time, the success of this Framework and others could help promote legal harmonization and pave the way for norm convergence, or even a norm cascade, including in the fields of trade secrets theft and privacy.[100] But the road will be long, even as the destination may now be coming into sharper relief. Ultimately, we all have a role in safeguarding both privacy and intellectual property in the digital age as part of a polycentric, all-of-the-above approach to fostering cyber peace in an age of seemingly endless cyber insecurity.

99 *See* NIST CYBERSECURITY FRAMEWORK, *supra* note 29, at 15–16.

100 *See* Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 895–98 (1998).

Appendix A: Non-comprehensive Review of Economic Espionage and Intellectual Property Protection from G34 Nations

Country Name	Year	Title of Cybersecurity Strategy	Quoted Language & Provisions[101]
Armenia	2005	Armenia National Strategy to Secure Cyberspace	Armenia's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping Armenia information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the country's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems. (P.3) Cyber attacks on Armenia information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures. (P.3)
Australia	2009	Australian Government Cyber Security Strategy	The Statement indicates electronic espionage, both commercial and state-based, will be a growing vulnerability as the Australian Government and society become more dependent on integrated information technologies. It states that this challenge must and will be met with full vigour and identifies cyber security as amongst the Australian Government's top tier national security priorities. (P.4) The Australian Security Intelligence Organisation's (ASIO) responsibilities are defined by the

101 All material is quoted directly from the listed cybersecurity strategy.

			Australian Security Intelligence Organisation Act 1979 and, in relation to cyber security, include: • Investigating electronic attacks conducted for purpose of espionage, sabotage, terrorism or other forms of politically motivated violence, attacks on the defence system and other matters that fall under the heads of security in the *ASIO Act* (P.29) Australia is vulnerable to the loss of economic competitiveness through the continued exploitation of ICT networks and the compromise of intellectual property and other sensitive commercial data. This has the potential to undermine Australians' confidence in the digital economy. (P.4)
Austria	2013	Austrian Cyber Security Strategy	The term "cyber attack" refers to an attack through IT in cyber space, which is directed against one or several IT system(s). Its aim is to undermine the objectives of ICT security protection (confidentiality, integrity and availability) partly or totally. Cyber attacks directed against the confidentiality of an IT system are referred to as "cyber espionage," i.e. digital spying. Cyber attacks directed against the integrity and availability of an IT system are referred to as cyber sabotage. (P.20)
Belgium	2014	Cyber Security Strategy	*The text is only available in French and Dutch.*
Canada	2010	Cyber Security Strategy	Canadian organizations had suffered a cyber attack. The loss of intellectual property as a result of these attacks doubled between 2006 and 2008. (P.4) The most sophisticated cyber threats come from the intelligence and military services of foreign states. In most cases, these attackers are well resourced, patient and persistent. Their purpose is to gain political, economic, commercial or military advantage. (P.5)
Czech Republic	2011	Cybersecurity Strategy of the Czech Republic	N/A

Denmark	2012	Danish Defense Agreement 2013–17	N/A
Estonia	2008	Cyber Security Strategy	Other forms of cyber crime include harassment, fraud, the distribution of illegal materials or the violation of intellectual property rights. (P.11)
Finland	2013	Cyber Security Strategy	N/A
France	2011	Information Systems Defense and Security	Cyberspace, like a virtual battleground, has become a place for confrontation: appropriation of personal data, espionage of the scientific, economic and commercial assets of companies which fall victim to competitors or foreign powers, disruption of services necessary for the proper functioning of the economy and daily life, compromise of information related to our sovereignty and even, in certain circumstances, loss of human lives are nowadays the potential or actual consequences of the overlap between the digital world and human activity. (P.3)
Germany	2011	Cybersecurity Strategy	The interests of the private sector to protect itself against crime and espionage in cyberspace should also be adequately taken into account. (P.5) The capabilities of law enforcement agencies, the Federal Office for Information Security and the private sector in combating cyber crime, also with regard to protection against espionage and sabotage, must be strengthened. (P.6) A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage. (P.9)

Hungary	2013	National Cyber Security Strategy	N/A
India	2013	National Cyber Security Strategy	N/A
Italy	2013	National Strategic Framework for Cyberspace Security	Cybercrime is a plague that can cause the bankruptcy of firms and the theft of their intellectual property, crippling the wealth of an entire nation. (P.5) Cybercrime: all malicious activities with a criminal intent carried out in cyberspace, such as swindles or internet fraud, identify theft, stealing of data or of intellectual property. (P.13)
Japan	2013	Cybersecurity Strategy: Toward a World-Leading, Resilient and Vigorous Cyberspace	In the EU, in addition to natural disasters, terrorism and other situations, new transnational threats of economic espionage or state-sponsored cyber attacks have led to an awareness of the growing frequency and scale of cybersecurity incidents . . . (P.16–17) Private companies, educational institutions and research institutions possess intellectual property related information such as technological information, financial information, manufacturing technology information and drawings, as well as personal information such as client lists, personnel information and educational information, and other critical information. (P.25)
Latvia	2010	Law on the Security of Information Technologies	N/A
	2014	Cyber Security Strategy of Latvia	N/A
Lithuania	2011	Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019	N/A
Luxembourg	2011	National Strategy on Cyber Security	Extensive coverage from pages 4–10.
Malaysia	2006	National Cyber Security Policy	THRUST 5: Research & Development Towards Self-Reliance Formalise the coordination and prioritization of cyber security

			research and development activities Enlarge and strengthen the cyber security research community Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development Nurture the growth of cyber security industry (P.5)
Netherlands	2011	The National Cyber Security Strategy	The threats from other states mostly concern the theft of confidential or competition sensitive information (cyber espionage), while professional criminals mainly focus on digital fraud and theft of information. (P.7) More active approach to cyber espionage The Dutch government is committed to raising awareness among citizens, businesses, organization and government bodies about information security and privacy. This means that awareness campaigns will partly focus on increasing knowledge and insight into the risks of cyber espionage. On the other hand, the government also ensures that the issue is prioritized within the intelligence and security services, which are given the tools to better document cyber threats and investigate and combat advanced attacks. To this end, the intelligence and security services have combined their cyber capabilities in the Joint Sigint Cyber Unit (JSCU). Furthermore, the government will prioritize a better protection of data citizens share with the government and being more transparent about data management. (P.24)
New Zealand	2011	Cyber Security Strategy	Criminals are increasingly using cyber space to gain access to personal information, steal businesses' intellectual property, and gain knowledge of sensitive government-held information for financial or political gain or other malicious purposes. (P.1)

			Some of the most advanced and persistent cyber attacks on governments and critical infrastructure worldwide are thought to originate from foreign military and intelligence services or organised criminal groups. Media organisations around the world are reporting attacks on government systems, national infrastructure and businesses that have resulted in access to commercially sensitive information, intellectual property and state or trade secrets. (P.5)
Norway	2012	National Strategy for Information Security	The trend toward targeted and professional hacking of critical ICT systems is increasing. Targeted espionage attacks against vital national security interests now constitute a significant challenge. Civil services, military units and private companies are all vulnerable to espionage and sabotage. Many countries are developing capabilies for espionage and warfare against critical infrastructure. We must assume that sophisticated sabotage and attacks will be directed against critical information resources, including the computer systems that control industrial processes and critical infrastructure. (P.12)
Poland	2013	Cyberspace Protection Policy	N/A
Qatar	2011	National ICT Plan 2015: Advancing the Digital Agenda	Protecting the intellectual property rights of digital content creators. (P.19)
Republic of Korea	2010	2010 Defense White Paper	N/A
Romania	2013	Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security	N/A
Russia	2000	National Security Concept of the Russian Federation	[R]einforcing the mechanisms of legal governance of relations in the field of intellectual property protection, and creating conditions for observance of the federally prescribed restrictions on access to confidential information.

Saudi Arabia	2013	Developing National Information Security Strategy for the Kingdom of Saudi Arabia	N/A
Singapore	2013	National Cyber Security Masterplan 2018	N/A
Slovak Republic	2008	National Strategy for Information Security	N/A
South Africa	2010	Cyber Security Policy	N/A
Spain	2013	National Cyber Security: A Commitment for Everybody	The threats against information are those that cause the loss, miss-handling, disclosure or misuse of information. Among these threats are: • Espionage. Within this category all varieties of espionage are included, from state espionage to industrial espionage. (P.17)
	2013	The National Security Strategy: Sharing a Common Project	Espionage has adapted to the new landscape of the globalised world and currently makes use of the possibilities provided by information and communication technologies. Aggressions by States, groups or individuals for the purpose of gaining information that gives them strategic, political or economic advantages have been a constant feature in history and continue to pose a major threat to security. Economic espionage is of great importance in today's competitive environment and consists of the illegal procurement of information, industrial property or critical technology, and even involves attempts to exert illegal influence on political decisions of an economic nature. Its potential impact is increasing on account of its ability to harm the economic system and affect citizens' well-being. Spain, like the rest of the EU and NATO members, faces hostile actions from other States. These actions are always contrary to national interests – regardless of whether they originate from within or outside Spanish territory – and

			are particularly aggressive in situations of conflict or tension. Together with traditional espionage methods, these activities are increasingly based on sophisticated technological training programmes that can provide access to huge amounts of information and, in a worst-case scenario, to sensitive data. (P.33)
Sweden	2010	Strategy for Information Security in Sweden 2010 – 2015	N/A
Switzerland	2012	National Strategy for Switzerland's Protection Against Cyber Risks	The private sector is thus very vulnerable to cyber risks, e.g. attacks to deceive, to obtain unjust financial gain or for economic espionage. Therefore, the inclusion of all stakeholders (e.g. private sector, in particular CI operators, ICT service or system providers) in the strategy is essential in order to protect against cyber risks. (P.6)
Turkey	2013	National Cyber Security Strategy and 2013-2014 Action Plan	N/A
United Kingdom	2011	Cyber Security Strategy	Some of the most sophisticated threats to the UK in cyberspace come from other states which seek to conduct espionage with the aim of spying on or compromising our government, military, industrial and economic assets, as well as monitoring opponents of their own regimes. (P.15) Organisations are not always aware of the new vulnerabilities that dependence on cyberspace can bring. Intellectual property and other commercially sensitive information (for example, business strategies) can be attractive targets. (P.16) The Centre for the Protection of National Infrastructure delivers advice that aims to reduce the vulnerability of organisations in the national infrastructure to terrorism and other threats such as espionage, including those from cyberspace. (P.28) Business is the largest victim of crime and economic espionage

			perpetrated through cyberspace. (P.32)
United States	2008	Comprehensive National Cybersecurity Initiative	N/A
	2011	Department of Defense Strategy for Operating in Cyberspace	Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DoD, and national security, can be devastating. (P.3) While the threat to intellectual property is often less visible than the threat to critical infrastructure, it may be the most pervasive cyber threat today. Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. As military strength ultimately depends on economic vitality, sustained intellectual property losses erode both U.S. military effectiveness and national competitiveness in the global economy. (P.4)

Appendix B: Non-comprehensive Review of Civil Rights and Civil Liberties from G34 Nations

Country Name	Year	Title of Cybersecurity Strategy	Quoted Provisions
Armenia	2005	Armenia National Strategy to Secure Cyberspace	Privacy and civil liberties must be protected in the process. Because no cybersecurity plan can be unreceptive to sophisticated and intelligent attack, information systems must be able to operate while under attack and have the resilience to restore full operations quickly. (P.4)
Australia	2009	Australian Government Cyber Security Strategy	Australia must pursue cyber security policies that enhance individual and collective security while preserving Australians' right to privacy and other fundamental values and freedoms. Maintaining this balance is a continuing challenge for all modern democracies seeking to meet the complex cyber security challenges of the future. (P.vi) Confronting and managing these risks must be balanced against the civil liberties of Australians, including the right to privacy, and the need to promote efficiency and innovation to ensure that Australia realises the full potential of the digital economy. (P.4)
Austria	2013	Austrian Cyber Security Strategy	Governance in the area of cyber security has to meet the high standards of the rule of law of the Austrian administration and guarantee compliance with human rights, in particular privacy and data protection as well as the freedom of expression and the right to information. (P.7)
Belgium	2014	Cyber Security Strategy	*The text is only available in French and Dutch.*
Canada	2010	Cyber Security Strategy	The Government is taking steps to protect cyberspace from becoming a criminal haven. We will deny cyber criminals the anonymity they are seeking while at the same time protecting the privacy of Canadians. (P.12)

Czech Republic	2011	Cybersecurity Strategy of the Czech Republic	There is no way how to achieve absolute cybernetic security. The Czech Republic will adopt measures based on realistic evaluation of risks and shall be appropriate to such risks. They will respect protection of privacy and basic rights as free access to information, freedom of speech and others. The measures shall be appropriate to the necessity to ensure security on one side and to respect basic rights and freedoms on the other side. (P.5)
Denmark	2012	Danish Defense Agreement 2013–17	N/A
Estonia	2008	Cyber Security Strategy	The procurement of national cyber security should be based on the following principles and guidelines: • cyber security action plans should be integrated into the routine processes of national security planning; • cyber security should be pursued through the co-ordinated efforts of all concerned stakeholders, of public and private sectors as well as of civil society; (P.7) In the Organisation for Economic Co-operation and Development (OECD), the issue of cyber security is the responsibility of the Committee for Information, the Computer and Communications Policy and its working groups, including the Working Party on Information Security and Privacy. The Committee has adopted several recommendations, including the Recommendation Concerning Guidelines for the Security of Information Systems and Networks (2002) and the Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007). (P.25)
Finland	2013	Cyber Security Strategy	Protection of privacy means the protection against the unlawful or hurtful invasion of personal privacy. Protection of privacy includes the right to privacy and other associated rights in the processing of personal data. Personal data means any information on a private individual and any information on his/her

			personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household. (P.13)
France	2011	Information Systems Defense and Security	N/A
Germany	2011	Cybersecurity Strategy	N/A
Hungary	2013	National Cyber Security Strategy	N/A
India	2013	National Cyber Security Strategy	N/A
Italy	2013	National Strategic Framework for the Security of Cyberspace	Balancing these often diverging objectives is a complex endeavor, if one considers for instance how monitoring the technical functionality of networks is essential to allow the fulfillment of the right to privacy and the integrity of one's communication appliances, or also how it can be difficult to find the right balance between the right to privacy and the fight against criminal activities such as child pornography, drugs smuggling, hate incitement, or terrorism planning - crimes that not only hurt individual and social liberties, but also undermine the very existence of an open, democratic and free Internet. (P.11–12).
Japan	2013	Cybersecurity Strategy: Toward a World-Leading, Resilient and Vigorous Cyberspace	As a result, cyberspace has provided us a variety of positive benefits including innovation, economic growth, and solutions for social issues while still ensuring freedom of expression and protection of privacy. (P.20)
Latvia	2010	Law on the Security of Information Technologies	N/A
	2014	Cyber Security Strategy of Latvia	N/A
Lithuania	2011	Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019	The purpose of the Programme is to determine the objectives and tasks for the development of electronic information in order to ensure the confidentiality, integrity and accessibility of electronic information and services provided in cyberspace, safeguarding of electronic communication networks, information systems and critical information infrastructure against

			incidents and cyber attacks, protection of personal data and privacy, as well as to set the tasks, implementation of which would allow total security of cyberspace and entities operating in this medium. (P.1)
Luxembourg	2011	National Strategy on Cyber Security	N/A
Macedonia	2012	Strategy for Personal Data Protection in Republic of Macedonia 2012–2016	Everyone has right to privacy. I own my privacy, is the motto of the Directorate for Personal Data Protection. Personal data protection is part of our everyday life and base for functioning of the modern and democratic society grounded on the constitutional guarantees for respecting the fundamental human rights. Guarantying privacy means establishing system for technical and organizational measures by the controllers and processors of personal data, as well as high public awareness in the society as a unavoidable condition for reaction in case of breach of the right of privacy and evaluation of the achieved results. (P.4)
Malaysia	2006	National Cyber Security Policy	N/A
Netherlands	2011	The National Cyber Security Strategy	Together with private sector partners, the government works to develop standards that can be used to protect and improve the security of ICT products and services. (P.10) *The Internet of Things (everything is connected to the internet) and hyperconnectivity (everything is connected to each other)* promotes innovation and results in usability. At the same time, it raises the question of whether or not digitally linked products and services are actually safe and what the implications may be for privacy. (P.15)
New Zealand	2011	Cyber Security Strategy	N/A
Nigeria	2011	Cybersecurity Bill, 2011	Anyone exercising any function under this section shall have due regard to the individual right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate

			measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement. (P.8)
Norway	2012	National Strategy for Information Security	Personal privacy is also threatened by new methods of communication and ways to use information systems and the Internet. Identity abuse is a growing challenge for individuals, businesses and public authorities. (P.14)
Poland	2013	Cyberspace Protection Policy	N/A
Qatar	2011	National ICT Plan 2015: Advancing the Digital Agenda	ictQATAR is working with stakeholders to develop a legal framework to protect the privacy of personal information, which is critical to the healthy development of Qatar's ICT sector. This framework, targeted for completion by the end ot [sic] 2011, will set the minimum level of privacy protection required for all sectors, including finance, education, health, and law enforcement. The framework will draw upon international best practices, while being innovative, forward looking, and technology neutral in its approach. (P.22)
Republic of Korea	2010	2010 Defense White Paper	N/A
Romania	2013	Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security	N/A
Russia	2000	National Security Concept of the Russian Federation	[S]ecuring the constitutional rights and freedoms of man and the citizen to personal and family privacy, the secrecy of postal mail, telegraph, telephone and other communications, as well as to the defense of honor and reputation.
Saudi Arabia	2013	Developing National Information Security Strategy for the Kingdom of Saudi Arabia	N/A
Singapore	2013	National Cyber Security Masterplan 2018	N/A

Slovak Republic	2008	National Strategy for Information Security	The approach to addressing security is driven by the need to resolve a problem which originated from scientific and technological development and has by now fully translated into a global social issue. Society seeks to resolve this problem and ensure both the protection of its valuable assets and individuals' privacy. (P.4)
South Africa	2010	Cyber Security Policy	N/A
Spain	2013	National Cyber Security, a Commitment for Everybody	Spanish society must become aware of individual risks (privacy and intimacy) and collective risks (national security, economic, social and cultural prosperity) to which it would be exposed in the event of an irresponsible use of cyber space. The Government of Spain must lead an educational model and promote cyber security. (P.38)
Sweden	2010	Strategy for Information Security in Sweden 2010 – 2015	N/A
Switzerland	2012	National Strategy for Switzerland's Protection Against Cyber Risks	A second sphere where interests might conflict are *personal rights*: Efforts to improve protective mechanisms in cyberspace (e.g. through stricter controls or surveillance), must be weighed against the protection of privacy. It is one of the tasks of this strategy, to take such considerations into account and to show how measures can be taken circumspectively. (P.7)
Turkey	2013	National Cyber Security Strategy and 2013-2014 Action Plan	The principles of rule of law, fundamental human rights and freedoms and protection of privacy should be accepted as essential principles. (P.16)
United Kingdom	2011	Cyber Security Strategy	We are determined to tackle the threats, but in a way which balances security with respect for privacy and fundamental rights. At home and internationally the UK Government will continue to work to ensure that cyberspace remains an open space – open to innovation and the free flow of ideas, information and expression. (P.5) Actions to strengthen our national security must also be consistent with our obligations, such as those

			concerning freedom of expression; the right to seek, receive and impart ideas; and the right to privacy. Defending security should be consistent with our commitment to uphold civil liberties. Of course, these are well-established and ongoing debates, but cyberspace can bring them into focus in new ways, and more quickly than in other areas. (P.17) At home we will pursue cyber security policies that enhance individual and collective security while preserving UK citizens' right to privacy and other fundamental values and freedoms. (P.22)
United States	2008	Comprehensive National Cybersecurity Initiative	Finally, the President directed that these activities be conducted in a way that is consistent with ensuring the privacy rights and civil liberties guaranteed in the Constitution and cherished by all Americans. (P.1) The CNCI was developed with great care and attention to privacy and civil liberties concerns in close consultation with privacy experts across the government. Protecting civil liberties and privacy rights remain fundamental objectives in the implementation of the CNCI. (P.2)
	2011	Department of Defense Strategy for Operating in Cyberspace	DoD, working with its interagency and international partners, seeks to mitigate the risks posed to U.S. and allied cyberspace capabilities, while protecting and respecting the principles of privacy and civil liberties, free expression, and innovation that have made cyberspace an integral part of U.S. prosperity and security. (P.1)

Navigating the Cybersecurity Act of 2015

*Jasper L. Tran**

INTRODUCTION

The year 2014 was known as "the year of the cyber breach."[1] The year 2015 was not much different. High profile cyberattacks have been "a main topic of conversation in the boardroom and at the dinner table."[2] Every day, hackers target American businesses for purposes of cyberespionage and theft, stealing intellectual property, trade secrets, and sensitive government information.[3]

Congress slowly responded with several cybersecurity bills from both the House of Representatives and the Senate.[4] Most notably, the Senate introduced the Cybersecurity Information Sharing Act ("CISA" or S. 754),[5] while the House introduced the Protecting Cyber Networks Act ("PCNA" or H.R. 1560).[6] These bills share the same purpose: creating a pathway enabling private entities to share cyber information. How to share cyber information is what distinguishes the bills from one another. For instance, PCNA allows the private sector to share cyber information with the federal government but not through the NSA or the Department of Defense ("DOD"). On the other hand, CISA seeks to enhance and provide liability protections for information sharing between corporate entities, between corporate entities and the government, and between different

---

* Humphrey Policy Fellow, Google Policy Fellow. Sincere thanks to Tom Bell, Jeff Kosseff, Scott Schakelford, Denis Binder, Stephen Flores, Mike Hornak, David Groshoff, Drew Simshaw and other participants of the 2016 Symposium of the *Chapman Law Review* for their thoughtful comments. All views expressed herein are mine only, not those of my employer, sponsor, or affiliates. Contact me at tran4lr@gmail.com.

1 U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMM. ON INTELLIGENCE, THE PROTECTING CYBER NETWORKS ACT (H.R. 1560) (2015), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/new%20bill%20summary%20pdf.pdf [http://perma.cc/2FW8-9EUR].

2 *Id.*

3 *Id.*

4 *See, e.g.*, Cyber Information Sharing Act, S. 754, 114th Cong. (2015); Cyber Threat Sharing Act of 2015, S. 456, 114th Cong. (2015); Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015). *See generally infra* Parts I, II.

5 *See infra* Section I.B.1.

6 *See infra* Section II.B.1.

government agencies. This Article discusses these two bills in detail in Parts I and II.

As Congress considered the legislation, the President issued Executive Order 13636,[7] entitled "Improving Critical Infrastructure Cybersecurity,"[8] directing the National Institute of Standards and Technology ("NIST") to develop a "voluntary framework . . . for reducing cyber risks to critical infrastructure."[9] Accordingly, the NIST released a framework ("NIST Framework") in February 2014,[10] sharing many similar provisions of CISA and PCNA on information sharing.[11] This Article discusses Executive Order 13636 in Part III.

Given the federal government's strong interest in implementing a new cybersecurity information-sharing framework, CISA and PCNA, along with other cybersecurity bills, were combined into the Cybersecurity Act of 2015 ("CA'15"), discussed in detail in Part IV. The NIST Framework following Executive Order 13636 is already in place. Part V discusses my initial concerns about CA'15, and ethical implications and recommendations for practicing attorneys.

I. FROM THE SENATE: THE CYBERSECURITY INFORMATION SHARING ACT

A. CISA's History

In 2009, President Barack Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation," and recognized that the United States is "not as prepared as we should be, as a government or as a country."[12] In 2013, the Center for Strategic and International Studies conducted a study and concluded that cybercrime costs the United States roughly $100 billion annually.[13] In 2014,

---

7 Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

8 *Executive Order -- Improving Critical Infrastructure Cybersecurity*, WHITE HOUSE (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [http://perma.cc/8Z8X-TRQT] [hereinafter WHITE HOUSE'S *Executive Order*].

9 *Executive Order 13636: Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH. (Nov. 12, 2013), http://www.nist.gov/cyberframework/ [http://perma.cc/E44P-WLXY].

10 *Id.*

11 *See generally* WHITE HOUSE'S *Executive Order*, *supra* note 8.

12 *Remarks by the President on Securing Our Nation's Cyber Infrastructure*, WHITE HOUSE (May 29, 2009), https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure [http://perma.cc/DNH4-DJW6].

13 Siobhan Gorman, *Annual U.S. Cybercrime Costs Estimated at $100 Billion*, WALL ST. J. (July 13, 2013, 6:49 PM), http://www.wsj.com/news/articles/SB10001424127887324328904578621880966242990.

PricewaterhouseCoopers surveyed and found that 69% of U.S. executives worry about the impact of cyberthreats to their company's growth, as compared to 49% of global executives who reported the same concern.[14]

From 2006 to 2015, incidents of loss, theft, and exposure of personally identifiable information increased by 1100%.[15] There were 3207 reported incidents of data breaches in 2012 and 813 million records exposed in 2013.[16] The year 2014 alone accounts for 67,168 cyber incidents against federal agencies, 27,624 of which involved personally identifiable information.[17] In 2015, the U.S. Office of Personnel Management suffered the theft of personal information[18] of 4.2 million current and former federal employees, and of 19.7 million applicants for background investigations.[19] These numbers only account for known incidents released to the public—the real numbers are likely much higher.

The threats are escalating,[20] calling for a nationwide security reform. The Senate responded by introducing CISA to enhance and provide liability protections for information sharing between corporate entities, between corporate entities and the government, and between different government agencies.[21]

CISA first appeared in the 113th Congress on July 10, 2014, as S. 2588, introduced by Senator Dianne Feinstein (D-CA).[22] It

---

14 PRICEWATERHOUSECOOPERS, U.S. CYBERCRIME: RISING RISKS, REDUCED READINESS 5 (2014), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf [http://perma.cc/UJ85-WMMF].

15 *S. 754 – Cybersecurity Information Sharing Act of 2015*, SENATE REPUBLICAN POL'Y COMMITTEE (Aug. 3, 2015), http://www.rpc.senate.gov/legislative-notices/s-754_cybersecurity-information-sharing-act-of-2015 [http://perma.cc/GAC5-M8GA] [hereinafter SENATE REPUBLICAN POL'Y COMMITTEE].

16 Fred Donovan, *Confirmed: 2014 Is the Worst Year Ever for Data Breaches*, FIERCE IT SECURITY (Nov. 20, 2014), http://www.fierceitsecurity.com/story/confirmed-2014-worst-year-ever-data-breaches/2014-11-20 [http://perma.cc/H7AS-73WK].

17 Andrea Peterson, *This Terrifying Chart Explains Why Cybersecurity Is Such a Big Problem for the Government*, WASH. POST (June 18, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/18/this-terrifying-chart-explains-why-cybersecurity-is-such-a-big-problem-for-the-government/ [http://perma.cc/BFJ2-5PNY].

18 Such personal information includes full name, birth date, home address, and Social Security numbers. *Cybersecurity Resource Center: Cybersecurity Incidents*, U.S. OFF. PERSONNEL MGMT., https://www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatHappened [http://perma.cc/Z3N7-YMKW].

19 *Id.* The 19.7 million figure does not include an additional "1.8 million non-applicants, primarily spouses or co-habitants of applicants." *Id.*

20 *See* SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15. In fact, cybersecurity experts warn that a very big cyber attack is coming, predictably affecting everyone in America "and we don't even know it." Christopher Mims, *The Hacked Data Broker? Be Very Afraid*, WALL ST. J. (Sept. 8, 2015), http://www.wsj.com/articles/the-hacked-data-broker-be-very-afraid-1441684860.

21 *See generally infra* Section I.B.1.

22 *S.2588 – Cybersecurity Information Sharing Act of 2014*, CONGRESS.GOV, https://

passed the Senate Select Committee on Intelligence by a 12–3 vote, but did not reach a full senate vote before the end of the congressional session.[23] CISA reappeared again in the 114th Congress on March 12, 2015, as S. 754 by Senator Richard Burr (R-NC) and passed the Senate Intelligence Committee by a 14–1 vote.[24] S. 754 combines two Senate bills: CISA, and S. 456, the Cyber Threat Sharing Act of 2015 ("CTSA").[25]

B. CISA in Detail

It is important to note that CISA is strictly voluntary, i.e., there is no duty to share.[26] It expressly prohibits the federal government from coercing parties into sharing.[27] It also provides a safe harbor for participating entities, when they share information according to CISA's provisions; CISA does not shield entities from potential liability for failing to act. Parties taking advantage of CISA could use defensive measures, but they are prohibited from hacking back (i.e., harming a third party's system).[28] Furthermore, shared information can be used to prosecute cybercrimes and as evidence for crimes involving physical force.[29]

1. CISA's Notable Provisions[30]

CISA's purpose is "[t]o improve cybersecurity in the United States through enhanced sharing of information about

---

www.congress.gov/bill/113th-congress/senate-bill/2588?q=%7B%22search%22%3A%5B%22%5C%22s2588%5C%22%22%5D%7D&resultIndex=2 [http://perma.cc/EQE6-8UVS].

23 *See* Gregory S. McNeal, *Controversial Cybersecurity Bill Known as CISA Advances out of Senate Committee*, FORBES (July 9, 2014, 6:55 AM), http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/ [http://perma.cc/7A3V-G6GS].

24 *See* Andy Greenberg, *CISA Cybersecurity Bill Advances Despite Privacy Concerns*, WIRED (Mar. 12, 2015, 7:18 PM), http://www.wired.com/2015/03/cisa-cybersecurity-bill-advances-despite-privacy-critiques/ [http://perma.cc/L3A7-WGU3].

25 Taylor Armerding, *Cybersecurity Legislation Still Draws Intense Opposition*, CIO (Sept. 23, 2015, 7:08 AM), http://www.cio.com/article/2985469/security/cybersecurity-legislation-still-draws-intense-opposition.html [http://perma.cc/A77Z-MVNP].

26 Patrick Eddington, *OPM, CISA, and the Cybersecurity Oxymoron*, JUST SECURITY (July 2, 2015, 10:08 AM), https://www.justsecurity.org/24360/opm-cisa-cybersecurity-oxymoron/ [http://perma.cc/K8R8-RXS4].

27 John Evangelakos et al., *Sullivan & Cromwell Discusses the Cybersecurity Act of 2015*, CLS BLUE SKY BLOG (Jan. 6, 2016), http://clsbluesky.law.columbia.edu/2016/01/06/sullivan-cromwell-discusses-the-cybersecurity-act-of-2015/ [http://perma.cc/6ZG8-F8FV].

28 *Data, Privacy & Security Practice Report – January 19, 2016*, KING & SPALDING (Jan. 16, 2016), http://www.kslaw.com/News-and-Insights/PublicationDetail?us_nsc_id=9483.

29 *This Week the Cybersecurity Information Sharing Act Is on the Senate Floor & Apple Vehemently Opposes it*, PATENTLY APPLE (Oct. 21, 2015), http://www.patentlyapple.com/patently-apple/2015/10/this-week-the-cybersecurity-information-sharing-act-is-on-the-senate-floor-apple-vehemently-opposes-it.html [http://perma.cc/U6GM-H6NL].

30 The provisions described are from the version available in September 2015.

cybersecurity threats."[31] Section 1 sets out the title of the bill as the "Cybersecurity Information Sharing Act of 2015," and includes a table of contents of ten total sections.[32]

a. Sections 2 and 3

Section 2 defines various terms: agency, antitrust laws, appropriate federal entities, cybersecurity purpose, cybersecurity threat, cyberthreat indicator, defensive measure, entity, federal entity, information system, local government, malicious cyber command and control, malicious reconnaissance, monitor, private entity, security control, security vulnerability, and tribal.[33] Particularly, subsection 2(4) defines "cybersecurity purpose" as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[34]

Notably, subsection 2(7) defines "defensive measure" as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability," excluding "a measure that destroys, renders unusable, or substantially harms an information system or data on an information system."[35] The authorization to employ defensive measures forbids an entity from gaining unauthorized access to a computer network.[36]

Section 3 discusses the federal government's timely sharing of information through procedures developed and promulgated by the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate federal entities.[37]

b. Section 4: Authorizations

Section 4 discusses authorization for preventing, detecting, analyzing, and mitigating cybersecurity threats: subsection 4(a) on authorization for monitoring, subsection 4(b) on authorization for operation of defensive measures, subsection 4(c) on authorization for sharing or receiving cyberthreat indicators or measures,

---

31 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).
32 *Id.* § 1.
33 *Id.* § 2.
34 *Id.* § 2(4).
35 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.
36 *Id.*
37 S. 754 § 3(a).

subsection 4(d) on protection and use of information, and subsection 4(e) on antitrust exemption.[38]

Specifically, subsection 4(a) "[e]nables a private entity to monitor information systems for a cybersecurity purpose."[39] Subsection 4(b) "[e]nables a private entity to operate a defensive measure that is applied to information systems for cybersecurity purposes and narrowly permits the type of defensive actions a private entity may take."[40] Subsection 4(c) enables "a private entity to share with, or receive from, any other entity or the federal government a threat indicator or defensive measure . . . for cybersecurity purposes."[41]

Subsection 4(d) requires "an entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure . . . to protect against unauthorized access to or acquisition of such" information.[42] Subsection 4(d) also requires an entity (i) to "review information and to remove personal information not directly related to a cybersecurity threat" before sharing cybersecurity information, and (ii) "to implement and utilize technical capability to remove any personal information not directly related to a cybersecurity threat."[43]

Subsection 4(e) provides for an antitrust exemption, i.e., there is no antitrust violation "for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat . . . ."[44]

c. Section 5: Information Sharing

Section 5 establishes procedures for the government to "facilitate cybersecurity information sharing not later than 60 days after enactment of the bill."[45] Subsection 5(a) requires the federal government to "provide guidelines on the types of information that qualifies as a cybersecurity threat indicator and information protected under applicable privacy laws that are unlikely to be directly related to a cybersecurity threat."[46]

---

38 *Id.* § 4.
39 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.
40 *Id.*
41 *Id.*
42 S. 754 § 4(d)(1).
43 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.
44 S. 754 § 4(e)(1).
45 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.
46 *Id.*

Subsection 5(b) requires the federal government to provide "guidelines relating to privacy and civil liberties that shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with the cybersecurity activities."[47] Section 5(b) also requires the government "to periodically review the guidelines and content comprising cybersecurity information."[48]

Subsection 5(c) requires the Secretary of the Department of Homeland Security ("DHS") to "develop and implement a capability and process within DHS to accept cyber threat information through an automated system in real time."[49]

Subsection 5(d) clarifies "that information sharing will not constitute a waiver of any applicable privilege or protection," but rather, is voluntary, and "rights to proprietary information will not be infringed upon."[50] Specifically, subsection 5(d) does not allow the government "to use cyber information to investigate and prosecute 'serious violent felonies.'"[51]

d. Sections 6 Through 10

Section 6 protects a private entity from liability "for the monitoring of information systems or sharing or receipt of cyber threat indicators and defensive measures."[52]

Subsection 7(a) requires federal agencies to "submit information to various inspectors general in order to examine and oversee the implementation of cybersecurity information sharing, including content, effectiveness, and privacy and civil liberties."[53] Subsection 7(b) requires the Privacy and Civil Liberties Oversight Board to submit a report assessing the Act's effects and sufficiency to Congress and the President once every two years.[54]

Subsection 8(i) exempts entities from liability "for choosing not to engage in the voluntary activities" the act authorizes.[55] Subsection 8(k) provides for the bill's narrow construction and preemption of federal and state laws.[56]

---

47 *Id.*
48 *Id.*
49 *Id.*
50 *Id.*
51 *Id.*
52 *Id.*
53 *Id.*
54 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. § 7(b) (2015).
55 *Id.* § 8(i).
56 *Id.* § 8(k). For a discussion on preemption, see Eric Lindenfeld & Jasper L. Tran,

Section 9 requires the Director of National Intelligence to submit a report on cyberthreats to the Senate Select Committee on Intelligence and the House Permanent Select Committee.[57]

Section 10 eliminates a new exemption in the Freedom of Information Act created specifically for cyber information; thus, information shared through the bill could still qualify under existing FOIA exemptions.[58]

2. CISA's Cost

CISA needs about twenty people to "administer the program, prepare the required reports and manage the exchange of information."[59]

The Congressional Budget Office ("CBO") estimates CISA's cost at about "$20 million over the 2016-2020 period, assuming appropriation of the estimated amounts."[60] Also, the "aggregate costs of the mandates on public entities would [likely] fall below the threshold for intergovernmental mandates."[61]

The Obama administration did not take a public stance on CISA prior the passage of the CA'15.[62]

II. FROM THE HOUSE: THE PROTECTING CYBER NETWORKS ACT

A. PCNA's History

Meanwhile, the House responded to the escalating cybersecurity threats with its own version of a cybersecurity bill—the PCNA. Congressman Devin Nunes (R-CA), along with eight cosponsors, first introduced PCNA to the House on March 24, 2015, and the House passed PCNA by a 307–116 vote on April 22, 2015.[63]

Beyond Preemption of Generic Drug Claims, 45 SW. L. REV. 241, 244 (2015).

57 S. 754 § 9.

58 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.

59 *Congressional Budget Office Cost Estimate: S. 754 Cybersecurity Information Sharing Act of 2015,* CONG. BUDGET OFF. (Apr. 14, 2015), https://www.cbo.gov/sites/default/files/114th-congress-2015-2016/costestimate/s7540.pdf [http://perma.cc/F7P4-8J6X].

60 *Id.*

61 *Id.*

62 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15. However, the Obama administration has supported the House's companion bill, H.R. 1560 entitled "Protecting Cyber Networks Act," in an administration policy statement. *See* EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 1560 - PROTECTING CYBER NETWORKS ACT (Apr. 21, 2015), https://www.whitehouse.gov/sites/default/files/omb/ legislative/sap/114/saphr1560r_20150421.pdf [http://perma.cc/SZ74-JZS8] [hereinafter STATEMENT OF ADMINISTRATION: H.R. 1560]. *See generally infra* Section II.B.1.

63 Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015). The eight cosponsors are Adam B. Schiff (D-CA), Lynn A. Westmoreland (R-GA), James A. Himes

B. PCNA in Detail

Providing strong protections for privacy and civil liberties, PCNA essentially enables the private sector to voluntarily share cyberthreat indicators with each other and with the federal government, but not through the NSA or the DOD.[64] In discussing PCNA's provisions, I will also note similarities between the PCNA and CISA.

1. PCNA's Notable Provisions

PCNA's purpose is to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats. Section 1 sets out the short title of the bill as the "Protecting Cyber Networks Act," and includes a table of contents of the eleven following sections.[65] Sections 2 and 4 amend Title I of the National Security Act of 1947.[66]

a. Sections 2 Through 4

PCNA's section 2, like part of CISA's section 5,[67] discusses the sharing of cyberthreat indicators and defensive measures in real time by the DOD and NSA with the private sector, including declassifying the information and sharing at an unclassified level.[68] Particularly, the federal government must remove "personal information or information identifying a specific person that does not directly relate to a cyber threat."[69]

PCNA's section 3, like CISA's section 4,[70] discusses authorizations for "preventing, detecting, analyzing, and mitigating cybersecurity threats" of private and non-federal entities. Particularly, "[s]ubsection (a) does not authorize the Federal Government to conduct surveillance of any person."[71] Notably, subsection 3(b) does not authorize any defensive

---

(D-CT), Peter T. King (R-NY), Frank A. LoBiondo (R-NJ), Terri A. Sewell (D-AL), Mike Quigley (D-IL), and Patrick Murphy (D-FL). *H.R.1560 - Protecting Cyber Networks Act*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/1560/actions [http://perma.cc/TT7Q-58MA].

64 *See generally infra* Section II.B.1.

65 H.R. 1560.

66 *Id.* §§ 2(a), 4(a).

67 *See supra* Section I.B.1.

68 U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMM. ON INTELLIGENCE, THE PROTECTING CYBER NETWORKS ACT: SECTION-BY-SECTION ANALYSIS http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/new%20section%20by%20section%20pdf.pdf [http://perma.cc/TZ9P-DLQ8] [hereinafter HR1560 SECTION-BY-SECTION].

69 *Id.*

70 *See supra* Section I.B.1.

71 HR1560 SECTION-BY-SECTION, *supra* note 68.

measure that "destroys, renders unusable or inaccessible . . . or substantially harms" other networks, which includes "hacking back" or other forms of cyber activities that use computers or networks without their owner's consent.[72]

PCNA's section 4, like CISA's section 5,[73] discusses sharing of cyberthreat indicators and defensive measures with appropriate federal entities.[74] PCNA's subsection 4(b) requires the Attorney General to outline privacy and civil liberties guidelines.[75] Subsection 4(d) specifies the purposes the federal government may use a cyberthreat indicator received from non-federal entities:

> cybersecurity purpose; preventing or prosecuting a threat of death or seriously bodily harm or an offense arising out such a threat; preventing or prosecuting a serious threat to a minor, including sexual exploitation; or preventing or prosecuting espionage, economic espionage, serious violent felonies, and violations of the Computer Fraud and Abuse Act.[76]

b. Sections 5 Through 7

Section 5 establishes a private cause of action as the exclusive means for seeking a remedy for a violation of the Act by the federal government.[77] It provides for statutory damages, reasonable attorney fees, and a statute of limitations for the federal government's violation of the privacy and civil liberties guidelines under subsection 4(b).[78]

PCNA's section 6, like part of CISA's section 6,[79] protect a private entity from causes of action for the monitoring of an information system or sharing of cyberthreat indicators or defensive measures.[80] Notably, section 6 defines "willful misconduct" as "an act or omission that is taken (A) intentionally to achieve a wrongful purpose; (B) knowingly without legal or factual justification and; (C) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit," and establishes the standard to prove willful misconduct.[81]

---

72 *Id.*
73 *See supra* Section I.B.1.
74 HR1560 SECTION-BY-SECTION, *supra* note 68.
75 *Id.*
76 *Id.*
77 *Id.*
78 *Id.*
79 *See supra* Section I.B.1.
80 HR1560 SECTION-BY-SECTION, *supra* note 68.
81 Protecting Cyber Networks Act, H.R. 1560, 114th Cong. § 6(c) (2015).

PCNA's section 7, like CISA's section 7, requires submission of reports for oversight of government activities.[82]

c. Sections 8 Through 11

PCNA's section 8, like CISA's section 9,[83] requires the Director of National Intelligence, in consultation with the Intelligence Community, "to submit a report to congressional intelligence committees on cybersecurity threats."[84]

Section 9 contains various construction and preemption provisions to make clear that, essentially, PCNA does not authorize the government to target a person for surveillance.[85] Section 9 also does not "limit or modify any existing information-sharing relationships outside of [PCNA] or prohibit any new information-sharing relationships outside of [PCNA]."[86]

Section 10 amends the United States Code, 5 U.S.C. § 552(b) and 10 U.S.C. § 2224.[87]

PCNA's section 11, like CISA's section 2,[88] narrowly defines various terms: agency, appropriate federal entities, cybersecurity purpose, cyberthreat, cyberthreat indicator, defensive measure, federal entity, information system, local government, malicious cyber command and control, malicious reconnaissance, monitor, non-federal entity, private entity, real time and real-time, security control, security vulnerability, and tribal.[89]

PCNA's section 11(4) defines "cybersecurity threat" as:

> an action, not protected by the first amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, confidentiality, integrity, or availability of an information system or information that is stored on, processed by, or transiting an information system[,] . . . [excluding] any action that solely involves a violation of a consumer term of service or a consumer licensing agreement."[90]

---

82 H.R. 1560 § 7; *see also supra* Section I.B.1.
83 *See supra* Section I.B.1.
84 HR1560 SECTION-BY-SECTION, *supra* note 68.
85 *Id.*
86 *Id.*
87 H.R. 1560 § 10; HR1560 SECTION-BY-SECTION, *supra* note 68.
88 *See supra* Section I.B.1.
89 H.R. 1560 § 11; HR1560 SECTION-BY-SECTION, *supra* note 68.
90 H.R. 1560 § 11(4).

2. PCNA's Cost

The CBO estimates PCNA's implementation cost at "$186 million over the 2016-2020 period, assuming appropriation of the estimated amounts."[91]

Although the Obama administration publicly supported PCNA,[92] out of the gate, both bills, especially S. 754, faced opposition from many organizations on the grounds of violating privacy and civil rights.[93] Names like "cyber-surveillance" were tossed around.[94]

III. FROM THE PRESIDENT: THE "VOLUNTARY" FRAMEWORK FOLLOWING EXECUTIVE ORDER 13636

As Congress considered legislation, the President in February 2013 issued Executive Order 13636, entitled "Improving Critical Infrastructure Cybersecurity," directing the NIST to develop a "voluntary" framework for reducing cyber risks to critical infrastructure.[95] Accordingly, the NIST released a framework in February 2014,[96] sharing many similar provisions of CISA and PCNA on information sharing.[97] Before the passage of CA'15, Executive Order 13636 was the only serious action taken by the government to strengthen U.S. cybersecurity, but the NIST Framework is voluntary in nature, encouraging—rather than requiring—action on the private sector's part.

"The private sector faces a rapidly shifting terrain without clear standards."[98] Following the Federal Trade Commission's

---

91 *H.R. 1560, Protecting Cyber Networks Act*, CONG. BUDGET OFF. (Apr. 13, 2015), https://www.cbo.gov/publication/50110 [http://perma.cc/6XB8-KNL3]. The CBO also addresses the small and potentially insignificant amount of "criminal prosecutions, which could increase federal revenues from fines as well as direct spending from the Crime Victims Fund," and the possibility of the government's liability "if an agency or department were to violate the privacy and civil liberty guidelines required by the bill." *Id.*

92 *See* STATEMENT OF ADMINISTRATION: H.R. 1560, *supra* note 62.

93 *See, e.g.*, *Consumer Advocates Letter to Senate on Cybersecurity Information Sharing Act*, CTR. FOR DEMOCRACY & TECH. (Oct. 21, 2015), https://cdt.org/insight/consumer-advocates-letter-to-senate-on-cybersecurity-information-sharing-act/ [http://perma.cc/SL4L-434Q].

94 *See, e.g.*, Robyn Greene, *Cybersecurity Information Sharing Act of 2015 Is Cyber-Surveillance, Not Cybersecurity*, NEW AM.: OPEN TECH. INST. (Apr. 9, 2015), https://www.newamerica.org/oti/cybersecurity-information-sharing-act-of-2015-is-cyber-surveillance-not-cybersecurity/ [http://perma.cc/3JZW-VGWM].

95 *Executive Order 13636: Cybersecurity Framework*, *supra* note 9.

96 *See id.*

97 *See generally* WHITE HOUSE'S *Executive Order*, *supra* note 8.

98 *Cybersecurity: Private Sector Faces Increasing Regulatory Risk from Agency Enforcement and Informal "Guidance" Becoming Standard of Care*, FEDERALIST SOC'Y (Oct. 15, 2015), http://www.fed-soc.org/events/detail/cybersecurity-private-sector-faces-increasing-regulatory-risk-from-agency-enforcement-and-informal-guidance-becoming-standard-of-care [http://perma.cc/TZE2-E43J] [hereinafter FEDERALIST SOC'Y].

("FTC") recent win in *FTC v. Wyndham*,[99] regulatory agencies are expanding "oversight through informal guidance and threat of enforcement."[100]

In October 2015, the Federalist Society and partners from the private sector met to discuss current cybersecurity trends and what the private sector faces in 2015 and 2016, as well as the following questions:

> Will the President's Executive Order, and the NIST Cybersecurity Framework, become the de facto standard for the private sector? Is the federal government regulating through the threat of enforcement by [the] FTC, FCC, and other federal agencies, instead of through more regular administrative processes? What should companies make of emerging agency "guidance" from agencies like the FDA, SEC, [the National Highway Traffic Safety Administration], and DoD, on operations and innovation in areas like the Internet of Things, mobile applications and devices, cloud services, [and] connected cars?[101]

IV. THE CURRENT LAW OF THE LAND: THE CYBERSECURITY ACT OF 2015

On December 18, 2015, President Obama signed into law the Cybersecurity Act of 2015 as part of the Omnibus Appropriations Act.[102] CA'15 contains the majority of CISA's provisions, but with three notable exceptions: (1) network operators have monitoring privileges; (2) network operators can operate defensive measures; and (3) network operators can share cyberthreat information with others.[103]

---

99 F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (affirming the district court's decision upholding the FTC's data protection authority).

100 FEDERALIST SOC'Y, *supra* note 98.

101 *Id.*

102 Everett Rosenfeld, *The Controversial 'Surveillance' Act Obama Just Signed*, CNBC (Dec. 22, 2015, 12:34 PM), http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html [http://perma.cc/C4Z4-VYWJ].

103 Orin Kerr provided some context for the provider exception, stating:

> The statutory surveillance laws . . . generally prohibit Internet surveillance subject to certain exceptions. Each of the laws has what is known as the provider exception. The provider exception allows telecommunications providers to conduct surveillance on their networks, and if necessary to disclose user communications, when it is 'a necessary incident . . . to the protection of the rights or property of the provider of that service.'

Orin Kerr, *How Does the Cybersecurity Act of 2015 Change the Internet Surveillance Laws?*, WASH. POST: THE VOLOKH CONSPIRACY (Dec. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/ [http://perma.cc/6UXK-UD6E].

The exceptions in CA'15 contain the following definitions:

(1) "monitor" is defined as "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system";[104]

(2) "defensive measure" is defined as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability," but does not include "a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system";[105] and

(3) "cyber threat indicator" is defined as "information that is necessary to describe or identify" the following item(s) or any combination thereof: malicious reconnaissance; malicious cyber command and control; a security vulnerability; a method of defeating a security control; a method of causing a user to enable the defeat of a security control; the actual or potential harm caused by an incident; or any other attribute of a cybersecurity threat.[106]

Orin Kerr has noted that CA'15:

> [S]ubstantially broadens the powers of network operators to monitor and disclose beyond the existing provider exception and trespasser exception. The new language focuses mostly on the purpose of the monitoring and disclosure, with relatively little in place about the scope of monitoring or disclosure (although there is a requirement of scrubbing personal data if known). And it seems to allow monitoring for cybersecurity purposes generally, including outsourcing of that role to others, instead of limiting the exception to monitoring to protect the provider's own network.[107]

Specifically, exception (1) contains unclear language that can be "broadly" interpreted; exception (2) is "largely a retread of the existing provider exception"; and exception (3) "expands on the provider exception because the disclosure does not need to be for the protection of the operator's own network."[108]

---

104 Cybersecurity Act of 2015, Pub. L. No. 114-113, § 102(13), 129 Stat. 2242, 2938. Information system is defined elsewhere as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." 44 U.S.C. § 3502(8) (2012).

105 § 102(7), 129 Stat. at 2937.

106 § 102(6), 129 Stat. at 2937; *see also* § 102(11), 129 Stat. at 2938.

107 Kerr, *supra* note 103.

108 *Id.*

On the other hand, Jennifer Granick has noted that the language in CA'15 could trump forthcoming federal regulatory efforts as well as state privacy laws.[109]

V. CONCERNS, ETHICAL IMPLICATIONS, AND RECOMMENDATIONS

The NIST Framework following Executive Order 13636 was already in place when CA'15 was signed into law. Given that the Obama administration publicly supported H.R. 1560,[110] it was foreseeable that CA'15 would be signed by President Obama to become the law of the land. CA'15 might be as good as it can get with bipartisan and presidential approval—the best Congress can do with the ongoing political gridlock.

I have several initial concerns. First, sharing information does little to prevent successful cyberattacks, given that there have been many already in place. For instance, in 2003, DHS established its U.S. Computer Emergency Readiness Team to collect and analyze data, but its results have been unclear. Second, the process of sharing information with the government and other private entities creates a new opportunity for more hacking and information being stolen. Third, CA'15—and its parent CISA—is still a surveillance bill that could use shared information to spy on U.S. citizens. Fourth, CA'15 has not solved the problem of incentivizing attorneys to disclose their clients' information. Lastly, CA'15 will very likely face constitutional challenges in courts; the battle of right to privacy in the realm of cybersecurity is far from over.[111]

Instead of expanding the provider exception in CA'15,[112] the government should focus its efforts on tackling the lack of incentive problem. New cybersecurity bills or acts are still focused on information sharing, which the NIST Framework from Executive Order 13636 was supposed to accomplish already.

Going forward, I leave with four ethical implications and recommendations for practicing attorneys. First, attorneys and corporations should carefully consider the manner in which an attorney shares client information. Attorneys can share IT

---

109 Jennifer Granick, *OmniCISA Pits DHS Against the FCC and FTC on User Privacy*, JUST SECURITY (Dec. 16, 2015, 6:09 PM), https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy/ [http://perma.cc/A3MF-CXG5].

110 *See* STATEMENT OF ADMINISTRATION: H.R. 1560, *supra* note 62.

111 At the 2016 *Chapman Law Review* Symposium, Denis Binder agreed and commented that there "will definitely be constitutional challenges" to CA'15. For a discussion on the right to privacy, see generally Jasper L. Tran, *The Right to Attention*, 91 IND. L.J. (forthcoming 2016).

112 *See generally supra* Part IV and note 103.

information, such as the manner of a cyberattack, without revealing too much confidential information, such as the content of the attack. How to share such information matters as well; it is better for an attorney to pick up the phone and call when communicating—leaving no paper trail behind.

Second, an attorney sharing cybersecurity information with a party who is not that attorney's client—including the federal government or others in the private sector—could result in a waiver of attorney-client privilege[113] and/or a violation of that attorney's duty of confidentiality.[114] An attorney must guard the privilege, as well as comply with this confidentiality duty.[115] Even inadvertent disclosure of a client's confidential information could waive this privilege. Attorneys want to keep their clients happy, and losing this privilege would not make anyone happy. Even if confidentiality concerns are resolved, the attorney still needs to ensure there are no conflicts of interest involved, which is difficult when there are too many people "in the loop."

Third, there is a lack of incentive for the attorney to disclose his/her client's confidential or sensitive information. There is an industry norm of keeping the information of an attorney's client private. No attorney wants to deviate from the industry norm; the client might mistrust that attorney and replace them with some other attorney whom the client can trust. As noted above, the current CA'15 has not solved this lack of incentive problem.

Fourth, the public announcement of a client's confidential or sensitive cybersecurity information could hurt the current client's business, and even result in an attorney losing future clients. This is often due to how much loss a client has suffered from a recent attack, or because a client was targeted for an attack in the first place—scaring that client's current and potential customers. No attorney wants a reputation for leaking a client's information.

In light of the above recommendations, attorneys can still share information when appropriate—exercising their best judgment.

---

113 *See, e.g.*, FED. R. EVID. 502 ("'[A]ttorney-client privilege' means the protection that applicable law provides for confidential attorney-client communication.").

114 *See, e.g.*, PAUL R. RICE ET AL., ATTORNEY-CLIENT PRIVILEGE IN THE U.S. § 2.1 (2015–2016 ed. 2015) ("The attorney-client privilege is a rule of evidence, with an importance long recognized. It protects the confidentiality of communications between an attorney and client.").

115 *See, e.g.*, MODEL RULES OF PROF'L CONDUCT r. 1.6 (AM. BAR ASS'N 2014).

CONCLUSION

This Article summarizes the legislative history, notable provisions, and current status of CISA, PCNA, Executive Order 13636, and CA'15. The Article ended with four ethical implications and recommendations. And the most important take-away is: when in doubt, attorneys should not share.

Legal Ethics' Next Frontier: Lawyers and Cybersecurity

*Eli Wald**

The publication of the Panama Papers containing confidential client information, following a cybersecurity breach at the law firm of Mossack Fonseca, demonstrated what many have long known, that law firms are particularly vulnerable to cyberattacks.[1] Yet since concerns about law firms' cyber practices have first surfaced, the legal profession has learned a lot about cybersecurity. We know who is perpetrating cyberattacks against lawyers, we know why they are doing it, and we even know quite a bit about how to prevent and defend against attacks, as well as how to mitigate their damage and respond when an attack takes place. Still, there are quite a few things we do not know. Most importantly, we do not know the extent and scope of cyberattacks against law firms, and we do not know whether lawyers are acting on the growing body of cybersecurity knowledge they possess to reasonably protect their clients' information from unauthorized access. Indeed, we have reason to believe that some

* Charles W. Delaney Jr. Professor of Law, University of Denver Sturm College of Law. I thank Denis Binder, Tanya Forsheit, Scott Garner, Marty Katz, Ron Rotunda, Drew Simshaw, and other participants in the "Cyber Wars: Navigating Responsibilities for the Public and Private Sector" Symposium at Chapman University Dale E. Fowler School of Law for their helpful comments. I also thank Diane Burkhardt, Faculty Services Liaison at the Westminster Law Library at the University of Denver Sturm College of Law, for her outstanding research assistance.

1 On the Panama Papers, see Luke Harding, *What Are the Panama Papers? A Guide to History's Biggest Data Leak*, GUARDIAN (Apr. 5, 2016), http://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers [http://perma.cc/PG79-Z7HM]; David Z. Morris, *The Laughably Bad Security at 'Panama Papers' firm Mossack Fonseca*, FORTUNE (Apr. 9, 2016), http://fortune.com/2016/04/09/bad-security-panama-papers/ [http://perma.cc/453A-ZXZB]. The Federal Bureau of Investigation publicly identified law firms as vulnerable in 2009, see Susan Hansen, *Cyber Attacks Upend Attorney-Client Privilege*, BLOOMBERG (Mar. 19, 2015, 11:56 AM), http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security [http://perma.cc/8LSR-5UEQ]. The FBI reiterated its caution in 2011, calling on major law firms to raise their level of awareness regarding cyberattacks. *See* Anne Marie Davine, *More Cyber Preparedness Needed, According to 2014 Law Firm Cyber Survey*, MARSH (Jan. 15, 2015), https://www.marsh.com/us/insights/more-cyber-preparedness-needed-2014-law-firm-cyber-survey.html [http://perma.cc/5SFK-TTQ9]. FBI officials and security experts maintain that law firms remain a weak link when it comes to online security. *Id.*

lawyers, notwithstanding their awareness of cybersecurity threats, fail to take reasonable steps to protect themselves and their clients, because they are underregulated, likely to escape any meaningful consequences for their inaction, and therefore, have little incentive to take reasonable cybersecurity action.

Lawyers' cybersecurity conduct is underregulated because the usual regulatory suspects, liability rules and market controls, do not rigorously apply. Since proving cybersecurity damages is often hard to do, lawyers do not systematically face the prospect of malpractice liability for failing to adequately protect clients' information. Since lawyers are generally under no duty to report cyberattacks to their clients or to others, they do not face market sanctions, such as being fired or suffering reputational losses. Of course, some lawyers have been at the forefront of practicing diligent cybersecurity. Yet, because practicing cybersecurity is expensive and the technological learning curve for lawyers is steep, in the face of underregulation and few practical consequences for inaction, some lawyers may fail to reasonably defend against cyberthreats, the known risks notwithstanding.[2] Moreover, because malpractice lawsuits are scarce, there is little in the way of judicial exposition of the meaning of *reasonable* cybersecurity practices, leaving even those lawyers who are committed to practicing reasonable cybersecurity in the dark.

This Article argues that the underregulation of lawyers' cybersecurity conduct may be addressed by the promulgation of robust rules of professional conduct, delineating the meaning of reasonable cybersecurity protections and mandating greater disclosure of unauthorized access to clients. Effective rules of professional conduct are likely to incentivize lawyers to take action for three related reasons. First, the threat of discipline will motivate some lawyers to take reasonable cybersecurity action and advise clients when attacks result in compromised information. Second, a mandatory disclosure duty will in turn enable more effective market regulation as clients will be able to sanction lawyers for inaction. Third, the promulgation of effective cybersecurity rules may result in peer pressure and the development of reasonable cybersecurity social norms among lawyers.

Part I of the Article summarizes the knowledge lawyers have recently gained about cybersecurity, namely, who is attacking them, why, and what can be done to defend against cyberattacks.

---

2 James R. Silkenat, *Privacy and Data Security for Lawyers*, 38 AM. J. TRIAL ADVOC. 449, 454 (2015) ("[B]ut in the case of cybersecurity, attorneys sometimes take a more 'do as I say, not as I do' approach.").

Part II examines the underregulation of lawyers' cybersecurity conduct and its consequences. Part III advances a proposal for a regulatory response, in the form of new and revised rules of professional conduct.

I. THE STATE OF LAWYERS' CYBERSECURITY KNOWLEDGE

The use of technology is pervasive in the practice of law. Like many other professions, lawyers e-mail, store information remotely, share files, and use mobile devices and wireless networks; their "widespread use of electronic records and mobile devices" presents "unprecedented challenges."[3] As *The ABA Cybersecurity Handbook* explains, "[c]reating, using, communicating, and storing information in electronic form greatly increases the potential for unauthorized access, use, disclosure, and alteration, as well as the risk of loss or destruction."[4] Lawyers must understand and respond to these risks in order to protect confidential client information, which if compromised, can expose clients to the loss of the attorney-client privilege, fraud, negative publicity and tarnished business reputations, liability to others, and even bankruptcy.[5]

Over the last few years, however, the legal profession has learned a great deal about cybersecurity. Lawyers now know why they have become likely targets for hackers, who is perpetrating the attacks, and what they can do to minimize the probability and severity of attacks before they take place, as well as respond to attacks when they happen. This part briefly summarizes the growing wealth of information about cybersecurity.

A. Why Lawyers Are Under (Cyber) Attack

Lawyers experience cyberattacks for three related reasons: they store valuable confidential client information, they are likely to be more vulnerable than their clients, and they are under increased pressure to take advantage of technologies that render them susceptible to attacks. To begin with, cybersecurity is traditionally concerned with protecting confidential information,

---

3 ABA CYBERSECURITY LEGAL TASK FORCE & SECTION OF SCIENCE & TECHNOLOGY LAW, REPORT TO THE HOUSE OF DELEGATES: RESOLUTION 109, ABA 4 (Aug. 2014) [hereinafter ABA CYBERSECURITY RESOLUTION], http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions/2014_hod_annual_meeting_109.authcheckdam.pdf [http://perma.cc/NS7C-JXS7].

4 JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 41 (2013). *See generally* MARC GOODMAN, FUTURE CRIMES – EVERYTHING IS CONNECTED, EVERYONE IS VULNERABLE, AND WHAT WE CAN DO ABOUT IT (2015).

5 Drew T. Simshaw, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data*, 38 AM. J. TRIAL ADVOC. 549, 550, 554 (2015).

maintaining the integrity of information, and ensuring the availability of stored information.[6] Protecting confidential information is especially important to the legal profession, as all lawyers and law firms are depositories of valuable confidential information related to the representation of clients. As the American Bar Association Model Rules of Professional Conduct ("Rules") explain, protecting confidential information is a "fundamental principle" that "contributes to the trust that is the hallmark of the client-lawyer relationship."[7] Confidentiality encourages clients "to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively."[8] Put differently, to effectively represent clients, lawyers routinely collect and store valuable client information. Because lawyers receive and store valuable confidential information pertaining to their clients' matters, they are likely targets for hackers.

Context always matters in the practice of law,[9] and it is essential to gaining an understanding of the cybersecurity practices of lawyers. Different types of law firms offer different types of potential value to hackers in terms of the confidential client information they store. For example, hacking large law firms, which tend to represent large entity clients,[10] is often more

---

6 David G. Delaney, *Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation*, 40 J. LEGIS. 251, 251 (2014) ("At its core, cybersecurity involves information security or assurance—preserving the confidentiality, availability, and integrity of information."). The core objectives of confidentiality, availability, and integrity of information inform cybersecurity legislation. For example, under the Health Insurance Portability and Accountability Act, covered entities "must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected." *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8334 (Feb. 20, 2003). Similarly, the National Institute of Standards and Technology ("NIST"), a Department of Commerce non-regulatory agency, "provide[s] standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services." *See Computer Security Resource Center*, NIST, http://www.nist.gov/itl/csd/csrc.cfm [http://perma.cc/K7RV-XMPR] (last updated Oct. 5, 2010).

7 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 2 (AM. BAR ASS'N 2013).

8 *Id.*

9 Eli Wald, *Resizing the Rules of Professional Conduct*, 27 GEO. J. LEGAL ETHICS 227, 235–44 (2014); David B. Wilkins, *Legal Realism for Lawyers*, 104 HARV. L. REV. 468, 473, 476, 515–19 (1990); David B. Wilkins, *Who Should Regulate Lawyers?*, 105 HARV. L. REV. 799, 814–19 (1992). *See generally* David B. Wilkins, *Making Context Count: Regulating Lawyers After Kaye, Scholer*, 66 S. CAL. L. REV. 1145 (1993).

10 *See* JOHN P. HEINZ & EDWARD O. LAUMANN, CHICAGO LAWYERS: THE SOCIAL STRUCTURE OF THE BAR 319–20 (1982) (finding that the legal profession consists of two categories of lawyers whose practice settings, socioeconomic and ethno-religious backgrounds, education, and clientele differ considerably); JOHN P. HEINZ ET AL., URBAN LAWYERS: THE NEW SOCIAL STRUCTURE OF THE BAR 29–47 (2005) (documenting that lawyers work in two fairly distinct hemispheres—individual and corporate—and that

efficient than hacking each of the law firms' large entity clients individually.[11] Large entity clients tend to store enormous quantities of information, though much of it may be of relatively little value to hackers, even if they had the resources to comb through it following a successful attack. For hackers, large law firms are a one-stop shop,[12] serving as filters of low value material,[13] because BigLaw will tend to receive from its clients and store only a subset of their vast information, namely, the valuable portion of it. Thus, while one might expect large law firms to be relatively well-protected, at least compared to smaller law firms, the payoff for hackers may be worth the investment.

Yet, this is not to suggest that small law firms and solo practitioners who tend to represent small businesses and individual clients[14] are not valuable depositories of client information. Rather, these lawyers may simply feature a different value proposition for hackers. For example, some of their clients may not ordinarily store sensitive information electronically and, thus, may be immune to cyberattacks. Yet, in the context of negotiating a transaction or bringing or defending a lawsuit, such clients are likely to collect information and then send it to their lawyers, who are likely to store it electronically, thus making the latter likely targets for cyberattacks.

Second, compared with their clients, lawyers are assumed to be relatively easy, vulnerable targets for cyberattacks,[15] "perceived to have fewer security resources than their clients,[16] and have less of an understanding of and appreciation for cyber risk."[17] Lawyers' relative cyber vulnerability exposes them not only to attacks seeking confidential client information, but also to hacking designed to disrupt the integrity and availability of information stored by law firms in an attempt to collect ransom payments.[18]

---

mobility between these hemispheres is relatively limited).

11 Simshaw, *supra* note 5, at 550.

12 Michael McNerney & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, 62 AM. U. L. REV. 1243, 1246, 1251 (2013).

13 Alan W. Ezekiel, Note, *Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft*, 26 HARV. J.L. & TECH. 649, 651 (2013).

14 *See supra* note 10.

15 JANE LECLAIRE & GREGORY KEELEY, CYBERSECURITY IN OUR DIGITAL LIVES 128 (2015).

16 Simshaw, *supra* note 5, at 550–51.

17 LECLAIRE & KEELEY, *supra* note 15, at 128 (2015); RHODES & POLLEY, *supra* note 4, at 105 ("Law firms are viewed as a 'very target-rich environment' with significantly less cybersecurity protection in place than their clients have.").

18 *See, e.g.*, Joe Dysart, *'Ransomware' Software Attacks Stymie Law Firms*, A.B.A. J. (June 1, 2015, 2:30 AM), http://www.abajournal.com/magazine/article/ransomware_software_attacks_stymie_law_firms [http://perma.cc/M62F-8RT4].

Once again, attention to context is paramount to the understanding of cyberthreats; whereas lawyers representing large entity clients are likely to be less sophisticated than their clients about cyber risks and have fewer resources and expertise to deal with threats, they nonetheless represent clients who know enough to insist that their law firms take reasonable cybersecurity measures. Lawyers representing small businesses and individuals may know as little as their clients about cyberthreats, but that is no measure of comfort. Not only do such lawyers collect and store their clients' information electronically, exposing it to cyber risk, but they, too, are likely easier targets than their clients who have more to lose and, therefore, a stronger incentive to protect their sensitive information. Worse, small businesses and individuals may erroneously assume that lawyers know enough, or at least more than them about cybersecurity and that their information will be secure with their attorneys. Therefore, they insufficiently inquire and supervise their lawyers' cyber practices.

Finally, the increased competitiveness and ongoing restructuring in the legal profession, both accelerated since the Great Recession, tend to make lawyers especially vulnerable to cyberattacks. Increased competitiveness in the market for legal services has led to the emergence of a dominant "around-the-clock, 24-7" culture of availability to clients.[19] Of course, enhanced lawyer availability is often desirable from the clients' point of view, but when accomplished through mobile remote technology, it enhances cybersecurity risks.[20] Similarly, as competitive pressures lead lawyers to resort to greater use of outsourcing and artificial intelligence,[21] the benefits to clients entail an increased risk of cyberattacks.

B. Who Is Attacking the Legal Profession?

All lawyers are susceptible to attacks by malicious insiders,[22] such as disgruntled current and former lawyers and staff members, yet context matters in identifying likely hackers. Large law firms representing large entity clients involved in large-scale

---

19 Eli Wald, *Glass-Ceilings and Dead Ends: Professional Ideologies, Gender Stereotypes and the Future of Women Lawyers at Large Law Firms*, 78 FORDHAM L. REV. 2245, 2264–73 (2010).

20 McNerney & Papadopoulos, *supra* note 12, at 1251.

21 *See, e.g.*, Milton C. Regan, Jr. & Palmer T. Heenan, *Supply Chains and Porous Boundaries: The Disaggregation of Legal Services*, 78 FORDHAM L. REV. 2137 (2010); John O. McGinnis & Russell G. Pearce, *The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services*, 82 FORDHAM L. REV. 3041 (2014).

22 Simshaw, *supra* note 5, at 552.

transactional work are more likely to be targeted by social engineers, including state-sponsored hackers,[23] and subject to corporate espionage and financial crimes.[24] Smaller law firms, however, while less likely to be attacked by state-sponsored actors, still carry valuable information attractive to social engineers.[25] Government intrusion and surveillance, a growing source of cybersecurity concern for lawyers and their clients alike,[26] may be of particular concern to criminal defense, immigration, and intellectual property lawyers.[27]

C. What Lawyers Can Do About Cyberattacks

Stopping all cyberattacks is impossible to do. Yet, 96% of hacking attacks employ simple techniques, and 97% of attacks can be blocked by common security practices that are within the reach of even small law firms and solo practitioners.[28] These common practices include using current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents, avoiding the use of web-based e-mail services and public Wi-Fi, replacing the default passwords on network hardware, and training employees to recognize deceptive ("phishing") attacks.[29] Beyond these basic measures, defending effectively against cyberattacks entails making decisions about trade-offs between business needs and

---

23 *Id.*

24 McNerney & Papadopoulos, *supra* note 12, at 1264.

25 Carrie A. Goldberg, *Rebooting the Small Law Practice: A Call for Increased Cybersecurity in the Age of Hacks and Digital Attacks*, 38 AM. J. TRIAL ADVOC. 519, 521–22 (2015); *see also* Noah G. Susskind, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573, 579 (2015) (exploring the vulnerability of smaller companies).

26 Silkenat, *supra* note 2, at 456; *see also* Sarah Jane Hughes, *Did the National Security Agency Destroy the Prospects for Confidentiality and Privilege When Lawyers Store Clients' Files in the Cloud – and What, If Anything, Can Lawyers and Law Firms Realistically Do in Response?*, 41 N. KY. L. REV. 405, 418 (2014).

27 *See, e.g.*, Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES at A1 (Mar. 29, 2016), http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0 [http://perma.cc/4SPB-R96Q]; Devlin Barrett, *Justice Department Seeks to Force Apple to Extract Data from About 12 Other iPhones*, WALL ST. J. (Feb. 23, 2016), http://www.wsj.com/article_email/justice-department-seeks-to-force-apple-to-extract-data-from-about-12-other-iphones-1456202213-lMyQjAxMTI2MjIzMzMyMTMwWj.

28 VERIZON ET AL., 2012 DATA BREACH INVESTIGATIONS REPORT (2012), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf [http://perma.cc/GTA4-3DN3].

29 Ezekiel, *supra* note 13, at 649; *see also* JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 239–44 (2011).

cybersecurity.[30] For example, is a firm willing to make it more inconvenient for traveling attorneys or lawyers working remotely to access their data, in exchange for more security? When does a business imperative of providing speedy service render certain actions "worth the risk"?[31] Navigating these trade-offs and systematically assessing the cyber risks involved in doing business requires developing and putting in place a comprehensive cybersecurity plan.

The first element of a comprehensive cybersecurity plan entails involving firm leadership in learning about cybersecurity threats and making strategic decisions about them.[32] This, to be sure, does not mean that firm executives need to (or can) become cybersecurity experts. It does, however, mean that firm leaders, ranging from members of large law firms' executive committees to solo practitioners managing their own practices, must understand basic cybersecurity realities to allow them to make informed strategic judgments about: what technologies to deploy; how to mine advantages to benefit clients and the practice, and at what costs and risk level; and what security measures to employ. Because putting together a cybersecurity plan calls for strategic decision making that must involve firm management, law firms would be well-advised to task a management-level leader with specific supervisory responsibility for cybersecurity planning.

Second, lawyers must know their data—that is, be cognizant of the actual information the firm possesses and, in particular, be mindful of highly valuable and sensitive information entrusted to firm lawyers, encompassing issues such as what information firm lawyers are working with and how they are using it. Once strategic decisions are made by management, many law firms will likely delegate the implementation of cybersecurity details to non-lawyers, yet lawyer insight and exercise of judgment regarding the nature of client information and its sensitivity must inform the design of cybersecurity plans. For example, a cybersecurity plan may include different levels of protection depending on the circumstances. While a firm may prohibit all

---

30 McNerney & Papadopoulos, *supra* note 12, at 1265.

31 *Id.* at 1265–66.

32 For example, "should the firm be more worried about an attack that disrupts its networks so that attorneys lose access to information, about an attack that reveals sensitive data belonging to clients, or about an attack, that exposes the firm's own secret business data?" Or, "[w]ho are the actors that might pursue each of these attacks? What can the company do to prevent each type of attack or, if the attack happens, to manage its consequences?" *Id.* at 1265; *see also* Cheryl A. Falvey, *Demonstrating Due Diligence in Building an Information Security Program*, *in* PRIVACY AND SURVEILLANCE LEGAL ISSUES 7 (2014).

lawyers from using public cloud providers, file-sharing services for sharing documents, web-based e-mail services, and public Wi-Fi while conducting firm business, it may demand using cryptographically strong passwords only when receiving or sending highly sensitive client information. A firm may delegate the creation and maintenance of its cybersecurity plan to non-lawyers and may create guidelines for the use of various protections, but ultimately, lawyers would have to be educated to make judgment calls about what measures to use based on their knowledge of their clients' information.

Third, following a strategic, management-level risk analysis of the trade-offs between cybersecurity and business imperatives applied to the actual data a firm possesses, lawyers can then delegate day-to-day operations and implementation authority to technology experts, either within or outside the firm. A large law firm may designate someone internally within its IT department for the task, whereas a solo practitioner or a small firm may hire an outside expert to help manage its security apparatus. Day-to-day implementation of a cybersecurity plan includes two related yet distinct tasks: prevention and breach management. Prevention includes responsibility for deploying secure technologies, restricting access to high-risk activities, and implementing cybersecurity policies and procedures. For example, "blocking malware, [and] detecting anomalous behavior, such as extraction of significant quantities of data off company networks, that can indicate a cyberattack."[33] Perhaps most importantly, it entails training of lawyers and staff to observe cybersecurity practices.[34] The *Wall Street Journal* reported that "the weakest links at law firms of any size are often their own employees, including lawyers."[35] Having a plan in the event of a data breach, in turn, includes containing an ongoing cyberattack, mitigating its damage, and communicating it to clients.[36]

While lawyers in general may delegate to cybersecurity experts the implementation of cybersecurity plans, complex legal ethics questions may arise requiring the insight, approval, and supervision of lawyers. For example, consider the use of honeypots, cybersecurity mechanisms set to detect, deflect, and counteract attempts at unauthorized access to protected

---

33 McNerney & Papadopoulos, *supra* note 12, at 1268.

34 Simshaw, *supra* note 5, at 568–69.

35 Jennifer Smith, *Lawyers Get Vigilant on Cybersecurity*, WALL ST. J. (June 26, 2012, 4:09 PM), http://www.wsj.com/articles/SB10001424052702304458604577486761101726748.

36 *See* Mercedes Kelley Tunstall, *The Path to Comprehensive Cybersecurity Laws in the United States*, *in* UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW 61, 63 (2015 ed. 2015).

information. Generally, honeypots consist of data that appears to be legitimate and thus of value to attackers, but is in fact deceptive information planted to attract hackers who are then tracked and blocked.[37] Among cyber experts, while risky, honeypots are considered a valid information security tactic.[38] Yet, whether law firms can deploy honeypots raises a complicated and unresolved question under the Rules, which generally prohibit lawyers from engaging in dishonest or deceptive practices in the practice of law.[39] Notably, it is a question lawyers need to be made aware of and help resolve.

Finally, law firms must develop a strong culture of cybersecurity,[40] because cyber "compliance and risk management intertwine around corporate culture."[41] Lawyers and staff who think of cybersecurity as somebody else's problem or responsibility are prone to make the very mistakes, like opening phishing e-mails, that expose a firm to heightened risk. Since a law firm's cybersecurity apparatus is only as safe as its weakest link, lawyers and staff must be trained to conceive of cybersecurity not as an imposition on doing business, but as an integral part of firm culture—that is, to move past thinking of business considerations and cybersecurity as a trade-off and accept cybersecurity as a business need.[42]

Context is likely to play an important role in the implementation of cybersecurity plans. Some security measures, indeed, even some basic security measures such as avoiding the use of web-based e-mail services and public Wi-Fi, as well as expensive training, may be out of reach for some solo practitioners and smaller law firms. Yet, as Carrie Goldberg points out, it is in these very types of attorney-client relationships that an attorney is likely to be "more stringent and informed than the client about necessary information security measures."[43] In such instances, a lawyer can enhance the cybersecurity of the attorney-client relationship by explaining to the client the lawyer's limited means and the risks entailed, and communicating the shared responsibility to maintain privacy,

---

37 *See* Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?* 20 RICH. J.L. & TECH. 12, 14–16 (2014).

38 *Id.* at 15.

39 MODEL RULES OF PROF'L CONDUCT r. 8.4(c) (AM. BAR ASS'N 2013); *see, e.g.*, *In re* Pautler, 47 P.3d 1175 (Colo. 2002) (disciplining an assistant district attorney who misrepresented himself to a suspected murderer as a public defender); *see also In re Gatti*, 8 P.3d 966 (Or. 2000) (disciplining a lawyer who misrepresented himself as a medical professional in order to obtain information related to the representation of a client).

40 McNerney & Papadopoulos, *supra* note 12, at 1266.

41 Susskind, *supra* note 25, at 608.

42 *Id.* at 608–12.

43 Goldberg, *supra* note 25, at 543.

especially as it pertains to a client's voluntary online behavior and habits.[44]

II. THE UNDERREGULATION OF LAWYERS' CYBERSECURITY CONDUCT

Critics from the left and the right have long disparaged professional ideologies, and rules of professional conduct that implement and codify them, as self-serving rhetorical tools meant to justify the profession's power and status,[45] monopoly over the provision of legal services, and anticompetitive fees.[46] At first glance, the recent flurry of changes to Rules regarding cybersecurity[47] appear unnecessary, and thus susceptible to this criticism. To begin with, the Rules have long required lawyers to protect confidential information and so the promulgation of subsection 1.6(c), stating in relevant part that "a lawyer shall make reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,"[48] seems like a redundant clause, a rhetorical nod regarding cybersecurity. Similarly, the Rules have long demanded competence and so the revision of Comment 8 to Rule 1.1, stating in relevant part that "to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology* . . . ,"[49] seems perfunctory. Moreover, the changes appear unnecessary because on initial consideration one would expect clients' reactions, such as firing a law firm following a security breach, withholding new business, or filing a malpractice lawsuit, to provide lawyers with ample motivation and incentive to reasonably protect clients' information. Cybersecurity thus appears to be the posterchild for advocates of market controls and deregulation; instead of promulgating new rules of professional conduct, let the market regulate lawyers' cybersecurity conduct.

Closer scrutiny, however, reveals that liability rules (e.g., malpractice suits) and market controls (e.g., termination of the attorney-client relationship) are not likely to effectively regulate lawyers' cybersecurity conduct.[50] Generally, a plaintiff in a

---

44 *Id.*

45 *See, e.g.*, RICHARD L. ABEL, AMERICAN LAWYERS (1989); MAGALI S. LARSON, THE RISE OF PROFESSIONALISM: A SOCIOLOGICAL ANALYSIS (1977).

46 RICHARD A. POSNER, THE PROBLEMATICS OF MORAL AND LEGAL THEORY 185–211 (1999).

47 *See infra* Section III.A.

48 MODEL RULES OF PROF'L CONDUCT r. 1.6(c) (AM. BAR ASS'N 2013).

49 *Id.* r. 1.1 cmt. 8 (emphasis added).

50 For a review of disciplinary, liability, institutional, legislative, and market

malpractice lawsuit must establish four elements: the existence of a duty, breach of the duty owed, causation, and damages.[51] Yet a plaintiff in a malpractice suit alleging negligence in failing to protect information is unlikely to be able to prove "damages because of the challenges in answering key questions about cybersecurity breaches: who perpetrated the cyberattack; what information did they steal; what is the value of that information to them or others; and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim?"[52] Consequently, there are hardly any cases litigating attorney (or even corporate) negligence for failure to protect confidential information.[53]

The same challenges—not knowing who perpetrated the cyberattack; what information they stole; what is the value of that information to them or others; and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim—limit the ability of clients to fire or otherwise sanction a law firm for failing to protect confidential information. Worse, clients are often prevented from reacting to lawyers' cybersecurity inaction because they do not find out about it. To be sure, some clients, usually sophisticated and powerful entity clients, have been pressuring their law firms to put in place cybersecurity measures and others have demanded being advised of security breaches.[54] Yet lawyers are under no general duty to report attacks to clients,[55] often do not learn about attacks themselves,[56] and when lawyers do find out about attacks, they often have insufficient information to allow for comprehensive reporting to clients.

Thus, clients often do not find out about lawyers' cybersecurity breaches, and when they do, they have insufficient information on which to respond or to successfully sue. Unfortunately, underregulation—the inability of clients to effectively utilize liability rules and market controls to ensure that lawyers face appropriate cyber incentives—compounds the

---

controls, see Wilkins, *Who Should Regulate Lawyers?*, *supra* note 9, at 804–19. *See generally* David B. Wilkins, *How Should We Determine Who Should Regulate Lawyers? Managing Conflict and Context in Professional Regulation*, 65 FORDHAM L. REV. 465 (1996).

51 RONALD E. MALLEN & ALLISON MARTIN RHODES, LEGAL MALPRACTICE: THE LAW OFFICE GUIDE TO PURCHASING LEGAL MALPRACTICE INSURANCE § 1:2 (2016).

52 McNerney & Papadopoulos, *supra* note 12, at 1261.

53 *Id.* at 1260; *see also* Hughes, *supra* note 26, at 426 ("[M]ost data breach class actions have been dismissed for lack of damages.").

54 *See, e.g.*, Monica Bay, *Understanding the Risks to Cybersecurity: Large Law Firms Are Viewed as Vulnerable and Store Information that Hackers Know Is Valuable*, 36 NAT'L L.J. 28, 28 (2014).

55 *See infra* Section III.A.

56 Simshaw, *supra* note 5, at 550–51.

underlying problem. As lawyers face insufficient incentives to implement appropriate cybersecurity measures and report attacks to clients, data about attacks and their consequences goes uncollected, diminishing the prospects of effective liability rules and market controls developing in the future. This is the kind of market failure that is unlikely to resolve itself without regulatory intervention, except that liability rules are not likely to constitute an effective regulatory response. It is also the kind of market failure that prevents the collection of the very data we need to better understand the extent of the problem we are facing.

To be sure, underregulation does not mean that lawyers face no regulatory forces pertaining to their cybersecurity conduct. To begin with, legislative controls regulate the cyber conduct of lawyers. State laws impose on lawyers, and others who hold personal information about customers, data breach notification duties if they reasonably believe that an unauthorized party has obtained the customers' information.[57] In addition, various federal statutes address data breach in specific industries. For example, attorneys working in the health care industry who have access to covered information are subject to the privacy and security provisions of the Health Insurance Portability & Accountability Act;[58] other federal statutes generally regulating data security may apply to lawyers as well.[59]

Next, even in the absence of reported malpractice decisions regarding failure to protect confidential client information, liability rules may indirectly inform attorneys' cyber conduct. For example, law firms accused of cybersecurity misconduct by clients may decide to settle cases to avoid having to publicly defend suits risking exposure of embarrassing cyber details and consequential reputational harm. Similarly, market controls may also inform lawyers' conduct, even if clients do not learn about cyberattacks and compromised information. Powerful clients can demand that their lawyers establish reasonable cybersecurity policies, and some lawyers, even in the absence of a duty to disclose information to clients about cyberattacks, may reveal information to build trust in the attorney-client relationship or to avoid undermining it upon subsequent disclosure. Other lawyers may take cybersecurity action to comply with insurance companies' protocols, even if the risk of malpractice liability is remote.

---

57 McNerney & Papadopoulos, *supra* note 12, at 1254–55.

58 Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

59 McNerney & Papadopoulos, *supra* note 12, at 1256 (describing guidelines advising corporations and attorneys to report material cyber risks and incidents to the SEC).

Yet other lawyers may respond to social norms, such as peer pressure and organically evolving norms within their legal communities. For example, as cybersecurity awareness increases, and Continuing Legal Education providers flood the marketplace with offerings, lawyers may be induced to take a class to keep up with the competition. Also, as younger attorneys, likely more tech-savvy, join the profession, law firms become both more aware of cyber conduct and more apt to engage with it more directly.

In sum, while the ineffectiveness of traditional liability rules and market controls results in the systematic underregulation of lawyers' cybersecurity conduct, other regulatory controls have led to significant changes in the cyber habits of some members of the legal profession, such as the increased use of two-factor authentication in lieu of a single password to access secure systems.[60] Before turning to explore rules of professional conduct as a possible remedy to lawyers' likely cybersecurity inaction, a word about Holmesian bad people.[61] Since we do not know enough about the extent and scope of cyberattacks against lawyers, admittedly in part because lawyers do not gather or share this information, why assume that lawyers do not do enough to protect their clients' information and best interests? Even conceding a legal world of increased atomism and individualism, one in which lawyers and their clients seek to maximize their short-term interests with little regard to the impact on others,[62] why assume that, but for regulatory intervention, most or even many lawyers will act as Holmesian bad people and try to get away with implementing insufficient cybersecurity measures? Surely some lawyers will do the right thing by their clients simply because it is the right thing to do.

Regrettably, in addition to the dominance of individualism (or the hired gun ideology)[63] and the relative decline of relational approaches in legal (and business) decision making made by both clients and lawyers,[64] three interrelated reasons suggest that,

---

60 *See, e.g.*, Ellen Blanchard & Rodney Blake, *Law Firms Are the New Target for IP Theft: Basic Protections*, IPWATCHDOG (June 19, 2015), http://www.ipwatchdog.com/2015/06/19/law-firms-are-the-new-target-for-ip-theft-basic-protections/id=58656/ [http://perma.cc/3G3U-9UBY].

61 *See* Russell G. Pearce & Eli Wald, *Rethinking Lawyer Regulation: How a Relational Approach Would Improve Professional Rules and Roles*, 2012 MICH. ST. L. REV. 513, 522–23 (2012).

62 *See* Russell G. Pearce & Eli Wald, *The Obligation of Lawyers to Heal Civic Culture: Confronting the Ordeal of Incivility in the Practice of Law*, 34 U. ARK. LITTLE ROCK L. REV. 1, 26–39 (2011).

63 *See generally* William H. Simon, *The Ideology of Advocacy: Procedural Justice and Professional Ethics*, 1978 WIS. L. REV. 29 (1978).

64 Pearce & Wald, *supra* note 62; Russell G. Pearce & Eli Wald, *The Relational Infrastructure of Law Firm Culture and Regulation: The Exaggerated Death of Big Law*,

absent regulatory intervention, some lawyers are likely to try to get away with offering insufficient cyber protection to clients and acting as Holmesian bad people.

First, implementing effective cybersecurity measures can entail significant expenses. While some costs can be easily rolled onto clients, for example, expenses directly related to undertaking specific measures in connection with the representation of clients with known security risks and needs, other expenses, such as the cost of upgrading the entire cybersecurity apparatus of the firm or the time investment of lawyers and staff learning about the apparatus, may be harder to recoup.

Second, even when the costs of implementing cybersecurity measures can be recouped, lawyers are notoriously technophobic.[65] To be sure, some lawyers are at the forefront of using new technological advances to better serve clients.[66] Yet the legal profession has a long, documented history of resisting technological advances due to ignorance,[67] vanity,[68] status envy,[69] and independence,[70] which suggests that, left to their own devices, lawyers are unlikely to implement the necessary cybersecurity measures to protect clients' information.

Finally, some cybersecurity measures, such as limiting access to unsecure networks and mobile devices, abstaining from using portable drives, frequent change of passwords, and timely lock down of computers in and out of the office, are likely to be perceived to be, and indeed are, cumbersome for lawyers. This is especially true for older and less technology-savvy attorneys, some of whom, by virtue of their seniority, are also likely to be powerful within their firms and therefore harder to reign in. In sum, because liability rules and market controls are unlikely to provide lawyers with a sufficient incentive to take appropriate cybersecurity action, and because implementing effective cybersecurity measures is expensive, time-consuming, and inconvenient, some lawyers are unlikely to reasonably protect their clients' information absent regulatory intervention.

---

42 HOFSTRA L. REV. 109, 110 (2013).

65 Timothy J. Toohey, *Beyond Technophobia: Lawyers' Ethical and Legal Obligations to Monitor Evolving Technology and Security Risks*, 21 RICH. J.L. & TECH. 9 (2015).

66 *See* William Henderson, *What the Jobs Are: New Tech and Client Needs Create a New Field of Legal Operations*, A.B.A. J. (Oct. 1, 2015, 6:00 AM), http://www.abajournal.com/magazine/article/what_the_jobs_are [http://perma.cc/WHB9-E4UC].

67 *See, e.g.*, Brian E. Finch, *The Legal Profession Needs to Get Smart About Cybersecurity*, NAT'L L.J. 27, at 27 (2015).

68 Vivia Chen, *Why is 'Phooling' a Lawyer So Easy?*, NAT'L L.J. 5, at 5 (2015).

69 Ezekiel, *supra* note 13, at 656.

70 *Id.*

III. THE LEGAL ETHICS OF CYBERSECURITY

Professional ideologies and rules of professional conduct promulgated by lawyers are often self-serving and warrant a healthy dose of skepticism, yet at the same time, they play an important and effective role in the regulation of lawyers. As liability rules, the rules of professional conduct—part and parcel of state law—define misconduct and give rise to a disciplinary system that incentivizes lawyers to comply with them.[71] As the embodiment of professionalism, rules of professional conduct are social norms that shape and guide the conduct of lawyers. Thus, notwithstanding criticisms of rules of professional conduct and acknowledging their chronic underenforcement,[72] legal ethics rules can play an important role in the regulation of lawyers.[73]

A. The Current Legal Ethics Stance on Cybersecurity

To their credit, the Rules have been revised in recent years to take account of technological changes impacting the practice of law. In August 2012, the ABA House of Delegates renumbered Comment 6 to Rule 1.1 on competence as Comment 8 and added a clause calling on lawyers to keep abreast of relevant technology affecting their practice. While the revision was made to a Comment rather than in the body of the Rule, was aspirational rather than mandatory, and failed to explicitly identify cybersecurity as a concern or a priority (stating instead that "to maintain the requisite knowledge and skill" mandated by Rule 1.1, "a lawyer *should* keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . ."),[74] the Comment revision was not without practical impact. It does open the door to discipline, designating ignorance of relevant technology as incompetence and thus misconduct, and, by identifying knowledge of relevant technology as a component of competence, it did help give rise to a cottage industry of Continuing Legal Education courses about cybersecurity.[75] Notably, however, the Comment does not deem

---

71 MODEL RULES OF PROF'L CONDUCT r. 8.4(a) (AM. BAR ASS'N 2013). Rules of professional conduct also establish standards of conduct which inform determination of civil liability for malpractice. *See id.* at Preamble & Scope ¶ 20.

72 Richard L. Abel, *Why Does the ABA Promulgate Ethical Rules?*, 59 TEX. L. REV. 639, 648 (1981) ("[S]tudy after study has shown that the current rules of professional conduct are not enforced."); Wilkins, *Legal Realism for Lawyers*, *supra* note 9, at 493 (noting that the rules of professional conduct tend to be "systematically underenforced").

73 Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338 (1997) (discussing how legal norms and rules affect professional conduct).

74 MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (emphasis added).

75 Darla W. Jackson, *Cybersecurity: Breaches and Heartbleed to BYOD – Are Bankers, Entertainment Company Executives, Celebrities, Postal Workers, Ice Cream Lovers, Home*

the failure to utilize technology or inaction with regard to technological risks as incompetent conduct. Rather, all it recommends is keeping abreast of benefits and risks of relevant technology.

Arguably, a more significant change was made to Rule 1.6 on confidentiality. Elevating a Comment to a new subsection of Rule, 1.6(c), the Rule now mandates that "[a] lawyer shall make *reasonable efforts* to prevent . . . the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[76] Importantly, exactly because the dearth of malpractice litigation regarding failure to protect information results in lack of judicial exposition of reasonableness, new Comments 18 and 19 to Rule 1.6 do offer a partial definition of reasonable efforts.

After emphasizing the central role of reasonableness, stating that "[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure,"[77] Comment 18 adds that:

> [f]actors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[78]

Comment 19 similarly identifies reasonableness as a key term of art, adding that "[w]hen transmitting a communication that includes information relating to the representation of a client,"[79] that is, confidential information,[80]

> the lawyer must take *reasonable precautions* to prevent the information from coming into the hands of unintended recipients . . . . Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.[81]

Builders, and CIOs the Only Ones Who Should Be Concerned?, 106 L. LIBR. J. 633, 638 (2014) (noting that the A.B.A. has begun offering a Cybersecurity Series); *see also ABA Cybersecurity Series*, A.B.A., http://www.americanbar.org/content/ebus/events/ce/cyber-security-core-curriculum.html [http://perma.cc/6X3H-LN49].

76 MODEL RULES OF PROF'L CONDUCT r. 1.6(c) (emphasis added).

77 *Id.* r. 1.6 cmt. 18.

78 *Id.*

79 *Id.* r. 1.6 cmt. 19.

80 *Id.* r. 1.6(a).

81 *Id.* r. 1.6 cmt. 19 (emphasis added).

Comments 18 and 19 take a first important step in defining the meaning of "reasonable efforts" to protect clients' information. They correctly identify reasonableness as a key element in assessing cybersecurity measures, and they begin to define the term, referring to the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients as relevant considerations of reasonableness.

Yet Rule 1.6(c) and Comments 18 and 19 fall short in several respects. First, they fail to require that lawyers put in place a cybersecurity plan which will regularly monitor their cybertechnology to detect breaches. Perhaps the Comment implies a duty to regularly monitor one's cybersecurity measures, after all, how can a lawyer assess "the likelihood of disclosure if additional safeguards are not employed" without monitoring the performance of existing safeguards? Similarly, assessing "the cost of employing additional safeguards" as well as "the difficulty of implementing the safeguards" implies a duty to assess one's existing apparatus. But the Comments fail to explicitly identify a duty to implement a cybersecurity plan, a noteworthy omission given that elsewhere the Comments do explicitly impose similar duties. For example, while a duty to monitor for conflicts of interest may be implied from a Rule prohibiting conflicts of interest, Comment 3 to Rule 1.7 on conflicts of interest explicitly states that:

> [t]o determine whether a conflict of interest exists, a lawyer should adopt reasonable procedures, appropriate for the size and type of firm and practice, to determine . . . the persons and issues involved . . . . Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule.[82]

Yet, while ignorance about cybersecurity attacks and their scope appears to be the norm, the Comment to Rule 1.6 fails to explicitly demand monitoring for cyberattacks akin to the monitoring of conflicts of interest.

Second, Rule 1.6(c) and its Comment do not sufficiently clarify what constitutes "reasonable efforts" and "reasonable precautions." Perhaps, in a world of constantly evolving technology, the Comment avoided specifying the nature of appropriate measures to prevent it from quickly becoming antiquated. Curiously, however, the Comment did not shy away

---

82 *Id.* r. 1.7 cmt. 3.

from delving into the meaning of reasonableness when such analysis benefited lawyers. Comment 19 states in relevant part that "[t]his duty," to take reasonable precautions to prevent the unauthorized disclosure of client information, "however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[83] This innocent sounding clause implicitly refers to ABA Formal Opinion 99-413, in which the ABA Standing Committee held that "[a] lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the [Rules] because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[84]

In other words, Comment 19, while ostensibly staying clear of defining the meaning of "reasonable efforts," nonetheless states that the use of unencrypted e-mail by lawyers is reasonable because apparently unencrypted e-mails "afford[] a reasonable expectation of privacy" based on Formal Opinion 99-413, which found that "[t]he same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail."[85] The point, to be clear, is not to debate whether the Committee's conclusion, made in 1999, that unencrypted e-mails afford a reasonable expectation of privacy, still holds true presently, although some have characterized the conclusion as "misguided."[86] Rather, it is that what Comment 19 does half-heartedly and indirectly[87]—delving into the definition of reasonable efforts—it ought to do openly and clearly.

Third, Rule 1.6(c) and its Comment fails to mandate disclosure to clients regarding cyberattacks and/or security breaches regarding client information. There are at least two possible good faith explanations for this omission. To begin with, attorney-client communications are generally governed by Rule 1.4, not Rule 1.6, and so there would be no reason to require communications regarding cybersecurity in the latter. Yet the

---

83 *Id.* r. 1.6 cmt. 19.

84 A.B.A. Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (discussing protection of confidentiality by means of unencrypted e-mail).

85 *Id.*

86 Toohey, *supra* note 65, at 23; *see also* Rebecca Bolin, *Risky Mail: Concerns in Confidential Attorney-Client Email*, 81 U. CIN. L. REV. 601, 618–21 (2012) (discussing and critiquing the effect of 99-413).

87 Curiously, Comment 19 fails to identify Formal Opinion 99-413, although it appears to cite its language. *Compare* MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 19 (AM. BAR ASS'N 2013), *with* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).

Rules and Comments often explicitly cross-reference other Rules such that the failure to reference Rule 1.4 is glaring. Indeed, Comment 18 does reference Rules 1.1, 5.1, and 5.3, making the omission to reference Rule 1.4 inexplicable. Next, Comments 18 and 19 do implicitly reference Rule 1.4, both stating in relevant part that "[a] client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule."[88] Rule 1.4(a)(1), in turn, states in relevant part that "[a] lawyer shall promptly inform the client of any decision or circumstance with respect to which the client's informed consent . . . is required,"[89] such that one could argue that the Comments 18 and 19 indirectly reference Rule 1.4 (by referring to informed consent, which requires communicating with clients). But even viewed in the light most favorable to the Rules, such indirect reference to Rule 1.4 is lacking as it fails to require disclosure to clients of cybersecurity attacks or breaches. It only indirectly triggers a duty to communicate regarding forgoing security measures as opposed to imposing a general duty to communicate regarding cybersecurity. Furthermore, Comments 18 and 19 fail to reference the subsections of Rule 1.4 that may give rise to a duty to communicate regarding cybersecurity concerns, namely 1.4(a)(2), 1.4(a)(3), and 1.4(b).

Notwithstanding the silence of Rule 1.6(c), does Rule 1.4 independently require lawyers to communicate with clients regarding cybersecurity, let alone advise clients about cyberattacks against the law firm and/or breaches of security? Most commentators opining on this issue believe the Rules do not impose such a duty,[90] and regrettably they appear to be right because the Rules essentially only mandate disclosure of material information to clients, and the usual uncertainty engulfing cyberattacks casts an inherent doubt on the materiality of cyberattacks and resulting breaches.

Rule 1.4(a)(2) states that "[a] lawyer shall . . . reasonably consult with the client about the means by which the client's objectives are to be accomplished."[91] Cybersecurity measures certainly qualify as part of the *means* by which the client's objectives are to be accomplished, and thus would support an interpretation pursuant to which a lawyer must reasonably

---

88 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 18.

89 *Id.* r. 1.4(a)(1).

90 *See, e.g.*, Ezekiel, *supra* note 13, at 653 ("Most astonishingly, the existing professional responsibility standards generally *do not require any disclosure to the client* when client information is stolen from a law firm.").

91 MODEL RULES OF PROF'L CONDUCT r. 1.4(a)(2).

consult with the client about reasonable security measures, for example, whether to encrypt communications regarding the representation, but the Rule falls short of explicitly demanding such a communication. Therefore, if a lawyer has in place cybersecurity measures, or reasonably believes that his cybersecurity measures or lack thereof are sufficient, Rule 1.4(a)(2) does not appear to require any communication whatsoever. Worse, Rule 1.4(a)(2) says nothing whatsoever about cyberattacks or security breaches.

Rule 1.4(a)(3) states that "[a] lawyer shall keep the client reasonably informed about the status of the matter,"[92] and Comment 3 adds that "paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation."[93] If cybersecurity measures are to be construed as the "*means* by which the client's objectives are to be accomplished," they are certainly not the *matter*, and thus, 1.4(a)(3) appears not to generally apply to cybersecurity communications. However, a significant cybersecurity breach that results in the disclosure of otherwise confidential and privileged information, or that foils the negotiation of a transaction on behalf of a client, can certainly impact the status of a matter. Comment 3 supports that interpretation because a significant cybersecurity breach would be a "significant development" affecting the substance of the representation.[94]

In any event, however, Rule 1.4(a)(3) falls short of imposing a general duty of communication regarding cybersecurity attacks and breaches. Rather, it only mandates disclosure to clients of significant cyber breaches which constitute a significant development and result in an impact regarding the status of the representation. Moreover, the same considerations that obscure clients' ability to prove damages resulting from a lawyer's failure to reasonably protect information—not knowing who perpetrated the cyberattack, what information they stole, what the value of that information is to them or others, and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim—would often shield lawyers from discipline for violating 1.4(a)(3). If a lawyer does not know who perpetrated the cyberattack, what information was stolen, what the value of that information is to them or others, and what other

---

92 *Id.* r. 1.4(a)(3).

93 *Id.* r. 1.4 cmt. 3.

94 *See* Colo. Bar Ass'n Ethics Comm., Formal Ethics Op. 113 (Nov. 19, 2005) (discussing the ethical duties of an attorney to disclose errors to a client).

harms resulted for the client, how could a lawyer ever conclude that a breach constitutes a "significant development"?

Rule 1.4(b) states that "[a] lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."[95] While Rule 1.4(b) appears to only apply to explaining the "matter" at hand, Comment 5 importantly clarifies that:

> [t]he client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation *and the means by which they are to be pursued* . . . . The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation.[96]

Rule 1.4(b) arguably gives rise to a general duty to communicate regarding cybersecurity and, in particular, about cyberattacks and breaches because cybersecurity measures are part of the means by which the client's objectives are to be pursued. Thus, the client should receive sufficient information from the lawyer to be able to participate intelligently in decisions concerning cybersecurity. ABA Formal Opinion 95-398 lends support to this interpretation, finding that "should a significant breach of confidentiality occur . . . a lawyer may be obligated to disclose such breach to the client or clients whose information has been revealed,"[97] citing Rule 1.4(b), and adding that "[w]here the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b)."[98] Yet, like Rule 1.4(a)(3), the communication appears to be mandated only with regard to severe cyberattacks with significant impact on a client, or limited to communications regarding cybersecurity "means" rather than a clear general duty requiring communication regarding cybersecurity measures, attacks, and breaches.[99]

Some commentators have argued that Rule 1.15 on safekeeping property pertains to protecting client information because Rule 1.15(a) states, *inter alia*, that "other property," presumably including information, "shall be . . . appropriately safeguarded."[100] No doubt Rule 1.15 applies, if only to impose on lawyers a duty to monitor client trust accounts for cyberattacks

---

95 MODEL RULES OF PROF'L CONDUCT r. 1.4(b).

96 *Id.* r. 1.4 cmt. 5 (emphasis added).

and breaches.[101] Yet, the application adds little to Rules 1.6(a) and 1.6(c), which impose a general duty to protect clients' confidential information from unauthorized disclosure.

Rule 5.1, regarding responsibilities of supervisory lawyers to other lawyers, and Rule 5.3, regarding supervisory responsibilities to non-lawyer assistance, have been slightly revised to reflect technological changes. Read together, Rules 5.1 and 5.3 require some lawyers to supervise the conduct of other lawyers and non-lawyers inside and outside of the practice. They state that supervisory lawyers "shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that,"[102] first, "all lawyers in the firm conform to the Rules of Professional Conduct,"[103] including Rules, such as 1.1 and 1.6 pertaining to cybersecurity, and second, that the conduct of non-lawyers employed by, retained by, or associated with the lawyer, "is compatible with the professional obligations of the lawyer."[104] As one commentator notes:

> These rules reflect the notion that a law firm's data security practices are only as strong as its weakest link. As a result, lawyers must make sure that subordinate attorneys, interns, paralegals, case managers, administrative assistants, and external business partners all understand necessary data security practices and the critical role that all parties play in ensuring the protection of client information.[105]

In addition, these changes make modest positive contributions to lawyers' understanding of new technological realities. For example, the title of Rule 5.3 was changed from

---

97 ABA Comm. on Ethics & Prof'l Resp., Formal Op. 95-398 (1995).

98 *Id.*; *see also* N.H. Bar Ass'n Ethics Comm., Advisory Op. #2012-13/4 (2013), https://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp ("Where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent."); Pa. Bar Assoc., Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2011), http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf [http://perma.cc/GJ87-T8TS] ("While it is not necessary to communicate every minute detail of a client's representation, 'adequate information' should be provided to the client so that the client understands the nature of the representation and 'material risks' inherent in an attorney's methods.").

99 See also Alaska Rule 5.3(d) (2014), dictating that "[a] lawyer who learns that any person employed by the lawyer has revealed a confidence . . . protected by these rules shall notify the person whose confidence or secret was revealed." Importantly, however, the rule does not generally apply to a law firm experiencing a cyberattack and compromised information but rather only to a third party employed by the law firm.

100 MODEL RULES OF PROF'L CONDUCT r. 1.15(a); *see also* Goldberg, *supra* note 25, at 529–30; Hughes, *supra* note 26, at 415–16.

101 Christine Daleiden, *Information Security Basics for Lawyers*, 18 HAW. B.J. 4, 8–9 (2014).

102 MODEL RULES OF PROF'L CONDUCT r. 5.1.

103 *Id.*

104 *Id.* r. 5.3.

105 Simshaw, *supra* note 5, at 563.

"Responsibilities Regarding Nonlawyer *Assistants*," to "Responsibilities Regarding Nonlawyer *Assistance*," to capture the notion that technology, including cybertechnology, assists lawyers in the practice of law. Rule 5.3, providing examples of the use of non-lawyers outside the firm, offers "using an Internet-based service to store client information" as an illustration.[106]

Yet, Rules 5.1 and 5.3, once again, forgo an opportunity to take a clear detailed stance regarding cybersecurity efforts and measures. For example, Comment 2 on Rule 5.1 states that "[p]aragraph (a) requires lawyers with managerial authority within a firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Rules,"[107] and goes on to give examples of such "internal policies and procedures," a perfect opportunity to require cybersecurity measures, including the adoption of cybersecurity plans. Instead, it states "[s]uch policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."[108]

Similarly, while Comment 3 on Rule 5.3 identifies lawyers' use of cloud computing as a form of non-lawyer assistance, it fails to detail any of the efforts and measures lawyers must employ in conjunction with the use of this technology. Instead, it generically states that: "[w]hen using such services outside the firm, a lawyer *must make reasonable efforts* to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations," adding that "[t]he extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; [and] the terms of any arrangements concerning the protection of client information."[109] In other words, the Rules once again invoke reasonableness without specifying its content and a commitment to protecting confidentiality without specific guidance as to the cybersecurity measures lawyers must put in place.

Lawyers' use of cloud computing has been the subject of various ethics opinions that serve as a revealing example of how

---

106 MODEL RULES OF PROF'L CONDUCT r. 5.3 cmt. 3.

107 *Id.* r. 5.1 cmt. 2.

108 *Id.* Arguably, given Rule 1.15's requirement that lawyers protect clients' property, including clients' trust accounts, Comment 2 could be read to demand cybersecurity measures to protect such accounts, but this would be at best an implied requirement.

109 *Id.* r. 5.3 cmt. 3.

ethics committees follow the lead of the Rules and offer only a limited insight into the meaning of reasonableness. Ethics opinions generally hold that cloud computing is permissible, as long as lawyers take reasonable steps when selecting and using services.[110] Notably, some states appear to impose additional, specific cybersecurity measures (Iowa requires lawyers to "[d]etermine the degree of protection the vendor provides to its clients' data"; New Jersey requires lawyers to "[m]ake sure that vendors are using available technology to guard against foreseeable infiltration attempts"; and North Carolina demands that its lawyers "[e]valuate the vendor's security and backup strategy"), and *The ABA Cybersecurity Handbook* wisely acknowledges that "[l]awyers should monitor and reassess the protections of the cloud provider as the technology evolves."[111] How lawyers are to go about meeting these requirements, however, is less than clear. As Drew Simshaw points out, "[i]t is also worth noting the limits of a lawyer's duties under the rules,"[112] according to these ethics opinions. For example, in New Hampshire, "a lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology," and "[w]hen it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard."[113]

All in all, the ABA must be commended for its proactive approach to addressing the evolving impact of technology on law practice. New subsection 1.6(c) explicitly identifies protection of client information, including cybersecurity measures, as a priority, and moving the language from a Comment to the body of the Rules signifies to lawyers the emphasis the Rules now place on information protection.[114] Next, the new subsection takes a first important step in shifting lawyers' focus from avoiding

---

110 *Cloud Ethics Opinions Around the U.S.*, A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloudethics-chart.html [http://perma.cc/VY84-VA7P]. In addition, *The ABA Cybersecurity Handbook* contains an appendix of "Ethics Opinions on Lawyer Confidentiality Obligations Concerning Cloud Computing." RHODES & POLLEY, *supra* note 4, at 245.

111 *Id.* at 77.

112 Simshaw, *supra* note 5, at 565.

113 N.H. Bar Ass'n Ethics Comm., Advisory Op. #2012-13/4 (2013), *supra* note 98.

114 For an excellent analysis of the Rules' new approach to cybersecurity, see generally Judith L. Maute, *Facing 21st Century Realities*, 32 MISS. C. L. REV. 345 (2013). The ABA has tried to stay at the forefront of enhancing lawyers' cybersecurity awareness. For example, in April 2016, ABA President Paulette Brown offered ABA members an opportunity to receive FBI cybersecurity alerts, noting that, "the ABA is keenly aware of the increase in efforts to hack into the computer systems of legal professionals to reach the significant amounts of non-public information they hold." *See* E-mail from Paulette Brown, President, Am. Bar Ass'n, to ABA Members (Apr. 12, 2016, 2:00 AM) (on file with author).

negligent and inadvertent disclosure to the new landscape of affirmatively protecting client information from unauthorized access by third parties. Moreover, Comments 18 and 19 to Rule 1.6 help clarify the meaning of the duty to protect client information by specifying the factors that render protective measures reasonable. Appropriate references to this new approach are made in Rules 1.1, 1.15, 5.1, and 5.3. Yet the Rules do not do enough to guide lawyers' cybersecurity conduct, especially given that liability rules and market controls are not likely to incentivize lawyers to sufficiently protect client information.

B. Responding to the New Frontier: The Future of Legal Ethics in the Age of Hackers and Cyberthreats to Clients' Information

The Rules embody, and have long taken, a one-size-fits-all, universal approach to the regulation of lawyers' conduct.[115] As such, they cannot, and should not, be amended frequently to reflect minor changes in the practice of law. Rather, the Rules are open-ended standards that can and should accommodate practice changes, for example via clarifying formal ethics opinions. However, sometimes changing practice realities do necessitate revisions to the Rules, and in such circumstances the Rules must be revised so they can continue to inform and guide lawyers' actual practice and avoid becoming antiquated.[116]

Cybersecurity is one such instance that necessitates changing the Rules. Protecting confidential client information, a fundamental tenet of law practice, used to be about avoiding negligent inadvertent disclosure. Typical examples of misconduct were leaving one's notes or laptop unattended in a conference room, or inadvertently disclosing confidential information to opposing counsel over e-mail.[117] Hackers, however, present a different challenge, one of affirmatively protecting information from unauthorized preying parties, often engaged in criminal activity. Technological advances commonly utilized in the practice of law, and the risks to unauthorized disclosure of client information they entail, thus require a regulatory shift in the Rules, from avoiding inadvertent disclosure to acknowledging a positive duty to protect confidential information. Put differently, the unique challenge cybersecurity concerns present is not merely coming to terms with technological advancements, which

---

115 Wald, *supra* note 9, at 228.

116 *Id.*

117 Silkenat, *supra* note 2, at 450; *see, e.g.*, MODEL RULES OF PROF'L CONDUCT r. 4.4(b) (AM. BAR ASS'N 2013).

the profession, while reluctant, has done in the past.[118] Rather, it is shifting from a passive regime of avoiding negligent disclosure to an active regime of affirmatively protecting information against parties, some of which engage in criminal activity.

To be clear, the emergence of lawyers' affirmative duty to reasonably protect client information from unauthorized disclosure is not a move toward strict liability. Fully protecting client information from all cyberattacks is not feasible given current available technologies, and even if complete protection was possible, it might so undercut the use of effective technology and be so cost prohibitive as to render it unreasonable. Furthermore, utilizing technology to better serve the needs of clients, and confronting the risks inherent in the use of technology, is and ought to be a joint attorney-client undertaking. As clients reap the benefits of new technologies and are sometimes better positioned as compared to their lawyers to address their risks, there is no reason to impose strict liability on lawyers for the use of technology in the practice of law. Accordingly, lawyers need only take reasonable steps to protect client information. Yet, the Rules' approach to cybersecurity must recognize and effectuate an affirmative duty to reasonably protect clients' information and develop a helpful definition of reasonableness that encompasses an obligation to protect client information from criminal activity. The Rules must clarify that a lawyer not only needs to avoid negligently leaving notes in plain view, but must also protect against theft of one's virtual briefcase.

1. Mandating the Adoption of Appropriate Cybersecurity Plans for All Clients

Lawyers' cybersecurity conduct is underregulated, which likely results in insufficient action to protect client information. Because liability rules and market controls are unlikely to effectively incentivize lawyers to take reasonable action, the Rules must require that lawyers adopt appropriate cybersecurity plans. Revealingly, the ABA's Resolution 109 "encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected."[119] Yet nothing in the Rules imposes a duty on lawyers to develop cybersecurity programs for all clients.

---

118 Toohey, *supra* note 65.

119 ABA CYBERSECURITY RESOLUTION, *supra* note 3 (emphasis added).

To be sure, Comment 18 on Rule 1.6 does state that: "[p]aragraph (c) requires a lawyer *to act competently to safeguard information* relating to the representation of a client against unauthorized access by third parties," and adds that: "[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer *has made reasonable efforts to prevent the access or disclosure*,"[120] arguably indirectly encouraging lawyers to put in place a cybersecurity plan for all clients. After all, "acting competently" and making "reasonable efforts" would seem to require at least implementing a cybersecurity plan. Yet the Rules do not affirmatively require the adoption of such a plan and would appear to tolerate an interpretation that at least in some circumstances the prongs of "acting competently" and making "reasonable efforts" could be satisfied without the implementation of a cybersecurity plan. Indeed, Comment 18 does not specify what constitutes "acting competently" nor "reasonable efforts."[121]

The Rules ought to require that all lawyers maintain an appropriate cybersecurity plan, akin to Comment 3 on Rule 1.7, which mandates the adoption of reasonable conflict-checking procedures.[122] Accordingly, a new Comment X to Rule 1.6 should read:

> [t]o competently safeguard information relating to the representation of a client against unauthorized access by third parties, a lawyer must adopt reasonable procedures, including reasonable cybersecurity measures, appropriate for the size and type of firm and practice, to protect a client's confidential information. Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule.[123]

---

120 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 18.

121 *See* Ezekiel, *supra* note 13, at 658–59 ("These rules generally require the law firms to take 'reasonable efforts,' 'reasonable steps,' or 'reasonable precautions' to avoid unauthorized disclosure, but are unspecific about what such precautions might entail. One rule demands that the precautions taken must "meet[] industry standards," but is unfortunately vague about whether it refers to the standards of the *legal* industry or those of the *Internet data storage* industry.") (internal citations omitted).

122 MODEL RULES OF PROF'L CONDUCT r. 1.7 cmt. 3.

123 The Comment to Rule 1.6 includes two sections, Comments 18 and 19, under the subheadings of "Acting Competently to Preserve Confidentiality." *See id.* The proposed Comment can be added as Comment 18, renumbering current Comments 18 and 19 as 19 and 20 respectively; or as Comment 20 (renumbering current Comment 20 regarding confidentiality duties owed to former clients as Comment 21). Or the proposed Comment can be added to the existing Comment. For a redline of the proposed revisions to the Rules, see Appendix A.

2. Defining "Reasonable Efforts": Reasonable Cybersecurity Measures

Just as Comment 3 on Rule 1.7 has resulted in virtually all law firms employing a conflict-checking software as the first step in detecting conflicts of interest, proposed new Comment X to Rule 1.6 should result in all law firms adopting basic cybersecurity measures, such as employing current virus scanners and firewalls, installing patches and updates, and using cryptographically strong passwords, reasonably replaced from time to time,[124] as the first step in implementing a comprehensive cybersecurity plan. Yet the adoption of basic cybersecurity measures should not be left to chance. Instead, adoption of such basic security measures must be explicitly recognized as a professional requirement for any attorney who stores sensitive client data on an Internet-connected computer.[125] For example, law firms must be expected to demonstrate their system's ability to detect and repel a cyberattack.[126]

Thus, to begin with, "reasonable efforts" must include basic cybersecurity measures such as "robust strategies for identifying, prioritizing, and securing . . . valuable information,"[127] periodical inspection of the firm's operating and information storage systems for signs of cyberattacks and data theft, the use of current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents, avoiding the use of web-based e-mail services and public Wi-Fi, replacing the default passwords on network hardware, and the adoption of training protocol for firm lawyers and staff, appropriate for the size and practice of the firm, for example, to recognize phishing attacks.[128]

A new Comment Y to Rule 1.6 should read:

> [r]easonable efforts to prevent the inadvertent or unauthorized disclosure of electronically stored information relating to the representation of a client would normally include robust strategies for identifying, prioritizing, and securing valuable information; periodical inspection of the firm's information storage system for signs of cyberattacks and data theft; the use of basic cybersecurity measures, including the use of current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords

---

124 *See supra* note 29 and accompanying text.
125 *See* Ezekiel, *supra* note 13, at 665.
126 Silkenat, *supra* note 2, at 455.
127 McNerney & Papadopoulos, *supra* note 12, at 1250.
128 *See supra* note 29 and accompanying text.

> updated from time to time, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents; and the adoption of cybersecurity training protocols for firm lawyers and staff. *See* Rule 5.1 and 5.3.[129]

An attempt to identify basic cybersecurity measures in the Comment entails two related risks. A closed-list of measures may, over time, be treated as a "check-a-box" procedure for purposes of avoiding discipline, or understood to constitute a safe harbor—in the sense that lawyers who employ these basic cybersecurity measures may never be found to have failed to make "reasonable efforts" to protect their clients' information. To avoid such misapprehension, the Comment should explain that basic cybersecurity measures form but a floor for appropriate cyber conduct, necessary but often insufficient means of satisfying the requirement of "reasonable efforts." Far from constituting a safe harbor, basic measures simply set up a default foundation for "reasonable efforts," which depend on a variety of factors already identified by the Comment. Moreover, the Comment should explicitly state that some circumstances may require the adoption of additional special cybersecurity measures.

Comment Z to Rule 1.6 may accordingly add that:

> [w]hether a lawyer may be required to take additional special security measures to safeguard a client's information, above and beyond basic cybersecurity measures, depends on the circumstances. For example, a lawyer may be required to take special security measures to protect sensitive information related to the representation of a client.[130]

Relatedly, technological advances may, over time, render proposed Comment Y obsolete, a concern compounded by the traditional delay involved in adoption of revisions to the Rules, first at the ABA level and subsequently by states to their respective rules of professional conduct. Indeed, one commentator concludes that given the long delay inherent in Rules revisions, the "ABA and state bar associations have demonstrated that they might not be the best sources of reform in this subject [cybersecurity]."[131] Yet one should not overstate the rate of relevant technological advances, indeed, many of the currently available basic cybersecurity measures, admittedly in more

---

129 See *infra* Appendix A for a redline of the proposed revisions to the Rules. Rules 5.1 and 5.3 ought to be amended respectively to reference proposed Comment Y to Rule 1.6.

130 *Id.*

131 Travis Andrews, *Technological Innovation, The Legal Profession and the Need for Uniform Law*, CHARLOTTE L. REV. (forthcoming 2016) (manuscript at 2), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2684950.

primitive forms, have been available for a few decades now. In any event, lamentable delays in promulgation and revision notwithstanding, the Rules remain the only practical and, therefore, most operative means of correcting for the underregulation of lawyers' cybersecurity conduct, given the ineffectiveness of liability rules and market controls and the distant probability of national cybersecurity legislation, let alone one that would apply to lawyers. If at all, a years-long delay in the promulgation of the Rules and their adoption by the states does not constitute a compelling reason to avoid regulation. Quite the contrary, the delay ought to be addressed by reforming the historical process of promulgation and adoption to ensure that the Rules remain relevant and helpful to lawyers. There is no denying that old political habits die hard, especially at the hands of the ABA House of Delegates and state supreme courts' advisory committees. Yet, failure by the legal profession to effectively regulate itself may result, and in fact has resulted, in increased federal and state legislation undermining the profession's privilege of self-regulation.[132]

Nor would an ABA Formal Opinion be an adequate substitute to proposed Comment Y to Rule 1.6. Ethics opinions, while relatively easier and faster to publish and withdraw, if rendered obsolete, have no binding authority and are therefore inferior to Rules' revisions.[133] Moreover, given the underregulation of lawyer's cybersecurity conduct, ethics opinions will simply not do. The Rules must be revised to send lawyers a credible message, both substantively and symbolically, about the importance of acting affirmatively to protect clients' information. If technology ends up rendering proposed Comment Y obsolete, it can be revised in accordance with evolving cybersecurity knowledge and expertise.

---

132 *See* Daniel R. Coquillette & Judith A. McMorrow, *Zacharias's Prophecy: The Federalization of Legal Ethics*, 48 SAN DIEGO L. REV. 123 (2011) (documenting the federalization of legal ethics); Bruce A. Green, *ABA Ethics Reform from "MDP" to "20/20": Some Cautionary Reflections*, 2009 J. PROF. LAW. 1, 4–7 (2009) (arguing that future reform to the regulation of lawyers may require abandoning the state-based approach); Eli Wald, *Federalizing Legal Ethics, Nationalizing Law Practice and the Future of the American Legal Profession in a Global Age*, 48 SAN DIEGO L. REV. 489 (2011); Fred C. Zacharias, *Federalizing Legal Ethics*, 73 TEX. L. REV. 335 (1994); *see also* Ted Schneyer, *Professional Discipline in 2050: A Look Back*, 60 FORDHAM L. REV. 125, 127 (1991) (predicting the adoption of a "Federal Code of Lawyering"). Of course, states may act independent of the ongoing federalization of legal ethics and regulate the practice of law within their jurisdictions. *See, e.g.*, CAL. BUS. & PROF. CODE § 6000 (West 2016).

133 *See* Peter A. Joy, *Making Ethics Opinions Meaningful: Toward More Effective Regulation of Lawyers' Conduct*, 15 GEO. J. LEGAL ETHICS 313, 317–19 (2002).

3. "Reasonable Efforts" Further Construed

To further clarify that basic cybersecurity measures merely define a floor rather than a ceiling for "reasonable efforts," the Comment to Rule 1.6 must spell out the meaning of "reasonable efforts" beyond such basic steps. Comment 18 already helps construe "reasonable efforts," stating in relevant part:

> [f]actors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[134]

Comment 19 adds that:

> [w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use *special security measures* if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.[135]

The Comment, however, does not define the term "special security measures," except indirectly by using language similar to the one used in ABA Formal Opinion 99-413 on encryption of confidential information.[136] Instead, the Comment can provide examples of "special security measures," such as the use of encryption to protect sensitive client information and attorney-client communications.[137]

Next, the Comment may explicitly state that a lawyer who fails to take the most basic security precautions violates Rule 1.6(c), even if the client's information was accessed by a third party criminally. In other words, the Comment should state that the criminal conduct of third parties does not constitute a safe harbor to lawyers who fail to make "reasonable efforts" to protect the information. Historically, the Rules made attorneys liable for their own conduct, for example, inadvertently disclosing

---

134 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS'N 2013).
135 *Id.* r. 1.6 cmt. 19 (emphasis added).
136 *See* ABA Comm. on Ethics & Prof'l Responsibility, *supra* note 84.
137 See proposed Comment U, Appendix A.

confidential client information, but not for the criminal actions of third parties. "This view," explains Alan Ezekiel, "that attorneys are not responsible for violations of client privacy that flow from criminal misconduct by third parties may have been informed by the evolution of legal standards regarding the use of mobile phones."[138] Whereas early ethics opinions in the 1990s suggested that attorneys might violate rules of professional conduct by discussing private client information on mobile phones because outsiders could overhear the conversations, later opinions reflected the view that "the Electronic Communications Privacy Act (which criminalized interception of wireless telephone conversations) created a reasonable expectation of privacy on a mobile phone, and thus the attorney could discuss client matters on a mobile phone without violating any ethical standards."[139] Importantly, "[t]he fact that an outsider might be able to overhear the conversation was irrelevant," adds Ezekiel, "because the outsider would thereby be committing a felony."[140]

Similarly, because "[a] hacker would be committing a felonious violation of the Computer Fraud and Abuse Act by accessing client records without authorization,"[141] Comment 19's statement that the duty to protect client information "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy"[142] can be read to suggest that an attorney who fails to prevent unauthorized criminal access to client information is not acting unreasonably. "But," asked Ezekiel compellingly, "should the fact that hacking is illegal excuse an attorney who fails to take even the most basic security precautions in an era of widespread data theft?"[143]

Of course, that a third party commits a crime to access client information is relevant in terms of determining the consequences for the client. For example, because the attorney-client privilege belongs to the client, only the behavior of the client—holder of the privilege—or the client's lawyer-agent can waive it. Therefore, in most jurisdictions, intercepted communications are still privileged, meaning that client information stolen from the lawyer would nonetheless continue to be privileged.[144] Such attempts to mitigate the consequences of information theft for

---

138 Ezekiel, *supra* note 13, at 659.
139 *Id.*
140 *Id.* at 659–60.
141 *Id.*
142 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 19 (AM. BAR ASS'N 2013).
143 Ezekiel, *supra* note 13, at 660.
144 Hughes, *supra* note 26, at 417–18.

victim-clients ought not, however, negate the misconduct of an attorney who fails to utilize basic cybersecurity measures to protect client information.

Thus, in addition to offering examples of "special security measures" and the circumstances which warrant them, the Comment to Rule 1.6 must clearly state that a third party's criminal activity accessing clients' information does not negate the responsibility of a lawyer who fails to take reasonable cybersecurity measures on behalf of clients. Comment V to Rule 1.6 may accordingly add that:

> [t]he unauthorized access to information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. However, an unauthorized access to information relating to the representation of a client may constitute a violation of paragraph (c) if the lawyer has not made reasonable efforts to prevent the access, even if a third party accessed the information unlawfully.[145]

4. Disclosure of Cyberattacks and Data Theft to Clients

The Rules do not impose a general duty on lawyers to advise clients when their information has been compromised in a cyberattack, let alone that the law firm was or is under attack.[146] Rule 1.4(a)(3) only requires lawyers to "keep the client reasonably informed about the status of the matter," which Comment 3 explains means advising clients regarding "significant developments affecting the . . . substance of the representation."[147] Yet, as we have seen, because often the identity of the attacker, the nature of the information compromised, and the extent of the damage to the client are unknown, a lawyer may not be in a position to conclude that the cyberattack or data theft constitute "a significant development" as opposed to a mere development, and so Rule 1.4(a)(3) is not triggered. Similarly, the inherent uncertainty often surrounding cyberattacks means that Rule 1.4(b)'s admonition for lawyers to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation"[148] may not be triggered because the impact on the matter at hand may be less than clear to the lawyer.

---

145 For a redline of the proposed revisions to the Rules, see Appendix A.

146 *See supra* Section III.A.

147 MODEL RULES OF PROF'L CONDUCT r. 1.4(a)(3).

148 *Id.* r. 1.4(b).

This prevailing interpretation of Rule 1.4 finds some support in the recent rule amendments regarding cybersecurity. Comment 18 on Rule 1.6 states in relevant part that:

> [w]hether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or *that impose notification requirements upon the loss of, or unauthorized access to, electronic information*, is beyond the scope of these Rules.[149]

Read narrowly, the Comment merely states the obvious, namely, that the Rules never, and do not in the case of cybersecurity, purport to construe "other law" such as state and federal laws that may or may not impose additional duties on lawyers. Yet the Comment may also imply or may be read by some lawyers to suggest that notification requirements to clients upon the loss or unauthorized access to their information are beyond the scope of the Rules.

The better interpretation of Rule 1.4, however, is that it does impose an affirmative duty on lawyers to notify clients when their confidential information has been compromised, even when the consequences and impact of the attacks on clients' information fall short of the "significant development" threshold of Rule 1.4(a)(3) or the duty to explain a matter and the means by which it is to be pursued to a client per 1.4(b). To see why imposing a disclosure duty is warranted, recall that Rule 1.4(a)(3), as construed by Comment 3, does impose a duty on lawyers to advise clients regarding a significant development affecting the representation. The Rule assumes that in most circumstance a lawyer would be able to determine whether a particular development is either significant (and therefore triggers 1.4(a)(3)) or less than significant (such that 1.4(a)(3) is not triggered). Cyberattacks, however, are an example of a circumstance possibly not anticipated by the Rules—one in which inherent uncertainty prevents a lawyer from reasonably concluding whether a development affecting the matter is significant or not. In such a case, lawyers as agents and fiduciaries of clients must err on the side of caution and advise their principals-clients of the development.[150] That is, in the face

---

149 *Id.* r. 1.6 cmt. 18 (emphasis added).

150 Elsewhere, I argue that Rule 1.4 should be revised and/or interpreted to mean that lawyers must advise clients regarding all material developments regarding the representation. *See* Eli Wald, *Taking Attorney-Client Communications (and Therefore Clients) Seriously*, 42 U.S.F. L. REV. 747, 789–91 (2008). Inherent uncertainty regarding cyberattacks may leave lawyers unable to determine whether an attack constitutes a material development affecting the representation. Taking attorney-client communications, and therefore clients, seriously dictates that when faced with such inherent uncertainty, lawyers must err on the side of disclosing more rather than less information relating to

of inherent uncertainty regarding the impact of cyberattacks and whether client information has been compromised, a question arises as to whether clients should know more or less about the development. Because clients are the principals in the attorney-client relationship and lawyers are mere agents-fiduciaries, it appears that in the face of inherent uncertainty, lawyers must err on the side of more, rather than less, disclosure to clients. This interpretation is especially compelling in the context of cyberattacks, in which clients, as opposed to lawyers, would often be in the best position to assess the impact of and respond to cyberattacks.[151]

Acknowledging that in general, lawyers must tell clients more about compromised client information requires detailing when lawyers must communicate with clients—identifying the specific triggering event for disclosure—and how they ought to go about discussing cyberattacks and their consequences with clients. In this regard, the Rules may learn from existing states' personal information data breach notification statutes.[152] For example, California Civil Code section 1798.82(a) states that:

> (a) A person or business . . . that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a [person] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay . . . .[153]

California's statutory notification provision is noteworthy in at least two ways. First, while it imposes a mandatory duty to notify customers,[154] the duty is triggered only when the protected information was or is reasonably believed to have been compromised.[155] The provision, to be clear, does not impose a notification duty when a cybersecurity system storing protected information is under a cyberattack, presumably because such a trigger would reveal little to customers if the system was able to thwart the attack. Rather, notification is mandated either when protected information was compromised, or, in the face of some uncertainty, when it is reasonable to assume that the protected information has been compromised. Second, the statute only requires notification when a person's "*unencrypted* personal

---

the representation to clients. *Id.* at 748–50.

151 *See* Goldberg, *supra* note 25, at 540–41.

152 McNerney & Papadopoulos, *supra* note 12, at 1254–56.

153 CAL. CIV. CODE § 1798.82(a) (West 2016).

154 *Id.* ("shall disclose a breach of the security of the system").

155 *Id.* ("whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person").

information was, or is reasonably believed to have been, acquired by an unauthorized person."[156] That is, because the statute only requires notification when unencrypted information was or is reasonably believed to have been compromised, arguably encryption of the information provides a practical safe harbor and negates the need to disclose a breach.

The statutory experience thus suggests two models the Rules can follow. Akin to California's notification apparatus, a modest revision to the Rules can require disclosure to clients only when a client's confidential information has been or is reasonably believed to have been compromised, and only if the confidential information was not reasonably protected, such that if a lawyer reasonably protects the information (via encryption or otherwise) no disclosure to clients would be mandated. For example, the Rules may be amended to state that:

> A lawyer who stores (or employs a third party provider to store) information related to the representation of a client, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a client, whose unreasonably protected confidential information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.

Such a disclosure provision would naturally follow and complement the above proposals requiring all lawyers to adopt cybersecurity plans for all their clients and to make reasonable efforts to protect clients' confidential information. Lawyers who take these two steps would, practically speaking, have no duty to report to clients when their information has been or is reasonably believed to have been compromised because they would be covered by a safe harbor of reasonableness.

In the alternative, the Rules may adopt the triggering event of the personal information notification statutes—information that was or is reasonably believed to have been compromised—without excusing disclosure to clients even when the lawyer did make reasonable efforts to protect the information. Comment W to Rule 1.4 should read:

> A lawyer who stores (or employs a third party provider to store) information related to the representation of a client, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a client, whose confidential information was, or is reasonably believed to have been, acquired by

---

156 *Id.* (emphasis added).

> an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.[157]

The latter approach appears to be warranted in the context of the attorney-client relationship. When a client's confidential information was or is reasonably believed to have been compromised, clients must be advised, even if the lawyer did make reasonable efforts to protect the information. One might argue that when a lawyer has made reasonable efforts to protect the information, imposing a mandatory duty on lawyers to advise clients that their information was, or is, reasonably believed to have been compromised is likely to be ineffective—burdening the client with irrelevant information, with possible distinct adverse consequences, such as chilling or eroding the attorney-client relationship. Put differently, would not mandating adoption of cybersecurity plans and spelling out reasonable efforts be enough? If these provisions end up ensuring reasonable conduct by lawyers, why force disclosure and risk clients developing "notice fatigue"? Would not clients be content with lawyers' adoption of reasonable efforts? If nothing else could have been reasonably done by lawyers, why tire the clients with additional disclosures?

These objections, however, must be rejected for three related reasons. First, they smack of lawyers' self-interest at the expense of clients, the very concern about and criticism of the Rules to which lawyers ought to be sensitive.[158] No doubt, reporting to a client that the client's confidential information was or is reasonably believed to have been compromised is likely to be awkward to the lawyer,[159] but that is not in and of itself a legitimate ground a lawyer should be able to invoke to avoid disclosing information to the client.

Second, recall that this Article advocates a revision to the Comment to Rule 1.6, pursuant to which "a lawyer must adopt reasonable procedures . . . appropriate for the size and type of firm and practice, to protect a client's information," including reasonable cybersecurity procedures.[160] With such a cybersecurity plan in place, a lawyer's communication to a client regarding a breach and compromised information following a cyberattack is

---

157 For a redline of the proposed revisions to the Rules, see Appendix A, proposed Comment W to Rule 1.4.

158 *See supra* notes 45–46 and accompanying text.

159 Recall that if a cyberattack has in fact resulted in disclosure of a client's material confidential information, then even a traditional reading of 1.4(a)(3) and 1.4(b) will mandate disclosure to the client. *See* MODEL RULES OF PROF'L CONDUCT r. 1.4(a)(3), 1.4(b) (AM. BAR ASS'N 2013).

160 *See supra* note 123 and accompanying text.

unlikely to chill the attorney-client relationship, because a lawyer would be able to cheaply and effectively explain to the client the reasonable efforts the law firm made to protect the client's information, and the inherent uncertainty surrounding the cyberattack, notwithstanding the reasonable security measures undertaken. Indeed, it is the current state of technology that prevents lawyers (and others) from stopping all cyberattacks and reasonable clients should be able to understand and accept a lawyer's reasonable conduct in the face of technological limitations and uncertainty.

Finally, any interpretation second-guessing disclosing information to clients when confidential information was or is reasonably believed to have been compromised on the ground that clients may not understand it or will be fatigued smacks of lawyers' paternalism vis-à-vis clients, inappropriate in the attorney-client relationship.[161] As I explain elsewhere, "for lawyers to assume that clients are unable to comprehend and appreciate the consequences and meaning of complex . . . information, even when offered a detailed explanation . . . would constitute unacceptable paternalistic withholding of material information."[162] The U.S. Supreme Court, in its landmark decision, *Basic, Inc. v. Levinson*,[163] construed the term "material" in securities law. It held that to address inherent uncertainty by not disclosing material information to clients amounts to assuming that clients are

> nitwits, unable to appreciate—even when told—that [cybersecurity measures] are risky propositions . . . . Disclosure, and not paternalistic withholding of accurate information, is the [desirable] policy . . . . The role of the materiality requirement is not to 'attribute to [clients] a child-like simplicity, an inability to grasp the probabilistic significance of [cybersecurity measures]' . . . but to filter out essentially useless information that a reasonable [client] would not consider significant, even as part of a larger 'mix' of factors to consider in making his . . . decision[164]

regarding the attorney-client relationship.

Moreover, fatigue assumes that clients would know and may not care or become indifferent about security breaches. Yet the assumption seems inapplicable here. Currently, clients do not usually learn about, and are unlikely to be indifferent about breaches regarding their confidential information. For the same reason, mandating disclosure to clients only when the unauthorized access of confidential information is likely to have a

---

161 MODEL RULES OF PROF'L CONDUCT r. 1.2(a).
162 Wald, *supra* note 150, at 795.
163 Basic Inc. v. Levinson, 485 U.S. 224 (1988).
164 *Id.* at 234; *see also* Wald, *supra* note 150, at 795–96.

prejudicial impact on their representation would not suffice. Just as the inherent uncertainty surrounding cyberattacks often precludes lawyers from concluding that a breach of confidential information constitutes a "significant development" mandating disclosure to clients, the same uncertainty will likely prevent lawyers from concluding that a breach has a prejudicial impact on clients' representation. Because a reasonable client would like to know when her confidential information was, or is, reasonably believed to have been accessed by an unauthorized party, a lawyer must disclose accordingly.

Mandating disclosure to clients when confidential information was, or is, reasonably believed to have been compromised has one additional important benefit. Disclosure would, in turn, enable clients to sanction lawyers who fail to put in place "reasonable efforts" to protect their confidential information and reward lawyers who do make reasonable efforts to protect confidential information. Put differently, the adoption of a rule of professional conduct mandating disclosure of cybersecurity information to clients would allow clients to exercise market controls over lawyers, further addressing the underregulation of lawyers' cybersecurity conduct. Finally, even if lawyers do make reasonable efforts to protect confidential information, a disclosure duty would result in more conversations with clients about cybersecurity, allowing clients to participate on an informed basis regarding the cyber means by which their objectives are to be pursued.

CONCLUSION

The inherent uncertainty often surrounding cyberattacks on law firms—who specifically perpetrated the attack, what information was stolen or compromised, and what damage, if any, did a client suffer as a result of the attack—renders liability rules, such as malpractice suits, and market controls, such as being fired by a client, ineffective in regulating lawyers' cybersecurity conduct. The Rules thus have an opportunity to play a meaningful role in informing and guiding the conduct of underregulated lawyers, by requiring lawyers to adopt and implement cybersecurity plans for all clients, defining the meaning of "reasonable efforts" necessary to prevent the unauthorized disclosure or access to information relating to the representation of a client, and by mandating disclosure to clients when their confidential information was, or is, reasonably believed to have been accessed by an unauthorized party.

Appendix A: Proposed Revisions to the Rules

Proposed revisions to the Rules are italicized.

Comment on Rule 1.6

Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

[X] To competently safeguard information relating to the representation of a client against unauthorized access by third parties, a lawyer must adopt reasonable procedures, including reasonable cybersecurity measures, appropriate for the size and type of firm and practice, to protect a client's confidential information. Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule.

The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

[Y] Reasonable efforts to prevent the inadvertent or unauthorized disclosure of information relating to the representation of a client would normally include robust strategies for identifying, prioritizing, and securing valuable information; periodical inspection of the firm's information storage system for signs of cyberattacks and data theft; the use of basic cybersecurity measures, including the use of current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords updated from time to time, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents; and the adoption of cybersecurity training protocols for firm lawyers and staff. See Rule 5.1 and 5.3.

Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing

additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

[Z] Whether a lawyer may be required to take additional special security measures to safeguard a client's information, above and beyond basic cybersecurity measures, depends on the circumstances. For example, a lawyer may be required to take special security measures to protect sensitive information related to the representation of a client.

A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules, *but see Rule 1.4, Comment [U].* For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy.

[U] Special security measures may include encryption of attorney-client communications or password-protecting information relating to the representation of a client on the lawyer's or law firm's information storage system.

Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws

that govern data privacy, is beyond the scope of these Rules, *but see Rule 1.4, Comment [3].*

[V] The unauthorized access to information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. However, an unauthorized access to information relating to the representation of a client may constitute a violation of paragraph (c) if the lawyer has not made reasonable efforts to prevent the access, even if a third party accessed the information unlawfully.

Comment on Rule 1.4

Communicating with Client

[3] Paragraph (a)(2) requires the lawyer to reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations — depending on both the importance of the action under consideration and the feasibility of consulting with the client — this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[W] A lawyer who stores (or employs a third party provider to store) *information related to the representation of a client, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a client, whose confidential information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.*

We Should Not Rely on Commercial Bar Reviews to Do Our Job: Why Labor-Intensive Comprehensive Bar Examination Preparation Can and Should Be a Part of the Law School Mission

*Mario W. Mainero**

ABSTRACT

Increasingly, law school bar passage rates are an important concern for faculty and administration, as well as students. The July 2014 and July 2015 bar exams saw a precipitous drop nationally in bar passage rates, including declines ranging from four to over twenty percentage points. At the same time, there have been declines in applications to law schools, declines in admissions statistics (LSAT and undergraduate GPA), and an empirically demonstrable decline in student preparedness for law school. The confluence of these events portends even greater declines in bar passage if law schools do not rethink how they prepare students for the bar exam. This Article examines developments in academic support and bar preparation programs with an eye toward suggesting models for effective in-house bar preparation programs. Specifically, this Article examines: (1) the evolution of academic support programs in law schools to include bar passage programs, with a brief description of the types of programs that traditionally have been available; (2) the particular difficulty posed by the California Bar Exam; (3) the existing types of supplemental programs, and concerns posed by programs that are limited to "bar tips" or even limited practice exams or substantive lectures, given the increased numbers of "at risk" students due to the increase in underpreparedness; (4) the supplemental program at Chapman University's Fowler School of Law, including the intensity of effort required of both faculty and

* Professor of Academic Achievement and Director of Bar Services, Chapman University Dale E. Fowler School of Law. I wish to express my deep gratitude to Dean Tom Campbell and Associate Dean Donald Kochan for their tireless efforts in editing and making suggestions for improving this Article. I particularly owe a tremendous debt to Research Librarian Sherry Leysen, without whose research, data mining, and work on formatting, footnotes, and general editing I could not have even contemplated writing this Article.

students in a comprehensive program applicable to all students; and finally, (5) the bar passage results at Chapman University's Fowler School of Law since adoption of a comprehensive supplemental bar passage program, that have been significantly better than would be expected by some commentators, given its ranking and relative youth as a law school. This Article suggests that the traditional focus of academic support programs, including bar preparation programs, that focus largely on perceived "at risk" students, is insufficient in light of the increased numbers of underprepared students. In order to avoid further calamitous declines in bar passage rates, law schools will have to move from traditional academic support models to models that encourage the entire cohort of students to work together, cooperatively, and that apply extensive time and effort to ensure that all students receive the benefit of these programs.

Table of Contents

INTRODUCTION

Recent drops in bar passage rates throughout the country have raised an alarm. As the *Wall Street Journal*'s Law Blog put it, "[a] steep decline in bar exam scores on the most recent test has led to an outbreak of finger-pointing over who's to blame for the downward swing."[1] But this "steep decline," ranging from five percentage points in New York[2] to seven percentage points among ABA-accredited law schools in California,[3] to over twenty percentage points in Montana,[4] raises far more important questions than who is to blame. How should law schools and law school faculties approach the topic of bar passage? Should bar passage be considered something students engage in after graduation, and thus not the concern of a law school administration or faculty? Should the law school curriculum be adapted to conform to topics tested on the bar examination? Should law schools dedicate considerable resources to in-house bar preparation programs, or continue to leave bar preparation largely to commercial reviews? This Article does not seek to answer all of these questions, but in light of this steep decline in bar passage and the decline in both admissions and admissions statistics going forward, it does propose that law schools should adopt comprehensive, labor-intensive, in-house bar preparation programs aimed at all students, rather than leave bar preparation solely to commercial bar reviews or administer limited, targeted programs aimed only at "at risk" students. It also invites a discussion in which others at law schools around the country who work with students on bar preparation might wish to participate.

In an era of declining applications and declining qualifications of applicants,[5] law schools face significant pressures,

---

1 Jacob Gershman, *Decline in Bar Exam Scores Sparks War of Words*, WALL ST. J.: L. BLOG (Nov. 10, 2014, 6:45 PM), http://blogs.wsj.com/law/2014/11/10/decline-in-bar-exam-scores-sparks-war-of-words/ [http://perma.cc/UM23-JESD].

2 Tania Karas, *Deans Dismayed by Declines in Bar-Pass Rates*, N.Y. L.J. (Nov. 13, 2014), http://www.newyorklawjournal.com/id=1202676229642/Deans-Dismayed-by-Declines-in-BarPass-Rates.

3 Don J. DeBenedictis, *State's Bar Passage Rate Plummets, Tracking National Trend*, DAILY J., Nov. 25, 2014, at 1, 1.

4 Jessica Mayrer, *University of Montana Bar Scores Drop*, MISSOULA INDEP. (Oct. 9, 2014), http://missoulanews.bigskypress.com/missoula/university-of-montana/Content?oid=2093254 [http://perma.cc/M22Q-Y88E].

5 Martha Neil, *Law School Applications Down 37% Since 2010; First Year Class Could Be Smallest in 40 Years*, A.B.A. J. (July 22, 2014, 8:25 PM), http://www.abajournal.com/news/article/law_school_applications_down_8_percent_new_lsac_survey_shows_theyve_dropped [http://perma.cc/54EX-NYFZ]; *see also* Keith Lee, *Top University Students Avoiding Law School—2014 Edition (Statistics and Graphs)*, ASSOCIATE'S MIND (Mar. 5, 2014), http://associatesmind.com/2014/03/05/top-university-students-avoiding-law-school-2014-edition-statistics-graphs/ [http://perma.cc/8UQV-KG6P].

including the pressure to maintain adequate bar passage rates. It is the thesis of this Article that, in most states, with declining admissions statistics and significant student underpreparedness for law school, law schools should resist relying on commercial bar review companies to provide the sole resource for bar preparation and institute a supplemental in-house bar preparation program with several characteristics.[6] The program must be available and open to all students. To that end, it should encourage students to be part of a cohesive group all focused on the same goal of bar passage, and it must not differentiate among students based on perceived "risk" or other factors. The program must be highly labor-intensive, so that faculty must demand extensive practice and work by students, and at the same time, faculty must also be prepared to expend considerable time and effort to meet students' needs. Bar preparation faculty must provide opportunities for prompt feedback on twenty to thirty-five essays per student, in addition to group classes and availability for one-on-one tutoring. In sum, faculty teaching bar preparation must be prepared to expend whatever time it reasonably takes to prepare each class of students, and all members of the class, for the bar examination. This is something that cannot be left to commercial bar review companies. As one researcher has put it, "bar exam study requires more work than a full-time job."[7] But just as bar exam study requires more work than a full-time job, bar exam preparation and teaching also requires more work than a full-time job.

Recent adoption of ABA accreditation standards and the interpretations of those standards set objective measures for bar passage.[8] These measures alternatively include a requirement that: (1) for students who graduated within the five most recently completed years, 75% of those sitting for a bar examination must pass a bar examination over that five-year period, or 75% must pass the bar exam in three of the past five years; or (2) in three of the five most recent calendar years, the first time taker bar passage rate must be not less than fifteen percentage points below the average for all first-time takers from ABA-approved

---

6 First and foremost, of course, students should be focused on general studies in the law and learning through a law school's normal curriculum. This Article is not focused on changing that curriculum, but on why, in addition, law schools should offer in-house bar preparation programs.

7 Denise Riebe, *A Bar Review for Law Schools: Getting Students on Board to Pass Their Bar Exams*, 45 BRANDEIS L.J. 269, 307 (2007).

8 ABA STANDARDS AND RULES OF PROCEDURE FOR APPROVAL OF LAW SCHOOLS 2013–2014 Standard 301(a) (AM. BAR ASS'N 2013), http://www.americanbar.org/content/dam/aba/publications/misc/legal_education/Standards/2013_2014_standards_chapter3.authcheckdam.pdf [http://perma.cc/T6WE-8VZJ]; *id.* Interpretation 301-6.

law schools in the jurisdiction.[9] In February 2016, the Section of Legal Education and Admission to the Bar's Standards Review Committee approved a further revision of these standards, proposing to amend Standard 316 to clarify and tighten the standard for bar passage to read as follows: "(a) At least 75 percent of a law school's graduates in a calendar year who sat for a bar examination must have passed a bar examination within two years of their date of graduation."[10] While there are further standards to show good cause in progressing toward the meeting of this "one size fits all" standard, the adoption of the clarified standard, reducing the time within a law school must see 75% of its students pass the bar exam, makes the need to improve bar passage rates imperative—it will have a direct effect on accreditation.[11] Given the adoption of these standards, it is no surprise that law schools are adopting programs to improve bar passage.

While some recent publications have identified a growing trend in law schools to offer bar preparation programs,[12] none has analyzed in substantial depth what component parts a program should include to be effective. None has done so in view of what appears to be a steep decline in student preparedness for law school, combined with the decline in admissions statistics.[13]

To illustrate what the accreditation standards and interpretations really mean for both law students and law faculty presenting bar preparation programs to their students, this Article focuses on the difficult California Bar Examination—its components, the challenges it poses for applicants, and how to help students achieve success. It also examines the few types of supplemental bar preparation programs currently offered by some law schools. Finally, it examines the supplemental in-house bar preparation program at the author's law school. For the last five years, that law school—Chapman University's Fowler School of Law—has been recognized by more than one author as having

---

9 *Id.* Interpretation 301-6.

10 AM. BAR ASS'N, STANDARDS REVIEW COMMITTEE 40 (2016), http://www.americanbar.org/content/dam/aba/administrative/legal_education_and_admissions_to_the_bar/standards_review/2016_02_src_meeting_materials.authcheckdam.pdf [http://perma.cc/T47K-GWVK].

11 *Id.*

12 *See, e.g.*, Aleatra P. Williams, *The Role of Bar Preparation Programs in the Current Legal Education Crisis*, 59 WAYNE L. REV. 383 (2013).

13 Rebecca Flanagan, *The Kids Aren't Alright: Rethinking the Law Student Skills Deficit*, 2015 BYU EDUC. & L.J. 135, *passim* (2015). This article is significant because it neatly summarizes important data and observations suggesting the decline in student preparedness for law school, which then poses a challenge in eventually preparing students for the bar examination.

outperformed its predictors and rankings in terms of bar passage.[14]

This Article consists of five parts. Part I will briefly discuss the evolution of academic support programs in law schools to include bar preparation programs, with a brief description of the types of programs that traditionally have been available. Part II will examine the particular difficulty posed by the California Bar Exam. Part III will survey in greater specificity the existing types of supplemental programs and explain why programs that are limited to "bar tips," or even limited practice exams or substantive lectures, are not sufficient in states with a relatively low bar passage rate, given the increased numbers of "at risk" students. Part IV will describe the supplemental program at Chapman University's Fowler School of Law, and demonstrate the intensity of effort required of both faculty and students in such a comprehensive program. Finally, Part V will show that the bar passage results at Chapman University's Fowler School of Law since adoption of a comprehensive supplemental bar passage program have been significantly better than would be expected by some commentators, given its ranking and relative youth as a law school.

I. LAW SCHOOL ACADEMIC SUPPORT AND BAR PASSAGE

Bar passage is one facet of the general discipline of academic support in law school. Thus, to understand the development of bar preparation programs, it is first important to briefly review the development of law school academic support programs. Since the advent of law school academic support programs, most programs have focused on mitigating the disadvantages "nontraditional" students face in law schools.[15] Thus, "traditional academic support programs were designed to help a limited, discrete group of students for a limited time."[16] Eventually, these programs transformed into two types, which often were merged: programs designed to provide assistance to non-traditional students, and programs for students who were deemed, due to demonstrated academic difficulty or lower admissions predictors, to face the risk of academic dismissal.[17]

---

14 Donald J. Smythe, Ranking Law Schools Using Reported California Bar Exam Results: Some Observations and Conjectures 7, 22 (June 10, 2012) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2085048; Paul Caron, *July 2013 California Bar Exam Results*, TAXPROF BLOG (Jan. 25, 2014), http://taxprof.typepad.com/taxprof_blog/2014/01/july-2013.html [http://perma.cc/T93M-982X].

15 Kristine S. Knaplund & Richard H. Sander, *The Art and Science of Academic Support*, 45 J. LEGAL EDUC. 157, 158–59 (1995).

16 Flanagan, *supra* note 13, at 171.

17 *Id.* at 172–74

A. Impact of Labor-Intensiveness of Work and Decline in Student Preparedness on Academic Support Programs

In light of the extensive work this Article proposes in order to generate successful bar preparation programs, it should be noted that a concern expressed by some academic support professionals, such as Professor Flanagan in her article, is that the labor-intensive nature of academic support, which requires significant one-on-one counseling and review,[18] is not well-suited to an expanding population of students served by academic support. For example, when I previously taught as the Director of Academic Support at another institution, each individual meeting with a student took one half-hour—so if just fifty students were in need of academic support in a class of 200, for example, those meetings alone occupied twenty-five hours out of a week—without including the time to review each student's written essays, outlines, or other work product.

Furthermore, the number of students underprepared to enter law school has increased dramatically.[19] Professor Flanagan ably tracks this increased underpreparedness in her recent article.[20] She tracks the work of Richard Arum and Josipa Roksa in their publication, *Academically Adrift: Limited Learning on College Campuses*,[21] and reports that, based on the Collegiate Learning Assessment ("CLA"), a test of "broad competencies" that should be developed in college—such as critical thinking, analytical reasoning, problem solving, and writing—45% of the students studied achieved no significant gains in these competencies by the end of the sophomore year of college.[22] This point in time was critical because, as Professor Flanagan writes, "previous studies have found that roughly 63% of the change in critical thinking skills occurs by the sophomore year."[23] Similarly, Professor Flanagan writes, the Wabash National Study of Liberal Arts Education found that "students made no measurable improvement in critical thinking skills during the first year of college, and thirty percent of students showed no growth or a decline in critical thinking skills after four years of college."[24]

---

18 *Id.* at 174.

19 *Id.* at 171 ("The empirical research suggests many students entering law school are unaccustomed to the amount of studying necessary for law school success; do not have the critical thinking and analytical reasoning skills that provide the foundation for 'thinking like a lawyer,' and expect grades above a 3.3.").

20 *Id.*

21 RICHARD ARUM & JOSIPA ROKSA, ACADEMICALLY ADRIFT: LIMITED LEARNING ON COLLEGE CAMPUSES (2011).

22 *Id.* at 36; Flanagan, *supra* note 13, at 140–41.

23 Flanagan, *supra* note 13, at 141.

24 *Id.*

One of the most compelling observations identified by Professor Flanagan is also more direct evidence of a decline in student preparedness. From 1961 to 2003, the percentage of college students studying twenty hours or more per week outside of class declined from 67% of students to 20% of students.[25] This represented a decline of about ten hours per week in average study time.[26] I believe that these data compel the conclusion that students have declined in their possession of the necessary skills, and perhaps work ethic, to succeed in law school.

Between the lack of increase in critical skills during college for a significant segment of the college student population, and the dramatic decrease in time and effort expended in studying, it is no surprise that students are far less prepared for law school than was true two generations ago.

This increase in underprepared students matriculating in law schools poses particular problems for academic support and, ultimately, bar passage. In law schools that have seen an increase in students underprepared to begin law school, there is an increased need for academic support to assist those students in quickly developing the necessary skills to academically succeed in law school. However, often due to lack of resources to fund enough instructors to meet the individualized needs of an increasing number of underprepared students, "[traditional academic support is] ill equipped to provide the necessary instruction and support to the large number of academically underprepared students matriculating at law schools."[27]

B. Expansion of Academic Support Programs to Include Bar Preparation

But, even as academic support programs have faced a strain on resources in preparing entering law students, academic support programs also have expanded to address a further issue beyond just law school performance: performance on the bar examination. In response to a 2002 survey by the Association of American Law Schools ("AALS"), 38.9% of all responding ABA-accredited law schools stated that they provided or sponsored activities, programs, or courses designed to enhance bar examination performance; 38.7% of all responding ABA-accredited law schools stated that they provided or sponsored activities, programs, or courses not specifically designed to enhance bar examination performance, but which

25 *Id.* at 152.
26 *Id.*
27 *Id.* at 176.

they believed enhanced such performance.[28] While there has been little published empirical data on whether bar preparation programs increase performance, the data that have been published suggest that such programs do increase bar exam passage rates over previous levels.[29]

As discussed above, academic support is labor-intensive and, thus, requires significant resources. Expanding academic support to bar passage programs is an even greater challenge to a law school's resources. As the number of underprepared law students—for whom undergraduate education has been less one of intellectual rigor and more like a "four-year vacation"—continues to grow,[30] law schools should make their bar preparation programs available to their entire student body. One reason to do so is to maintain cohesiveness of the cohort and a mutually supportive atmosphere among all the students.[31] Furthermore, if law schools indeed lack the increased resources to support additional instructors, as Professor Flanagan suggests,[32] academic support professionals may have to simply work more and harder, if necessary, to deliver these programs at an effective level. If academic support professionals need to work more and harder to deliver these bar preparation programs, then they should consider what kinds of programs are most effective.

Despite the demonstrated need for bar preparation programs, little has been done to survey their existence or formats. The 2002 survey by the AALS provided very little in terms of specific descriptions of the nature or content of such programs or activities, except to conform them to four general categories: (1) supplemental programs designed and administered by the law school; (2) programs offered in partnership with commercial bar reviews; (3) bar exam strategies lectures; and (4) individual mentoring and counseling programs.[33]

The survey describes supplemental programs only briefly as "multisession programs during spring semester of the third year," with "typical components" such as lectures in substantive law, sample multiple choice questions, "essay-writing instruction and practice," and advice on time management and

---

28 Comm. on Bar Admissions & Lawyer Performance & Richard A. White, *AALS Survey of Law Schools on Programs and Courses Designed to Enhance Bar Examination Performance*, 52 J. LEGAL EDUC. 453, 457 (2002) [hereinafter *AALS Survey*].

29 Linda Jellum & Emmeline Paulette Reeves, *Cool Data on a Hot Issue: Empirical Evidence that a Law School Bar Support Program Enhances Bar Performance*, 5 NEV. L.J. 646 (2005).

30 Flanagan, *supra* note 13, at 171.

31 *See infra* Part III.

32 Flanagan, *supra* note 13, at 174.

33 *AALS Survey*, *supra* note 28, at 461.

outlining.[34] This broad definition tells little about the substance of these programs. It does not evaluate particular programs or their components, or critique those programs for their effectiveness or ineffectiveness. Consequently, those of us interested in designing workable bar preparation programs received little, if any, guidance from this survey.

In the context of the third year of law school, when students are still taking substantive classes, or spending significant time on externships, clinics, or similar work, "supplemental" can often mean nothing more than a few weekend sessions, or perhaps one class of several sessions. As a consequence, at some law schools, the bulk of bar exam preparation has traditionally been left to the commercial bar review companies.[35] Not surprisingly, these companies have proliferated,[36] but as the title of this Article suggests, this is not necessarily the best outcome for students.

Students certainly have choices. As of January 2014, the number of commercial bar preparation resources, reviews, and services was extensive and expensive. There were at least sixteen different bar review courses, three other "tutoring" services, and countless other books and study materials, all costing law students anywhere from $500 for online MBE products to $7500 for full-service bar review programs.[37]

It is my experience, however, that commercial reviews, while valuable, have their limitations, and vary in services, quality, and format. Those that, in essence, *require students to attend* either live sessions or videos and *monitor* students' attendance and progress are more effective than online applications. Given that students enter law school underprepared, it is my experience that they do not exit law school as expert learners who can be trusted to adequately self-teach using technological aids and online reviews.

The traditional commercial bar review companies such as BarBri have their limitations. For example, in California, which saw 6080, 6485, and 6635 applicants take the July 2011, 2012, and 2013 general bar exams, respectively,[38] commercial bar reviews simply are not able to provide much individualized service or feedback. BarBri's Paced Program assigned only six, eight, six, and five essays that students could turn in to BarBri

---

34 *Id.*

35 Williams, *supra* note 12, at 395.

36 *See infra* Part III.

37 *Guide to Bar Review Courses*, NAT'L JURIST (Jan. 17, 2014), http://www.nationaljurist.com/content/guide-bar-review-courses [http://perma.cc/GL86-C9DZ].

38 *See Statistics*, STATE BAR OF CAL., http://admissions.calbar.ca.gov/Examinations/Statistics.aspx (last visited Feb. 29, 2016).

for grading in July 2011, 2012, 2013, and 2014, respectively.[39] But there are thirteen possible essay subjects on the California Bar Exam,[40] so students taking BarBri will not, due to resource limitations, receive specific essay feedback, beyond the helpful general essay approach, in a number of subjects. Much of the time, then, students must rely on "self-checking" their work, which is an unreliable means of feedback, since students are not likely to be well-qualified at evaluating their own work, even if they use a "model answer" or other rubric to compare to their work.

Underprepared students require monitoring, often in the form of one-on-one counseling, "to determine the source of their academic challenge and frequently require additional meetings to ameliorate academic deficiencies."[41] But, as discussed briefly, commercial bar review companies, who sell their product to thousands of students, do not monitor students in order to ensure that those students are doing the work.

Only law school faculty administering an intensive bar preparation program, who have already developed a personal relationship with their students, can deliver the intensive, direct, and personalized feedback needed to compensate for the underpreparedness of students facing a bar examination. The increase in underprepared students—together with a decline in predictors of likelihood of academic success and bar passage by law school matriculants, which tends to result from a decline in applications—likely means that only a program that is committed to serving all of a law school's graduates with such an intensive and personalized program can make up for the deficiencies of commercial bar reviews and be successful.

As Professor Flanagan has noted, students enter law school with a consumer mentality, focusing "on the end product of the transaction—a satisfactory grade—instead of the process of learning and gaining knowledge."[42] But by the time those students graduate from law school, their focus is on a different end product—bar passage. Law schools should work to adequately develop learning and critical thinking skills in students during law school, and avoid over-reliance on commercial bar reviews whose cookie-cutter approaches simply cannot suffice, particularly in states and for students of schools where bar passage is problematic.

---

39 On file with the author.

40 STATE BAR OF CAL., COMM. OF BAR EXAM'RS/OFFICE OF ADMISSIONS, SCOPE OF THE CALIFORNIA BAR EXAMINATION 1 (2015), http://admissions.calbar.ca.gov/Portals/4/documents/gbx/BXScope_R.pdf [http://perma.cc/K6BQ-RCF9].

41 Flanagan, *supra* note 13, at 174.

42 *Id.* at 155.

Given that a law school faculty-administered intensive bar preparation program is needed to adequately monitor and assist the increasing number of underprepared law students in preparing for the bar examination, the remainder of this Article will explore the difficulty of bar passage in California and examine the amount of labor it takes to implement a successful in-house supplemental bar preparation program—one that exceeds expectations in terms of student performance. The focus on California is appropriate precisely because of the unusual difficulty of bar passage in that state. If particular methodologies of bar preparation programs can work there, they can certainly work for law schools and students in states with a much less daunting pass rate issue than California.

II. BAR PASSAGE IN CALIFORNIA

The California Bar Examination is generally acknowledged as one of the most difficult bar examinations in the country. It is one of the most difficult based on its three-day format, the length of its written portions, and the kinds of scores needed to pass. This Part focuses on the California experience as a prime example of why there is a need for in-house intensive bar preparation programs, in large part because of the student underpreparedness discussed above.

The California Bar Examination consists of six one-hour essays, two three-hour performance tests, and the Multistate Bar Examination ("MBE").[43] The essays may be from among thirteen different subjects: Business Associations, Federal and California Civil Procedure, Community Property, Constitutional Law, Contracts and Sales, Criminal Law and Procedure, Federal and California Evidence, Professional Responsibility, Real Property, Remedies, Torts, Trusts, and Wills and Succession.[44]

The California Bar Examination is longer than in most states—three days.[45] Moreover, unlike many states, such as those that use the Uniform Bar Examination ("UBE"),[46] essays

---

43 STATE BAR OF CAL., COMM. OF BAR EXAM'RS/OFFICE OF ADMISSIONS, *supra* note 40.

44 *Id.*

45 Only seven states conduct a three-day bar exam: California, Delaware, Louisiana, Nevada, Ohio, South Carolina, and Texas. Forty-three states and the District of Columbia conduct two-day bar exams. Information on file with author. Due to cost considerations, the California Bar Exam is moving to a two-day exam beginning in July 2017, as recently approved by the California Supreme Court. The format will be revised to include five one-hour essays, one 90-minute performance test, and the MBE. Thus, the significant differences will be that the MBE will now count for 50% of the score, rather than 35%, and the performance test will be a small part of the exam—equivalent to two essays, and thus, worth about 14.3% of the total score, rather than the current 26% of the total score.

46 Twenty states use the UBE: Alabama, Alaska, Arizona, Colorado, Idaho, Iowa, Kansas, Minnesota, Missouri, Montana, Nebraska, New Hampshire, New Mexico, New

and performance tests in California are much longer. The UBE utilizes the Multistate Essay Exam—six 30-minute essays,[47] and two Multistate Performance Exams, each of which is 90 minutes in length.[48] Many other jurisdictions also use essays of 30–40 minutes. For example, the New York Bar Examiners recommend that applicants take 40 minutes to answer each individual essay.[49] Texas Bar Exam essays are 30 minutes in length.[50] California, in contrast, requires six 60-minute essays, and two 180-minute performance tests.[51]

As a consequence of the structure and length of the California Bar Examination, California applicants are required to know a broader scope of material, and in greater depth. Longer essays allow for a greater exploration of material that, because it is not as intensively covered in a traditional law school curriculum, is less often previously tested during a student's law school years. Thus, instead of knowing one or two general rules, as is often the case on a 30-minute essay, students taking a 60-minute essay must often know several rules, exceptions, and often are faced with "crossover" questions that test multiple subjects. The July 2013 Bar Examination included an essay question that raised the scope of the Thirteenth Amendment,[52] and the February 2014 Bar Examination included an essay question that raised the scope of lateral support[53]—neither of which are typically tested law school essay subjects. California exams have also tested Professional Responsibility as a "crossover" topic with subjects ranging from Corporations to Community Property. The length, depth, and breadth of coverage in 60-minute essays poses a particularly difficult challenge to bar applicants.

York, North Dakota, South Carolina, Utah, Vermont, Washington, and Wyoming. *See Jurisdictions That Have Adopted the UBE*, NAT'L CONF. B. EXAMINERS, http://www.ncbex.org/about-ncbe-exams/ube/ [http://perma.cc/G7HS-ZX3M].

47 *Jurisdictions Administering the MEE*, NAT'L CONF. B. EXAMINERS, http://www.ncbex.org/exams/mee/ [http://perma.cc/9XJB-MT3B].

48 *Jurisdictions Administering the MPT*, NAT'L CONF. B. EXAMINERS, http://www.ncbex.org/exams/mpt/ [http://perma.cc/2GJT-J48M].

49 *The New York State Bar Examination*, N.Y. ST. BOARD L. EXAMINERS, http://www.nybarexam.org/TheBar/TheBar.htm [http://perma.cc/BK4Z-Q5SA].

50 *Texas Bar Examination Scoring and Weighting*, TEX. BOARD L. EXAMINERS, http://www.ble.state.tx.us/ExaminationInfoPage/Grading%20Explanation%20as%20of%201-11-08_pdf.pdf [http://perma.cc/GB3T-EXYX].

51 STATE BAR OF CAL., COMM. OF BAR EXAM'RS/OFFICE OF ADMISSIONS, *supra* note 40.

52 *See* STATE BAR OF CAL., CALIFORNIA BAR EXAMINATION 3 (July 2013), http://admissions.calbar.ca.gov/Portals/4/documents/gbx/July2013-CBX_Questions_R.pdf [http://perma.cc/7VU9-9EJX].

53 *See* STATE BAR OF CAL., CALIFORNIA BAR EXAMINATION 43 (Feb. 2014), http://admissions.calbar.ca.gov/Portals/4/documents/gbx/February2014_CBX_Essays_PTs.pdf [http://perma.cc/L397-NZAE].

Even more than just the qualitative difference in length of the administration and the writing portions of the California Bar Examination, the raw performance numbers illustrate the difficulty of bar passage in California. The State Bar of California publishes the bar passage numbers, both raw numbers and percentages, for each individual law school, and all references herein to those rates and numbers were compiled by me from the California State Bar website.[54] The following table illustrates the July bar examination first-time taker pass rates on the California Bar Examination of California ABA-accredited law schools, non-California ABA-accredited law schools, and California non-ABA-accredited law schools over the past eight years.

Year	California ABA	Non-California ABA	California Non-ABA
2007	76%	67%	30%
2008	83%	75%	35%
2009	79%	69%	31%
2010	75%	68%	34%
2011	76%	66%	32%
2012	77%	64%	29%
2013	76%	64%	32%
2014	69%	60%	33%
2015	68%	59%	21%

Almost no other state consistently passes only about two-thirds of out of state ABA-school graduates, and only about three-fourths of in-state ABA graduates.[55] These percentages, except for the recent drop on the July 2014 Bar Examination, represent an increase from the past. "During the 1980s, the [California] statewide pass rate averaged . . . about 67 percent for first-time takers from ABA-accredited schools [in-state and out of state]."[56]

One reason for the low pass rate in California is the "cut score." The cut score is the minimum passing score. In California, that score is a scaled 144 out of 200 on the MBE, which is the second highest in the country, second only to Delaware at 145. The average nationwide scaled cut score on the MBE is 135.1, and the median nationwide cut score for the July 2013 bar exam

54 The website from which all such statistics were obtained is the Bar Examination Statistics portion of the State Bar of California website, found at http://admissions.calbar.ca.gov/Examinations/Statistics.aspx. Within the "Statistics" portion of the web page, the State Bar publishes statistics by test administration.

55 *See 2011 Statistics*, B. EXAM'R, March 2012, http://www.ncbex.org/dmsdocument/146 [http://perma.cc/B538-TUTZ] (last updated Apr. 9, 2012).

56 Knaplund & Sander, *supra* note 15, at 200.

was 135.[57] Because the cut score is scaled, or curved, that difference of nine between California's cut score and the national mean and median cut scores can represent up to a difference of eleven correct questions needed to pass.[58] At least one analysis has concluded that an increase of one point in cut score translates generally to a 1.2% decrease in bar passage rate.[59]

Given that the national median and average cut scores are about ten below that of California, this means that California's pass rate will be up to twelve percentage points below the average pass rate in the rest of the country, putting California law students at a general disadvantage in passing the bar exam that is greater than their counterparts nationwide. Thus, while law students' decline in preparedness nationally puts them at greater risk for failing the bar exam, that risk is heightened significantly by the cut score, as reflected by the much lower pass rates in California.

As Professor Flanagan notes, the most selective law schools are the recipients of the most academically prepared students.[60] Students at the top ranked ABA-accredited California law schools disproportionately, and unsurprisingly, fare better than those at lower-ranked schools. Of the twenty-one ABA-accredited schools in California, nine have been consistently ranked in the top 100 of the *U.S. News and World Report* rankings of law schools (Stanford, UC Berkeley, UCLA, USC, UC Davis, Pepperdine, UC Hastings, University of San Diego, and Loyola).[61] Historically, those nine schools have represented a disproportionate number of the passing applicants, as shown by this chart.

Year	CA ABA	Top 9 CA ABA	Remaining CA ABA	Differential
2007	76%	82.34%	68.04%	-14.30%
2008	83%	86.25%	79.44%	-6.81%
2009	79%	86.15%	70.32%	-15.83%
2010	75%	82.99%	65.57%	-17.42%

57 Gary Rosin, *On Illinois and State Bar Exam Difficulty,* FAC. LOUNGE (Apr. 15, 2013, 8:00 AM), http://www.thefacultylounge.org/2013/04/on-illinois-and-state-bar-exam-difficulty.html [http://perma.cc/9SJJ-65QG].

58 *See, e.g.*, STATE BAR OF CAL., COMM. OF BAR EXAM'RS/OFFICE OF ADMISSIONS, CORRECTED MBE CONVERSION TABLE (Nov. 18, 2011), http://admissions.calbar.ca.gov/Portals/4/documents/CorrectedMBEConversionTable_201107.pdf [http://web.archive.org/web/20141212095454/http://admissions.calbar.ca.gov/Portals/4/documents/CorrectedMBEConversionTable_201107.pdf]. For that year (the July 2011 Bar Examination), a scaled score of 144 represented 128 correct questions, and a scaled score of 135 represented 117 correct questions.

59 Rosin, *supra* note 57.

60 Flanagan, *supra* note 13, at 175.

61 *Best Law Schools*, U.S. NEWS & WORLD REP. (2015), http://grad-schools.usnews.rankingsandreviews.com/best-graduate-schools/top-law-schools/law-rankings?int=992008.

Year	CA ABA	Top 9 CA ABA	Remaining CA ABA	Differential
2011	76%	80.71%	70.38%	-10.33%
2012	77%	82.51%	70.50%	-12.01%
2013	76%	83.15%	68.49%	-14.66%
2014	69%	79.40%	57.96%	-21.44%
2015	68%	72.10%	63.54%	-8.56%
2007–2015	***75.09%***	***82.08%***	***66.86%***	***-15.22%***

Based on these results, those nine schools need academic support and supplemental bar preparation programs the least. Students at most of the other ABA-accredited schools in California need this assistance more. Based on the bar passage results, many of these students either are not getting it, or what they are getting is not enough.[62] This suggests that these schools, in particular, have the most to gain from investing in labor-intensive, in-house faculty-administered bar preparation programs.

While these schools have much to gain from investing in in-house bar preparation programs, that conclusion still begs the question of what kinds of programs are appropriate or helpful. It is not enough to identify the problem: the need for in-house bar preparation programs. Only programs that contain helpful components, and that can actually work to increase bar passage rates, are part of the solution for schools facing challenging bar passage rates. This Article now turns to a discussion of what programs and elements of programs might be most helpful.

III. THE STATE OF SUPPLEMENTAL BAR PREPARATION PROGRAMS TODAY

While there are any number of suggestions concerning how to improve bar passage, ranging from curricular changes to drastically reduced admissions in order to improve selectivity to increased academic support in the first year of law school, the purpose of this Article is to explore supplemental programs directly aimed at improving bar passage as well as discuss both the existing content of such programs, and what might be the

62 California also is home to twenty California-accredited, but non-ABA accredited, law schools and twenty-two California non-accredited law schools (five distance learning, seven correspondence, and ten fixed facility), all of whose graduates are permitted to take the California Bar Examination. *Law Schools*, ST. B. CAL., http://admissions.calbar.ca.gov/Education/LegalEducation/LawSchools.aspx#unaccredited [http://perma.cc/8N CZ-TLSH]. The pass rate for these law schools is typically quite low: in July 2013 the rate for California-accredited, but non-ABA accredited, law schools was 35.61%, and for California non-accredited law schools was 13.64%. *See Statistics*, *supra* note 38. Since these schools are not attempting to comply with ABA mandates for bar passage—and generally serve students who work full-time or are not qualified to attend ABA-accredited schools—this Article does not seek to address issues of bar passage at these schools.

optimal structure and content of such programs. Thus, this Article is not concerned with the efficacy of changes in curriculum in improving bar passage, or whether curricular adjustments even affect bar passage. The one prominent article on that subject suggested that the *number* of bar-tested courses only statistically significantly affected bar passage for third-quartile graduates.[63] But even that study, by limiting itself to one law school in one state, and to the *number* of bar-tested courses rather than which courses were taken, cannot speak to general principles of curricular adjustment and relationship to bar passage. And certainly, the study and its analysis did not purport to examine the efficacy of courses expressly designed to increase bar passage, such as for-credit or post-graduation bar preparation courses.[64]

This Part will examine examples of supplemental bar preparation programs, and seek to identify the most helpful components of a successful program. To do so, it will examine some current programs, other commentators' thoughts on the elements of successful programs, and empirical studies involving current programs.

A. Examples of Current, but Incomplete, Supplemental Bar Preparation Programs

Remarkably, there is very little literature beyond the 2002 AALS survey detailing the components of in-house supplemental bar preparation programs. One of only a few recent articles addressing some related issues is *The Role of Bar Preparation Programs in the Current Legal Education Crisis*, by Professor Aleatra P. Williams of the Charleston School of Law.[65]

Professor Williams referenced the 2002 AALS survey, and identified the same four-type grouping discussed in Part I above.[66] But as Professor Williams notes, one change that occurred since the 2002 AALS survey was that the ABA

---

63 Douglas K. Rush & Hisako Matsuo, *Does Law School Curriculum Affect Bar Examination Passage? An Empirical Analysis of Factors Related to Bar Examination Passage During the Years 2001 Through 2006 at a Midwestern Law School*, 57 J. LEGAL EDUC. 224, 228 (2007).

64 As discussed herein, most bar preparation courses focus on both substantive law as well as organizational and writing skills.

> Clearly other factors are causing the extremely high bar failure rates for graduates who rank in the bottom 10 percent of their graduating class. Further research is warranted in this area. A simplistic approach of forcing the lowest ranked law school students to take more upper division bar examination subject-matter courses will not solve the bar examination failure problem.

Id. at 236.

65 Williams, *supra* note 12.

66 *Id.* at 401.

standards changed. ABA Standard 302(f) had stated, "A law school may offer a bar examination preparation course, but may not grant credit for the course or require it as a condition for graduation."[67] That Standard was replaced in 2004 by Standard 302, which provided the requirements for substantial instruction, including:

> (1) the substantive law generally regarded as necessary to effective and responsible participation in the legal profession; (2) legal analysis and reasoning, legal research, problem solving, and oral communication; (3) writing in a legal context, including at least one rigorous writing experience in the first year and at least one additional rigorous writing experience after the first year; (4) other professional skills generally regarded as necessary for effective and responsible participation in the legal profession, and (5) the history, goals, structure, values, rules and responsibilities of the legal profession and its members.[68]

At the same time, the ABA adopted Interpretation 302-7, which stated, "If a law school grants academic credit for a bar examination preparation course, such credit may not be counted toward the minimum requirements for graduation established in Standard 304. A law school may not require successful completion of a bar examination preparation course as a condition of graduation."[69] This Interpretation was repealed in 2008.[70] The result was that there were then no restrictions at all on bar preparation courses being offered for credit in law schools.[71]

The number and types of bar exam assistance programs increased, in part, as a result of the release from restrictions on offering course credit for bar preparation courses, but undoubtedly as well due to the pressure to improve bar examination pass rates. Professor Williams identified at least nine such types of bar assistance programs:

> intensive personal coaching, for credit bar review courses, heavy load of required courses, state-focused course offerings, bar review focus throughout law school, post-graduation bar exam boot camps, flagging and releasing at-risk law students, critical skills programs focused on analysis and writing, or collaboration with commercial bar review programs.[72]

---

67 *Id.* at 396.

68 Catherine L. Carpenter, *Recent Trends in Law School Curricula: Findings from the 2010 ABA Curriculum Survey*, 81 B. EXAM'R, June 2012, at 6, 13 n.13, http://ncbex.org/assets/media_files/Bar-Examiner/articles/2012/810212beCarpenter.pdf [http://perma.cc/2B4V-57Y4].

69 *Id.* at 12–13 n.12.

70 *Id.*

71 *Id.*

72 Williams, *supra* note 12, at 401–02.

A survey conducted by the Chapman University Fowler School of Law research librarians has confirmed this wide array of programs. The most prevalent programs are those that make a for-credit course a centerpiece of bar preparation, those that are primarily composed of bar skills workshops, summer programs that include some essay feedback, and those that largely rely on the commercial bar reviews.[73] At least two law schools charge their students or graduates to take a post-graduation supplemental bar preparation course.[74]

Professor Williams focused on four programs.[75] The study was useful, but limited, because it described in a somewhat general way only four programs. These programs utilized methods such as short review classes, some essay grading and feedback, academic attrition, first-year instruction in bar preparation, "bar tips," and student competitions featuring mock multiple choice questions.

Unfortunately, it is difficult to tell how much work students must put into these programs, and how much feedback they receive. Moreover, some of the methods used strike me as not the best practices. For example, the problem with overusing attrition in any form is that it masks either a failure or unwillingness of the institution to expend the resources or effort necessary to make sure all of its students are being given a real opportunity to pass the bar examination. Some attrition is, of course, necessary, because some students, unfortunately, probably should not be in law school. My argument is not with attrition, per se, but with the manipulation of attrition rates with an eye solely toward bar passage. Simply put, any law school can set its attrition rate high enough to guarantee good bar passage rates, but in doing so it may well abandon its educational mission to too many students.

Furthermore, as Professor Williams observed, a first-year bar preparation course at most reinforces skills,[76] but it seems that such a course is premature, so that much of the substance, and perhaps some of the skills, will be forgotten by the third year of law school. As one author has written, "I would think schools with [priorities involving bar passage rates] would realize that

---

73 Survey conducted in August and September 2014. On file with the author.

74 *See Bar Preparation*, UMKC SCH. L., http://law.umkc.edu/academics/bar-prep/ [http://perma.cc/5EQR-G2Z4]; *myBAR FAQ's*, ARIZ. SUMMIT L. SCH., https://www.azsummitlaw.edu/student-resources/student-success-programs/mybar/mybar-faqs [http://perma.cc/4C3M-KXNA].

75 The programs were at Campbell University, North Carolina Central University, Nova Southeastern University, and John Marshall School of Law. Williams, *supra* note 12, at 401–07.

76 *Id.* at 405.

the first year is a very odd place to teach the details that most people try to remember for the days of the [bar] exam."[77]

Finally, the difficulty with non-structured MBE testing as described by Professor Williams, whether in the form of a question per week, or competitions, is that, absent a structured and comprehensive discussion of the reasoning behind each question, there is little guarantee that students will absorb both the substantive law and the analysis of patterns in the law necessary to successfully navigate the MBE portion of the bar exam. For this same reason, simply directing students to do thirty or fifty multiple choice questions each night, without feedback beyond a written explanation, is incomplete as a teaching tool. Such a process is no different than the cookie-cutter approach of commercial bar review products, which "target large numbers of students" rather than individual learning styles.[78]

B. Possible Components of Successful and Complete Bar Preparation Programs

Recognizing the large amount of work necessary to implement an effective bar exam preparation program, one academic support professional sought to identify the appropriate features of a for-credit law school bar preparation course.[79] Denise Riebe addressed five issues: course content; course hours; course methodology; class size, target students, and mandatory v. voluntary classes; and course grading.

Professor Riebe suggests that the course content should include grounding the teaching of learning skills in the substantive law that students need to learn for the bar exam,[80] with "many opportunities to complete practice questions."[81] She also recommends incorporating time and stress management concepts into the course.

In my view and experience, one way to do this is to cover one subject per week, with a midterm and final examination, so that students are taught to study subjects more completely at the times they are covered, rather than "cramming" as they might for an ordinary law school class. When an exam is covering six, seven, or eight subjects at one time, students should be taught to prepare each subject early, and then return to review each subject at least weekly. This process mirrors bar exam study: the

---

77 Ethan J. Leib, *Adding Legislation Courses to the First-Year Curriculum*, 58 J. LEGAL EDUC. 166, 176 (2008).

78 Riebe, *supra* note 7, at 307–08.

79 *Id.* at 326–38.

80 *Id.* at 327.

81 *Id.*

commercial bar reviews cover a subject for two or three days, and students must, on their own, return to those subjects weekly, and increasingly as the bar exam approaches.

Professor Riebe recommends a three- or four-credit course that allots sufficient class time to allow students to complete practice exams, recognizing that the competing demands on law students' time may leave them unable to complete practice questions except in a classroom setting.[82]

But it seems to me that if the course *requires* completion of the practice question or essay—under threat of a grade penalty, but combined with the incentive of prompt feedback—then students will in fact likely turn in their assignments timely, and will complete even more practice essays than they would otherwise. Professor Riebe, indeed, seems to acknowledge this fact.[83]

Professor Riebe recommends "occasional" meetings during the bar review preparation period, or, alternatively, "touching base" with students during that period through e-mails or meetings to reinforce the knowledge and skills learned during the academic year.[84] Thus, Professor Riebe did not address or anticipate significant institutional involvement post-graduation in bar preparation.

In recommending course methodology, Professor Riebe advocates a panoply of different teaching methods, including "active learning, collaborative learning, self-regulated learning, skills instruction, practice opportunities, and peer or professional tutors."[85]

Professor Riebe primarily focuses on the self-regulated learning process: planning a learning task; performing the learning task; and reflecting on the learning experience.[86] Similarly, Raymond J. Wlodkowski and Margery B. Ginsberg, in their book, *Teaching Intensive and Accelerated Courses*,[87] address developing self-efficacy for learning and, like Professor Riebe, identify the importance of planning and self-assessment in learning. But they also point to something Professor Riebe does not address—the importance of prompt feedback:

> Prompt feedback while learning leads to stronger feelings of personal control and self-efficacy. This is one of the main reasons some online

---

82 *Id.* at 329.

83 *Id.* at 337 ("Students are honest in admitting their need for 'carrots and sticks' to make them do what they know they should do.").

84 *See id.* at 330.

85 *Id.* at 330–31.

86 *Id.* at 332.

87 RAYMOND J. WLODKOWSKI & MARGERY B. GINSBERG, INTENSIVE AND ACCELERATED COURSES (2010).

> instruction programs can be so powerful for increasing motivation: the computer program can give immediate feedback so that learners have moment-to-moment awareness of their progress in learning . . . [which] . . . gives them a strong sense of control in the learning process.[88]

While essay feedback cannot be moment-to-moment, it can and should be relatively prompt—certainly, in my experience, no more than forty-eight hours. Thus, a hallmark of a good for-credit bar preparation course is not only outside, required essay writing, but prompt feedback, to encourage students to take control of their own learning process.

Professor Riebe focuses her class size and targeting discussion on at-risk students, a common focus in the academic support community.[89] Her focus, like that of Professor Flanagan, is in part derived from a concern about resources.[90] Professor Riebe's piece, however, was written in 2006–2007, before much attention was paid to what Professor Flanagan identifies as a general increase in underpreparedness of law students. Not only has there been an increase in underpreparedness, but there has been a steep decline in applications over the last several years. This also has the potential of substantially increasing the pool of "at risk" students. "Applications for the class that begins law school [in 2014] are down 8 percent following double-digit declines the two previous years, according to statistics compiled by the Law School Admission Council. That adds up to a total drop in applications of 37 percent since 2010."[91] As a consequence, median LSAT and undergraduate GPA numbers have also dropped. "The average decline in median LSAT scores between 2010 and 2013 across U.S. News 'tiers' of law schools was 1.54 among top 50 schools, 2.27 among schools ranked 51–99, 2.11 among schools ranked 100–144, and 2.79 among schools ranked alphabetically."[92]

This decline in LSAT medians augurs poorly for future bar passage. "For any given cut score, bar passage rates not only fall as law school LSAT scores fall, they fall at increasing rates. Moreover, raising the cut score magnifies this effect."[93] As these

---

88 *Id.* at 86.

89 *See, e.g.*, Flanagan, *supra* note 13, at 173.

90 "Because resources are limited, targeting at-risk students for participation is necessary at most law schools. Most schools neither want to invest in assisting students who would pass without extra support nor displace resources that could be used for students genuinely at risk." Riebe, *supra* note 7, at 333.

91 Neil, *supra* note 5.

92 Paul Caron, *Median LSAT Scores for the 2015 U.S. News Law School Rankings*, TAXPROF BLOG (Mar. 5, 2014), http://taxprof.typepad.com/taxprof_blog/2014/03/median-lsat-scores.html [http://perma.cc/KZ9P-XDG7].

93 Gary S. Rosin, *Unpacking the Bar: Of Cut Scores and Competence*, 32 J. LEGAL

trends have continued, more and more students are at risk of failing the bar exam, so more and more students should be given the opportunity to participate in supplemental bar preparation courses.[94]

While Professor Riebe concludes that, with respect to a for-credit course, "pass-fail grading may be appropriate," she also acknowledges that student attitudes, the need for incentives and dis-incentives, and student "self-handicapping behavior . . . might weigh in favor of using grades as an incentive for students to perform the required course work."[95] On this, I agree; my experience with students is that ungraded or pass-fail assignments are not met with the same level of effort or seriousness as graded assignments or exams. Given that, as discussed earlier, the bar examination requires more work than a full-time job,[96] that work should always be approached with seriousness of purpose, something that is more likely when a student's grade depends on the effort.

As mentioned earlier, Professor Riebe also discusses limiting participation in for-credit courses to at-risk students. I respectfully disagree, because there are other reasons to extend the opportunity to participate in for-credit bar preparation courses to the entire class. For example, participation by most or all of the class from the beginning of the academic year (or semester, depending on whether the course is offered for a full year or semester) will help create a group mentality where everyone is supportive of everyone else, and as a group, everyone is responsible for everyone else. Thus, as a cohort, the entire class can experience the effort and time expenditure necessary for adequate preparation for the bar examination. Even for those top-level students who may not need a bar preparation program, my experience—and at least some belief, perhaps unproven, of others—is that there are intangible benefits, such as increased confidence at the bar exam itself.[97] Ultimately, I have found, this level of inclusion has led to a common and healthy *esprit de corps* among the entire class.

PROF. 67, 93 (2008).

94 In this context, it is particularly concerning to see some law schools charge their law students to participate in a law school supplemental bar preparation program. Unlike tuition, which students can plan for, students generally learn about this extra charge in their third year, as graduation approaches. Such an extra charge beyond tuition, much less the charges of $600–$2000 or more, can therefore deter students who may well need the supplemental academic assistance from receiving it. Arizona Summit charges $2550 and UMKC charges $600. *See Bar Preparation*, *supra* note 74 *myBAR FAQ's*, *supra* note 74.

95 Riebe, *supra* note 7, at 337–38.

96 *Id.* at 307.

97 Jellum & Reeves, *supra* note 29, at 679–80.

One other result of limiting participation in for-credit courses to at-risk students is that it denies students a choice of classes. Given the importance of the bar examination, denial to some groups of students the choice of whether to take a for-credit bar preparation course is inadvisable. It seems unfair to deny students the opportunity to take courses of their own choosing, particularly if they believe, and it has been demonstrated, that the courses are helpful to them. Indeed, denying the course to some on the basis that they do not need the course can lead to a fracturing of the class and a disincentive later during the pre-bar summer to work together toward the common goal of bar passage for everyone. This fracturing seems to the author to be something that tends to be ignored in the rush among many in the academic support community to focus their efforts primarily on what they perceive to be "at-risk" or even "non-traditional" students. As more and more law students, whatever their background, fall into the "underpreparedness" category, this focus on one discrete group seems less and less productive. Professor Riebe concedes that there is a risk of stigmatizing at-risk students who are placed in academic support classes, but she suggests that "most students, with positive encouragement, are able to disregard stigma issues."[98] While there may be some anecdotal evidence of the overcoming of stigma on the part of the students benefiting from the academic support, the effect of stigma goes both ways: students receiving the academic support not granted to others may feel stigmatized, but those not granted the academic support may resent the opportunities given to others. It seems better, particularly when the goal is bar passage, which is an equal and common goal of all the students, to extend support to all the students, and generate a common culture of mutual support and hard work.

As previously discussed, law school bar preparation programs include for-credit courses and supplemental programs offered during the summer before the bar exam. In this context of an overall host of bar preparation programs, Professor Riebe's discussion largely focuses on a for-credit course offered during the school year, which is a good start, but she does not focus on either the need or the substance of a post-graduation supplemental bar preparation program. But commercial bar review courses, while helpful to some extent, are simply not sufficient in giving enough feedback for many students, particularly those who entered law school underprepared, and remain there even at graduation. Thus, law schools must not

98 Riebe, *supra* note 7, at 334.

only evaluate for-credit courses; they must consider offering post-graduation supplemental programs.

For all these reasons, then, it is anachronistic to apply an older model of academic support to contemporary students by limiting programs to for-credit courses, and those courses to certain perceived at-risk groups. Instead, with this ever-increasing decline in preparedness and qualification of students, bar preparation programs must be designed and implemented to apply both before and after graduation, and to all students.

C. Empirical Studies of the Effectiveness of Some Bar Preparation Programs

Whether the bar preparation program utilizes for-credit courses, a summer supplemental program, or both, what is clear from the only empirical studies that have been published is that programs with intensive essay writing practice do increase bar passage. Both the University of Richmond and the University of the District of Columbia David A. Clarke School of Law ("UDC") instituted bar preparation programs, and these are the two which have published empirical studies of the effectiveness of their programs.[99]

Richmond's program includes a bar preparation class scheduled for a student's final semester. It includes a two-hour lecture, time to complete twelve to fifteen multistate questions and one or two essay questions, and review of those questions. Richmond also includes individual tutoring in essay writing, requiring and giving individual feedback on multiple essays.[100]

In 2005, UDC instituted a bar preparation program that included several components: a BarBri videotaped lecture series and essay writing workshop; a separate essay writing class taught by members of the law school's Bar Passage Task Force; PMBR multistate workshops; and the MBE review workshop presented by video by Professor Richard Litvin, then of Quinnipiac University.[101] Chapman University's Fowler School of Law uses a modified version of the Litvin program, taught live by faculty of the law school.[102]

---

99 *See* Jellum & Reeves, *supra* note 29; *see also* Derek Alphran, Tanya Washington & Vincent Eagan, *Yes We Can Pass the Bar. University of the District of Columbia, David A. Clarke School of Law Bar Passage Initiatives and Bar Pass Rates—From the Titanic to the Queen Mary!*, 14 UDC/DCSL L. REV. 9 (2011).

100 Jellum & Reeves, *supra* note 29, at 661–63.

101 Alphran, Washington & Eagan, *supra* note 99, at 21–22.

102 *See infra* Part IV.

In 2006, after the ABA began allowing bar preparation courses for credit, UDC proposed instituting a bar skills essay writing class for credit.[103] The "PTEX"-administered essay writing course began in 2007. It is a fourteen-week practicum "that provides an intensive writing experience for students in preparation for the written portions of the bar exam, the essay examination, and the MPT."[104]

In the cases of both the Richmond and UDC programs, they were able to show increases in bar passage. Both programs utilized a chi-square analysis to determine that these increases were statistically significant.

Because Richmond had significant data from both before and after its implementation of a program, Richmond used a proportions test to determine the effect of bar passage. Richmond showed a 6.2 percentage point increase in bar passage overall, with improvements in the third and fourth quartiles of 13.9 percentage points and 20.4 percentage points, respectively. These results were statistically significant using a 0.05 significance level, meaning that the results would not occur randomly more than 5 times out of 100.[105]

Richmond also tested the effect of participation in the program, using a chi-square analysis. Applied to the bottom half of the class from July 2001–2004, Richmond found that 83 of 116 program participants (71.55%) passed the bar examination, while only 59 of 106 non-program participants (55.66%) passed the bar examination. Richmond found that this difference was statistically significant, again at the 0.05 significance level.[106]

Borrowing from Richmond's methodology, UDC also determined whether their increase in bar passage was statistically significant. UDC compared bar pass rates from 2003–2006 with those from 2007–2008, which involved application of the more intensive writing skills course. The bar pass rate among all students improved from 51.7% to 69.7% for all students, and from 31.3% to 50.9% for the bottom half of the class.[107]

UDC also analyzed and compared performance by those participating in the bar skills program initiated originally in 2003 and PTEX in 2007 with those not participating in those programs. Participation in the bar skills program significantly

---

103 Alphran, Washington & Eagan, *supra* note 99, at 25.
104 *Id.* at 27.
105 Jellum & Reeves, *supra* note 29, at 672, 679 n.197–99.
106 *Id.* at 678–79.
107 Alphran, Washington & Eagan, *supra* note 99, at 35.

improved the likelihood of bar passage: from 2003–2008, 62.5% of those participating in the bar skills program passed while only 47.8% of those not participating in the bar skills program passed; in the bottom half of the class, during the same period, 46.6% of those participating in the bar skills program passed while only 21.6% of those in the bottom half not participating in the bar skills program passed. Using a chi-square test, both of these results were statistically significant to well below a 0.05 significance level.[108]

Participation in the PTEX program did not significantly improve bar passage based on law school GPA, although for the bottom half of the class, there was a slightly better result for participants than for non-participants.[109] However, it appeared that participation in the PTEX essay writing skills program did result in significant improvement based on LSAT scores. For students with an LSAT below 150, those who participated in PTEX passed at a 50.0% rate, while those who did not participate passed at a 31.0% rate. Using the chi-square test, at a 0.05 significance level, this result was significant.

It thus appears that, in those programs that have applied some statistical analysis to their results, their bar passage programs made a significant difference in bar passage. Both of those programs share some common characteristics, the most important of which is a significant focus on improving essay-writing skills, utilizing ample feedback. Both as well gave fairly quick feedback on MBE practice, including in-depth analysis of questions and the possible options.

Extrapolating from and applying these data, it seems fair to conclude that a comprehensive in-house bar preparation program that combines rigorous for-credit courses with a summer supplemental program that includes focus on both essay writing and multistate review, with ample and prompt feedback, should then result in improved bar passage rates. Without more data, however, we cannot be sure which part of the program makes the most difference. As shown below, such a program requires significant time and labor, both on the part of the students and the faculty, but it produces results.

IV. A COMPREHENSIVE EFFORT: CHAPMAN UNIVERSITY'S FOWLER SCHOOL OF LAW

Because the decline in student preparedness and admission statistics is increasing the pool of at-risk students, this Article

108 *Id.* at 36–37, n.129.
109 *Id.* at 37–38.

has argued that bar preparation programs require both for-credit courses and supplemental post-graduation bar preparation programs, highly labor-intensive for both students and faculty, and targeted toward all students to develop a cohesive class studying for the bar examination. As demonstrated, it appears that such programs can have a positive effect on bar passage. The final two Parts of this Article describe an example of such a highly labor-intensive program available to all students, and describes empirical evidence of the effectiveness of such a program.

In 2007, Chapman University's School of Law (now named the Fowler School of Law)[110] initiated a supplemental bar preparation program, consisting of some essay assistance and MBE practice using a series of videos produced by then-Quinnipiac Law School Professor Richard Litvin. The program was expanded to something approaching its current format during the 2008–2009 academic year, and the results since then have been, with one exception, promising.[111] Except for an anomalous bar examination pass rate in July 2010, bar passage at Chapman University's Fowler School of Law has exceeded the California ABA school average each year.

This Part has three sections: one detailing the development of the Academic Support Program at Chapman; a second examining the structures and components of the for-credit bar preparation courses offered by Chapman; and a final section examining the structure and components of the post-graduation supplemental bar preparation program at Chapman.

A. Academic Support and Bar Preparation at the Chapman University Fowler School of Law

Since 2004, when Chapman first hired a Director of Academic Achievement, it has been steadily refining its academic support and bar preparation programs, adding new layers across the years in response to the growing need for such services.

Early on, these included three specific programs for academic support: (1) workshops throughout the academic year—and particularly in the first semester—for first-year students, designed to develop the skills needed to succeed in law school; (2) individual tutoring with the Director; and (3) establishment of study groups

110 *See* Dawn Bonker, *Law School Receives Historic $55 Million Gift, Naming The Dale E. Fowler School of Law*, CHAP. U.: BLOGS (Aug. 14, 2013), http://blogs.chapman.edu/happenings/2013/08/14/school-of-law-receives-historic-2nd-largest-reported-gift-to-a-law-school-school-is-named-the-dale-e-fowler-school-of-law/ [http://perma.cc/UR8P-E6KV].

111 *See infra* Part V.

for first-year classes led by student "Academic Fellows."[112] In addition, Chapman contracted with two commercial bar preparation programs to provide six bar exam workshops for graduating students in the spring semester.

Chapman eventually expanded the Early Bar Preparation Program that included weekend lectures and workshops on bar essay subjects for third-year students during the academic year. It also included some assistance to students and essay review.

Beginning for the 2007–2008 academic year, Chapman also offered a course titled "Legal Writing Skills," which is required for students who receive a grade of 1.9 or below in either semester of their first-year Legal Research and Writing ("LRW") course, or where the student's LRW professor recommends that the student take Legal Writing Skills. Legal Writing Skills is an intensive workshop designed to improve the writing and analytical skills of struggling students. At that time, Chapman also began to offer a course titled, "Legal Analysis Workshop," focusing largely on the skills required to successfully complete the performance test portion of the California Bar Exam.

Chapman has made several efforts to institutionalize both early bar preparation and continued supplemental bar preparation after graduation as a way of life for Chapman students. To that end, in the fall of 2008, I began teaching a for-credit bar preparation course as an adjunct professor at the law school. I have subsequently progressed through the academic ranks to my current full-time position as Professor of Academic Achievement and Director of Bar Services.[113]

B. Chapman's For-Credit Bar Preparation Courses

In Part III, I advanced the view that a comprehensive bar preparation program should have both for-credit courses and a post-graduation supplemental program. This section addresses the for-credit bar preparation courses. The law school offers two for-credit bar preparation courses: "Legal Analysis Workshop" and "Select Topics in American Law." Both courses are open to

---

112 These students are generally selected by the Director of Academic Achievement in consultation with the faculty whom the Academic Fellows would serve, based on the students' performance in the particular faculty member's course.

113 I had formerly been the Associate Dean for Academic Support at Whittier Law School and Chief of Staff to Orange County Supervisor John Moorlach. In the summer of 2009, I also coordinated the Supplemental Bar Preparation Program (described in detail below). In August 2009, I was appointed Visiting Associate Professor of Academic Achievement by the Dean of the Chapman University School of Law, and was re-appointed to that position for the 2010–2011 academic year by the Interim Dean, and given the additional title of Director of Bar Services.

all students, but both courses are required for those students who begin their third year in the bottom quartile.

Legal Analysis Workshop is a three-unit course. Since the 2010–2011 academic year, two sections have been offered in the fall, and two sections have been offered in the spring. In the course, students learn the skills needed to write good three-hour performance tests similar to those given on the California Bar Exam. Each student writes a weekly ungraded, but required, practice performance test on which the instructor provides extensive feedback as to form and content. In addition, students write two midterm examinations and one final examination, each in the form of a three-hour performance test. Students receive written feedback on their examinations, and are also required to meet with their professor for one-on-one discussions of each of their midterm examinations. Historically, about half the students in a graduating class tend to take Legal Analysis Workshop, and most are generally in the bottom half of the class.[114]

Select Topics in American Law is a three-unit course. One section is offered in the fall, and three sections are offered in the spring. Since the 2009–2010 academic year, three of the four sections each year have been taught by me, and one section, taught in the evening in spring semester, has been taught by another faculty member or an adjunct faculty member with my supervision. About 90% or more of the graduating class historically takes the course,[115] with about 105–120 students taking the course from the author and about 20–25 students taking the course from the other faculty member.

The course is primarily directed at essay writing for the California Bar Examination, and covers every identified subject on the examination. Each class session is three hours long. In the first week, students review good techniques for bar examination essay writing, including proper Issue-Rule-Application-Conclusion ("IRAC") structure, formulation of precise rule statements, thorough use of facts, and proper analytical reasoning, as well as good format, style, and general grammar and syntax issues. In each week thereafter, students are assigned to thoroughly read an outline of the law on the particular week's subject and to write a take-home essay—a prior California Bar Exam essay—and upload it to the course "TWEN" website for feedback from the professor, which is provided very soon after its submission. In class, the professor begins with an approximately 90-minute lecture on the particular subject, discussing the areas that

114 Records on file with the author.
115 Records on file with the author.

historically tend to be tested on the California essay exam, the applicable black letter law, approaches for analyzing issues presented involving that law, and examples from prior essay exams involving that subject. The class then together reviews, with the professor, the take-home exam, and looks at an example of a passing essay, with the professor pointing out the parts of the essay that were done well and the parts that were not done well. The class then takes one hour and each student writes an in-class essay consisting of another prior California Bar Exam essay in the subject, after which the professor discusses with the class the proper format and content of the in-class essay, individually questioning students to draw them into a discussion of the essay and to give immediate feedback on student wording of the various parts of their essays. The class again reviews an example of a passing essay, with the professor again pointing out the parts of the essay that were done well and the parts that were not done well.

Once class is over, students can download the following items from TWEN each week: (1) lecture notes from the professor, detailing the essay approaches, including black letter law and analysis directions, for the subject just covered; (2) the professor's model answers to both the take-home essay and the in-class essay; and (3) the sample "passing" answers. Students are instructed to learn the material from a subject that week by reviewing the lecture notes and beginning to memorize them, and by reviewing the model answers for structure and form. The faculty explains to students that this duplicates bar study, because commercial bar reviews only cover a subject once, and students are expected to study on their own. Thus, students are instructed to review each set of lecture notes not only the week they are published, but each week thereafter until the midterm or final exam, so that they cumulatively study and memorize each subject, just as if they were doing so while studying for the bar exam. This causes students to avoid "cramming" for the midterm or final examinations, and to develop an early habit of constant and cumulative studying in order to master multiple subjects.

In addition to the twelve take-home essays and twelve in-class essays students are required to write, and for which they receive feedback as discussed above, there is a midterm examination and a final examination, each of which counts for 50% of the student's grade. Each examination is three hours long and consists of three essays, all of which are "cross-over" type essays, covering a minimum of two subjects. The midterm examination covers the following subjects: Contracts and

Sales; Torts; Federal and California Civil Procedure; Criminal Law and Criminal Procedure; and Real Property. The final examination covers the following subjects: Federal and California Evidence; Business Associations (Agency, Partnerships, and Corporations); Constitutional Law; Professional Responsibility; Wills, Trusts, and Estates; Community Property; and Remedies.

Grading in the course is far from liberal. While the maximum median at the law school applicable to upper-level courses of twenty or more students is 3.0, the actual median grade awarded in Select Topics has never exceeded 2.8. In the fall semester, which has a lower population largely consisting of students preparing to take the February Bar Exam, the median over the six years the course has been taught has averaged 2.725. The high grade in the fall semester has averaged 3.48, and the low grade in the fall semester has averaged 1.70. In the spring semester, when well over 100 students take the course, the median over the six years the course has been taught has averaged 2.78. The high grade in the spring semester has averaged 3.74, and the low grade in the spring semester has averaged 1.59.[116]

As a consequence, the course has developed a reputation among students as being very demanding, requiring a significant amount of work, and very difficult—just as a course preparing students for the rigors of concentrated study for the bar exam should be. Nevertheless, the course has grown from inception in the 2008–2009 academic year where 6 students took it in the fall and 60 in the spring, to one in which 155 students out of 169 bar takers took it in the 2012–2013 academic year and 130 students out of 143 bar takers took it in the 2013–2014 academic year.[117]

C. Chapman's Supplemental Bar Preparation Program

As discussed earlier, a comprehensive bar preparation program should have both for-credit courses and a post-graduation supplemental program. This section addresses Chapman's post-graduation Supplemental Bar Preparation Program ("Supplemental Program").

At first, the post-graduation supplemental program was rudimentary, with some essay review and essay workshops in the summer of 2007. Beginning in the summer of 2008, the law school began developing a more extensive post-graduation Supplemental Program, designed to supplement whatever commercial bar preparation course in which students were enrolled.

---

116 Records of grades on file with the author.

117 Records on file with the author.

Originally, the Supplemental Program consisted of two components: (1) mock MBEs and DVD lectures on the MBE subjects given by Professor Richard Litvin of Quinnipiac University Law School, purchased by the law school, administered locally but largely taught long-distance by Professor Litvin; and (2) occasional assigned specific essays with feedback by academic support faculty and several of the LRW professors.

The second component of the Supplemental Program (the essay writing) was improved in the summer of 2009. While the author was still employed as an adjunct professor, he and several others critiqued, with a twenty-four to forty-eight hour turnaround, *any* practice essay submitted to them by students. This essay grading was in addition to the assigned essays that were part of the original program. As a result, many more student essays were graded in the summer of 2009—approximately 900 for 142 first-time takers.

When I was appointed Visiting Associate Professor of Academic Achievement late in the summer of 2009, an institutional commitment was made to improve the Supplemental Program. As Director of Bar Services, I replaced the Litvin program with Chapman's own mock bar exams and live sessions conducted by the Director of Academic Achievement and me. This allows students to ask questions at each session, and each session covers all the multiple choice questions from one of the six subjects on the previous mock bar. There are six sessions after each mock bar—one for each subject (Contracts, Torts, Criminal Law and Procedure, Evidence, Constitutional Law, and Real Property). There are three mock bars, and students' progress is tracked and given to them in written reports that detail which questions they correctly answered and which ones they missed, how well they did on each subject, as well as on important topics in each subject, and how well they did in the morning session and the afternoon session. Students are then given a final 100-question mock bar less than a week before the California Bar Examination.[118]

In addition, I reformulated the essay writing component of the program. All potential essays may be uploaded by students to the course TWEN website. The adjunct professors who teach Legal Analysis Workshop during the academic year critique performance tests submitted by the students. The author and up to eleven other full-time and adjunct faculty members and other

118 Historically, students average about 52% correct on the first mock bar exam, which is a baseline pre-test; by the end of the Supplemental Program, in each year since it was implemented fully in 2010, students average from 74%–78% correct on the final mock bar exam.

non-faculty graders[119] critique all student essays, and return them to students with comments within twenty-four to forty-eight hours. This team critiqued approximately 1700 written submissions from 138 first-time students in summer 2010; 2400 written submissions from 159 first-time students in summer 2011; 3000 written submissions from 157 first-time students in summer 2012; 4450 written submissions from 157 first-time students in summer 2013; and, after reasonable and appropriate caps on the maximum number of reviewable essays per student were instituted,[120] 2800 written submissions from 130 first-time students in summer 2014.

Students are directed to write an equal number of essays on their own and self-check them. If they have any questions about those essays, particularly given the tendency of commercial bar reviews to write "model" answers that are overly dense, complex, and too long for any student to write in a one-hour time frame, they may contact me to discuss any essay they have written.

I also send frequent e-mails to all the students in the Supplemental Program, discussing substantive issues of law that are frequently tested. Additionally, students may e-mail substantive law questions to me at any time from graduation until the bar examination ends, and I respond promptly so long as the questions are sent between the hours of 7:00 a.m. and 11:00 p.m.

Finally, Chapman also has offered the Supplemental Program to those students taking the February bar examination, beginning in February 2010. That program begins in mid-December, and concludes less than a week before the February bar examination, but is largely identical to the summer program, except that it serves far fewer first-time takers and some repeaters.

The Supplemental Program begins shortly after graduation in May for the July bar examination, and in mid-December for the February bar examination, and is available free to all Chapman graduates, whether they are first-time takers or repeaters, and whether they are taking the California Bar Examination or the bar examination of another state. In each case, the sessions reviewing MBE questions run until about five

---

119 I select non-faculty graders based on their past law school performance and experience as teaching assistants, and I train them on how to critique essays, always selectively reviewing their critiques to make sure their work is consistent and complete.

120 Prior to the Supplemental Program for the February 2014 Bar Examination, there were no limits on the number of essays students could submit for grading. Currently, students may submit up to thirty essays for grading, and more with the permission of the author.

to six days before the bar examination, and students may submit essays to the team of faculty until late in the afternoon of the Friday before the bar examination, although they may continue to submit essays to me through the morning of the Sunday before the bar examination.

The Supplemental Program requires significant time and labor on the parts of both the students and faculty. If students write thirty essays for grading, plus another thirty or so on their own for self-checking, then they will write sixty essays in about an eight-week period.[121] This means that, in addition to attending an average of twenty hours of classroom instruction from the commercial bar review each week, and six hours of classroom instruction from the Supplemental Program sessions, as well as significant study time outside of the classroom, students are writing an average of more than seven essays per week. As discussed both with respect to the Richmond and UDC programs, and in Part V below, a significant key to passing the bar examination is repeated and intensive writing practice. There is, simply put, no substitute for sustained hard work by both faculty and students, and the program is structured on that reality.

Given that Supplemental Program faculty critique thousands of essays over the eight-week period, they each put in substantial time as well. Generally, I critique about half the essays written by each student, and the remaining team members grade the other half. This means that each grader, other than I, averaged about 205 essays in the summer of 2013, and 127 essays in summer of 2014. I tend to critique up to 2000 essays each summer and, combined with the essays graded in Select Topics over the academic year, grade over 4000 essays per year. This labor-intensive effort is needed when the program seeks to adequately service the entire graduating class, and this amount of labor is necessary no matter how many graders the program can employ.

From the perspective of some academic support professionals, resources are insufficient to adequately provide one-on-one academic assistance to an ever-growing number of at-risk and other students needing such assistance without incurring additional cost,[122] or asking other faculty for assistance in

121 Students may begin to turn in essays beginning the first week in January for the February bar examination, and beginning the first week in June for the July bar examination. In both cases, students may turn in essays until 4:00 p.m. on the Friday before the bar examination—which allows time to return all critiqued essays before students pack up to go to a hotel near where they are scheduled to take the bar examination. Thus, on average, students may turn in essays over the course of eight weeks.

122 Flanagan, *supra* note 13, at 174–77.

teaching,[123] and some academic support faculty complain that they "remain relegated to second-class status, staffed by non-tenure track faculty."[124] However, none of these issues is important from the perspective of the students being served. Given the high cost of education, every student has a right to our time and hard work, at whatever level it reasonably takes, to provide the kind of comprehensive and labor-intensive bar preparation program described herein. Moreover, as mentioned earlier and as described in Part V it is more than worthwhile in terms of the results.

V. A DESCRIPTIVE AND STATISTICAL ANALYSIS OF STUDENT PERFORMANCE AT CHAPMAN UNIVERSITY'S FOWLER SCHOOL OF LAW

As mentioned above, once significant pieces of the comprehensive bar preparation program at Chapman were introduced (including the for-credit Select Topics and Legal Analysis Workshop courses as well as the summer Supplemental Program), the results have, with the exception of one anomalous exam administration, been promising.

A. Chapman's Performance on the California Bar Examination Since Adopting Its Program

As shown by the following chart, Chapman has exceeded the California ABA school average pass rate every July bar examination since 2009 except for one, and has seen its bar passage rates come much closer to those posted by the nine California law schools in the *U.S. News and World Report* Top 100 Law Schools than those posted by the eleven law schools either not yet rated in the so-called third and fourth tiers, and one not-yet rated (UC Irvine).

Year	(1) CA ABA	(2) Top 9 CA ABA	(3) Remaining CA ABA	(3)-(2) Differential	(4) Chapman	(4)-(2) Differential
2009	79%	86.15%	70.32%	-15.83%	80.99%	-5.30%
2010	75%	82.99%	65.57%	-17.42%	69.57%	-13.41%
2011	76%	80.71%	70.38%	-10.33%	79.25%	-1.46%
2012	77%	82.51%	70.50%	-12.01%	81.53%	-0.98%
2013	76%	83.15%	68.49%	-14.66%	77.07%	-6.08%
2014	69%	79.40%	57.96%	-21.44%	74.80%	-5.40%
2015	68%	72.10%	63.54%	-8.56%	71.20%	-0.90%
2009–2015	***73.87%***	***81.46%***	***64.98%***	***-16.48%***	***76.65%***	***-4.81%***

123 *Id.*
124 *Id.* at 174.

As the chart also shows, Chapman exceeded the California ABA school average pass rate on the July 2014 and July 2015 Bar Examinations. In July 2014, when the California ABA school average pass rate dropped significantly, from 76% to 69%,[125] and bar exam rates dropped nationally,[126] Chapman's bar passage rate was 75%.[127] In July 2015, when the California ABA school average pass rate dropped further to 68%, Chapman's bar passage rate was 71.2%.[128]

Chapman's achievement is consistent with the findings of two scholars who have analyzed the data. In his paper, *Ranking Law Schools Using Reported California Bar Exam Results: Some Observations and Conjectures*, Professor Donald Smythe sought to rank law schools based on their bar passage rates, particularly from 2007–2011, and compared those rankings to the *U.S. News and World Report* rankings.[129] He found that:

> in addition to the elite Californian schools, Pepperdine, Loyola, San Francisco, Santa Clara, California Western, Chapman, San Diego, and McGeorge all had California bar passage rates for reported first-time takers of the exam over the period from 2007-2011 which exceeded those of at least three schools that the US News ranked in its top twenty-five.[130]

He also found that:

> Chapman is a relatively newly-accredited law school, and it placed only 110th in the US News ranking, but from 2007-2011 its California bar passage rate for reported first-time takers also exceeded the passage rates of many schools that rank in the US News top fifty, and even some in the top twenty-five, as well as San Diego's and McGeorge's [law schools].[131]

As Professor Smythe also noted in a footnote, "Chapman's relatively strong showing is also reflected by the favorable comparison with other relatively newly-accredited Californian schools such as La Verne and Western State, which had significantly lower bar passage rates."[132] Professor Smythe's study was written in 2012, and thus did not take into account Chapman's even stronger performance on the July 2012 and 2013

---

125 For the most recent statistics published by the State Bar of California, see *Statistics*, *supra* note 38.

126 *See, e.g.*, Marino Bar Review, *Declining Nationwide Bar Exam Pass Rates*, ABOVE L. (Oct. 27, 2014, 10:15 AM), http://abovethelaw.com/2014/10/declining-nationwide-bar-exam-pass-rates [http://perma.cc/3VKQ-A3BS]; *see also* Gershman, *supra* note 1.

127 For the most recent statistics published by the State Bar of California, see ABOVE L., *supra* note 126.

128 *See id.*

129 Smythe, *supra* note 14.

130 *Id.* at 21–22.

131 *Id.* at 22.

132 *Id.* at 22 n.33.

bar examinations, when it ranked 7th and 9th among California ABA-accredited law schools, ahead of not only the other five schools with equivalent predictors, but also ahead of law schools such as UC Davis (July 2011 and 2012), UC Hastings (July 2012 and 2013), and Loyola (2012).[133]

Professor Paul Caron's analysis was completed in January 2014, after the July 2013 bar results were released. He explained that Chapman, with a *U.S. News and World Report* rank of 12th among all 21 California ABA-accredited law schools and 126th overall, outperformed UC Hastings (48th), University of San Diego (68th), Santa Clara (96th), and McGeorge (124th), as well as University of San Francisco (144th).[134]

Indeed, since Chapman adopted its complete supplemental bar preparation program beginning in July 2009, it has exceeded the California ABA school average in six of the seven years. Moreover, in the last five years (2011–2015), Chapman has ranked 8th, 7th, 8th, 9th, and 9th among all California ABA-accredited law schools (21 in total) in pass rate, exceeding at times the pass rates of several of the top 100 ranked law schools in California.[135]

Based on comparisons both with equivalently situated law schools and with California ABA-accredited law schools overall, it would appear that the labor-intensive approach at Chapman, stressing significant practice and immediate feedback, is effective. But are Chapman's results statistically significant?

B. Statistical Analysis of For-Credit Bar Preparation Course at Chapman

As has been noted, virtually the entire graduating class takes the for-credit Select Topics course, and those that do not are at the top of each class, and likely to pass the bar with or without additional assistance. Almost every graduate takes the summer Supplemental Program. As a result, there is no longer a

---

133 *See Statistics*, *supra* note 38.

134 Caron, *supra* note 14.

135 For example, in the most recent rankings (2016, ranked in 2015) the University of San Diego School of Law (USD) is ranked 71st by *U.S. News and World Report*, but in the seven years that Chapman has fully implemented its supplemental bar preparation program, it has exceeded USD's pass rate *all but one of the seven years*. UC Hastings College of Law is ranked 59th by *U.S. News and World Report*, but in the seven years that Chapman has fully implemented its supplemental bar preparation program, it has exceeded Hastings' pass rate four times, including July 2014 and July 2015. Similarly, UC Davis School of Law is ranked 31st by *U.S. News and World Report*, but Chapman has exceeded Davis' pass rate twice. Most recently, Pepperdine Law School is ranked 52nd by *U.S. News and World Report*, but in July 2015, Chapman's bar passage rate exceeded that of Pepperdine.

large enough control group of students who do not take Select Topics to run a meaningful statistical analysis. Specifically, in each graduating class, out of 150–169 students, there are no more than 10 or so who do not take Select Topics, and almost all of them are students near the top of the class who, based on historical performance, likely would pass the bar exam with or without Select Topics or any other bar preparation course.[136] Thus, there is no group large enough each academic year to compare performance in Select Topics against, because there are not enough students who do not take Select Topics to reach a statistically significant conclusion.

However, the first year that Select Topics was offered, only 59 students took it out of a graduating class of 142. Therefore, 83 students did not take Select Topics, which means that the two groups (Select Topics takers and Select Topics non-takers) were each large enough that a meaningful statistical comparison of their relative results on the bar examination could be performed, similar to the studies done by Richmond and UDC.

In academic year 2008–2009, fifty-nine students who subsequently took the July 2009 Bar Examination took Select Topics in American Law. Of those students, fifty-one passed the July 2009 Bar Examination and eight did not. Of the students who subsequently took the July 2009 Bar Examination but did not take Select Topics, sixty-four passed and nineteen did not.

As with the Richmond and UDC studies, a chi-square (χ^2) analysis can be done on this two-by-two distribution. A chi-square analysis tests the relationship between two independent variables—in this case, taking or not taking Select Topics and passing or failing the California Bar Examination. Each variable has two possible outcomes, and thus, there are four possible outcomes: (1) took Select Topics and passed the California Bar Examination; (2) took Select Topics and failed the California Bar Examination; (3) did not take Select Topics and passed the California Bar Examination; and (4) did not take Select Topics and failed the California Bar Examination.

Placing this data into cells looks like this:

	Pass	**Fail**	**Total**
Took Select Topics	51	8	59
Did Not Take Select Topics	64	19	83
Total	115	27	142

136 Records on file with the author.

The formula for determining chi-square is: $\chi^2 = \sum(o - e)^2/e$. Chi-square sums the squares of the differences in observed frequencies and expected frequencies. The observed frequency is the actual number of students in each cell. The expected frequency is the number of students one would expect in each cell if taking Select Topics had no bearing on bar passage. For example, since 59 students took Select Topics, the expected frequency is 29.5 passing students and 29.5 failing students. The chi-square test results in a number from 0 to infinity. A "0" result, or something near it (the "null hypothesis"), exists when the frequency of results in each cell approaches the expected frequency, in other words, there would be no real effect on passing or failing whether a student did or did not take Select Topics if a chi-square at or near 0 results.

The null hypothesis is that there is no relationship between taking Select Topics and passing the California Bar Examination. Assuming a null hypothesis, as described above, the expected frequency in the cells for "Took Select Topics" is 24.5, and the expected frequency in the cells for "Did Not Take Select Topics" is 41.5.

To determine whether the chi-square result matters and is statistically significant, statisticians determine whether the result would be expected in less than 5% of random occurrences. To determine this, we first decide on the "degrees of freedom," which refers to the number of cells not being restricted to a single frequency. Once the cell "Pass" is filled, the cell "Fail" is automatically filled, so there is only one degree of freedom. The total degrees of freedom with two variables is the product of the two. Because this is a two by two cell structure, there are total degrees of freedom of $(r-1)(k-1) = 1$. Whether a chi-square result is statistically significant depends on whether the probability that this chi-square value will be exceeded is less than 5%, given the applicable degrees of freedom.

This matrix results in a chi-square of 55.7536. As is typical and accepted, the null hypothesis can be rejected if the chi-square value of 55.7536 exceeds the critical chi-square value within one degree of freedom at the .05 significance level (meaning the result would be expected to occur less than 5% of the time). At the .05 significance level, for one degree of freedom, the chi-square value must exceed 3.84.[137] A chi-square of 55.75836 in fact suggests that the probability of the bar preparation course having no effect is less than .005 (1/2 of 1%).

---

137 Based on a chi-square table. *See, e.g.*, PERRY E. JACOBSON, JR., INTRODUCTION TO STATISTICAL MEASURES FOR THE SOCIAL AND BEHAVIORAL SCIENCES 601 app. (1976).

Thus, the null hypothesis can be rejected, and it appears that the results are significant: taking Select Topics was helpful in passing the California Bar Examination.[138]

The July 2009 results also suggested significant improvement at the lower quartiles. Based on prior years' performance, the expected pass rate in the third quartile was 69.32%, but the actual pass rate in the third quartile was 86.11%. The expected pass rate in the fourth quartile was 30.30%, but the actual pass rate in the fourth quartile was 50.00%.[139] These results appear to be significant.

For example, the chi-square matrix for the third quartile is:

	Pass	Fail	Total
Took Select Topics	8	1	9
Did Not Take Select Topics	22	4	26
Total	30	5	35

This matrix results in a chi-square of 5.3429. As noted above, at the .05 significance level, for one degree of freedom, the chi-square value must exceed 3.84. A chi-square of 5.3429 in fact suggests that the probability of the bar preparation course having no effect is less than .025. Thus, for the third quartile, the null hypothesis can be rejected, and it appears that the results are significant: taking Select Topics was helpful to third quartile students in passing the California Bar Examination.[140]

C. Adjustments Made Due to the July 2010 Results

As remarked upon earlier, the July 2010 results were disappointing, although somewhat consistent with the national trend suggested by the data provided earlier.[141] Chapman's first-time bar passage rate on that administration dropped to 72% for the graduating class, and 70% for all first-time takers.[142]

The July 2010 results may have been an anomaly, due in part to the national decline, which itself may have been due in part to a first-time effort by the largest commercial provider, BarBri, to compete with other companies by offering their

138 Calculations on file with the author.

139 On file with the author.

140 Calculations on file with the author.

141 Smythe, *supra* note 14, at 21–22.

142 Data for the graduating class on file with the author. The first-time pass rate for Chapman overall in July 2010 is also found at STATE BAR OF CAL., GENERAL STATISTICS REPORT: JULY 2010 CALIFORNIA BAR EXAMINATION 4 (2011), http://admissions.calbar.ca.gov/LinkClick.aspx?fileticket=ECWYhV4t0wE%3d&tabid=2269 [http://perma.cc/P82D-GFNM]. The difference is due to several students from earlier classes who took the bar examination but did not participate in any of Chapman's bar preparation programs.

lectures online. At Chapman, this resulted in a large drop in attendance in the regimented BarBri classes. Anecdotally, BarBri officials told the author that they experienced a drop in both attendance in bar review classes and pass rates nationally in July 2010. As a result of the July 2010 results, both BarBri and Chapman now constantly notify students that bar passage rates are lower for students who study online rather than attending classes, which notification has resulted in much more consistent attendance at Chapman for the commercial review "live" lectures in the years since 2010.

This also suggests another reason that law schools should not rely entirely on commercial reviews for preparing their students for the bar examination. Commercial reviews provide a product, but once they are paid, they do not insist that students use the product, nor do they continually urge students to do the work in using the product. While students can track their progress using the commercial reviews' software, no one will be calling students or meeting with students to push them to do the work. But law schools can be more of a presence in their students' study lives. Where a law school offers essays and other practice sessions, faculty teaching bar preparation can track student effort and participation and remind students who are not writing enough or whose attendance has fallen to get back on track.

D. Effect of Essay Practice and Feedback: Statistical Analysis

Not only does it appear that Chapman's bar preparation programs are helpful, but it also seems that essay writing and feedback are a significant factor in the program's success. The bar passage results suggest that more practice, and thus more intensive work, do in fact translate into higher bar passage for all students. This result, if correct, is another persuasive reason why law schools should take a greater hand in running bar preparation courses that require significant work and are available to all the school's students.

As discussed in Part IV, because commercial bar reviews often limit significantly the amount of practice essays that can be turned in, since July 2009, Chapman has permitted students to turn in essays and performance tests for twenty-four-hour turnaround in feedback. Until the summer 2014 Supplemental Program, students could turn in as many essays as they wanted. There is now a cap of thirty-five essays per student, which we have determined is a sufficient number from the perspective of the student's performance and to provide the needed amount of

practice and feedback, while maintaining reasonable logistical limits on faculty labor.

Intuitively, it would seem that the more essays a student writes for feedback, the more likely the student will pass the bar examination. The author decided to test this hypothesis, again using a chi-square analysis applied to a multivariate distribution based on the number of essays submitted on the Supplemental Program TWEN page and bar passage.

Data was available from the 2011, 2012, and 2013 Supplemental Programs through archived TWEN pages. For each student, the number of essays they submitted on TWEN, as well as whether they passed or failed the bar examination on their first attempt, could be tracked. As a consequence, for each of the three years, results could be allocated based on the number of essays submitted, a variable that served as a representative of work ethic in studying for the bar examination. For each of the three years, a 2 x 7 table was created: one variable was bar passage (pass or fail); and the other variable was number of essays submitted (40+; 30–39; 25–29; 20–24; 15–19; 10–14; 0–9).

The tabular results are as follows:

July 2011[143]

Total Essays Submitted	Pass	Fail	Total
40+	9	2	11
30–39	7	3	10
25–29	6	2	8
20–24	7	2	9
15–19	14	0	14
10–14	18	3	21
0–9	64	22	86
Total	125	34	159

The chi-square test for two or more independent samples with one nominal variable is calculated for an r by k contingency table as follows:

$$\chi^2 = \sum_{i=1}^{rk} (o_i^2 / e_i) - n$$

As before, o represents each observed cell frequency, and e represents the expected frequency. Thus, for example, 29 students submitted 25+ total essays, so the expected frequency assuming a null hypothesis in the relationship between essays

143 On file with the author.

submitted and bar passage would be 14.5 students in both the "Pass" and "Fail" cells. The *n* variable means the total number of students who took the July 2011 Bar Examination for the first time—in this case, 159 students.

Applying the formula results in a χ^2 value of 54.4976. The degrees of freedom for a 7 x 2 matrix equals (7−1)(2−1) = 6. As is typical and accepted, the null hypothesis can be rejected if the chi-square value of 54.4976 exceeds the critical chi-square value within six degrees of freedom at the .05 significance level. This means that the probability of error is .05 or smaller. At the .05 significance level, for six degrees of freedom, the chi-square value must exceed 12.59. A chi-square of 54.4976 in fact suggests that the probability of error is less than .005 (1/2 of 1%), because it exceeds the critical chi-square value for six degrees of freedom at that level of 18.55. Thus, the null hypothesis can be rejected, and it appears that the results are statistically significant, if not intuitive: writing more and more essays was helpful in passing the California Bar Examination.

The results for July 2012, July 2013, and July 2014 were similar. See the following tables for those examination administrations:

July 2012[144]

Total Essays Submitted	Pass	Fail	Total
40+	15	1	16
30–39	16	2	18
25–29	11	0	11
20–24	11	0	11
15–19	18	2	20
10–14	20	7	27
0–9	37	17	54
Total	128	29	157

July 2013[145]

Total Essays Submitted	Pass	Fail	Total
40+	34	5	39
30–39	15	4	19
25–29	11	2	13
20–24	13	5	18
15–19	13	2	15
10–14	8	1	9
0–9	24	20	44
Total	118	39	157

144 On file with the author.
145 On file with the author.

July 2014[146]

Total Essays Submitted	Pass	Fail	Total
40+	10	1	11
30–39	16	3	19
25–29	16	6	22
20–24	11	3	14
15–19	20	1	21
10–14	7	2	9
0–9	14	16	30
Total	94	32	126

The χ^2 values for July 2012, July 2013, and July 2014 are 71.6055556, 35.8839534, and 45.47684, respectively. As was true with the July 2011 exam, there are six degrees of freedom, so that the minimum chi-square value at the 0.05 significance level is 12.59, and the minimum chi-square value at the 0.005 significance level is 18.55. Thus, the results for all four years suggest that the null hypothesis is disproven, and that the results are statistically significant at least to the 0.005 significance level.

Moreover, all four years show the same pattern: high pass rates when students write more than ten essays each, and a markedly lesser success rate at 0–10 essays (a nearly fifteen percentage point drop in the pass rate for those who submitted 1–9 essays and a nearly twenty percentage point drop in the pass rate for those who submitted no essays).[147] I have seen a tendency, particularly with our encouragement, for students to write an almost equal number of essays that they self-check against model answers, so even students who turn in about 10□20 essays in fact write double that number, which partially explains why the success rate increases at the 10 essays or more level.[148] Nevertheless, to insure full coverage among the thirteen or more different essay subjects on the California Bar Examination, I recommend that students turn in at least 20–25 essays for grading, and this study suggests that students who do so will be highly successful.

As noted earlier, Chapman has now instituted a cap on essay submissions of 35 essays per student. The following chart

146 On file with the author.

147 *See supra* tabular results chart p. 589 and note 143.

148 A further explanation may be that, even before students take the Supplemental Program, almost all of them take the for-credit bar preparation course (Select Topics), which requires them to write two essays for each of the twelve subjects, for a total of twenty-four essays. *See supra* Section IV.B. Therefore, most students who succeed write a minimum of nearly thirty-five essays.

illustrates the results for July 2011–2014 for students who wrote more than 35 essays and those who wrote 35 or fewer.

Combined July 2011–2014[149]

Total Essays Submitted	Pass	Fail	Total
36+	79	11	90
0–35	386	123	509
Total	465	134	599

Those who wrote 36 or more essays passed at a rate of 87.78%, which is only marginally more than the pass rate for those submitting at least 20 essays. Furthermore, the combined pass rate for those submitting 20–35 essays in that same time period was 82.91% (131 passed and 27 failed),[150] so again, there is only a marginal increase in pass rate for submissions over 35 essays.

These results seem to validate the decision to adopt a cap of 35 submissions per student. By recommending at least 20 essays per student, and capping the number at 35 essays, the program accommodates students who need to be pushed to write as many as 20 essays in order to achieve success on the bar examination, but allows for the highly motivated student who writes a higher number of essays, without over-burdening faculty with too many students writing too many essays.

At the other end, however, as mentioned above, the drop off in success among those who do not write essays or write fewer essays is apparent.

Combined July 2011–2014[151]

Total Essays Submitted	Pass	Fail	Total
10+	325	60	385
1–9	93	42	135
0	47	32	79
Total	465	134	599

Those who submitted 10 or more essays passed at an overall rate of 84.42% on these three administrations. Those who submitted 1–9 essays passed at an overall rate of 68.89%. Finally, those who submitted no essays (almost all of whom did participate in the Supplemental Program sessions nevertheless)[152]

149 On file with the author.
150 On file with the author.
151 On file with the author.
152 On file with the author.

passed at an overall rate of 59.49%. Thus, it seems that, at a minimum, turning in at least 10 essays for feedback was a break point for effectiveness in substantially increasing the pass rate to the 80% or better level.

This is confirmed by the chi-square analysis: $\chi^2 = 204.5174$. Since, at the .005 significance level, for two degrees of freedom, the chi-square value must exceed 10.60, the chi-square value of 204.5174 suggests that the probability of error is less than .005 (1/2 of 1%).

Our results also suggest that the group helped the most by this work ethic are third quartile students. This can be shown by the following charts:

July 2014: Third Quartile Students[153]

Total Essays Submitted	Pass	Fail	Total
25+	8	3	11
20–24	4	0	4
15–19	4	1	5
10–14	3	1	4
0–9	5	2	7
Total	24	7	31

July 2013: Third Quartile Students[154]

Total Essays Submitted	Pass	Fail	Total
25+	14	2	16
20–24	4	1	5
15–19	5	0	5
10–14	2	0	2
0–9	7	4	11
Total	32	7	39

July 2012: Third Quartile Students[155]

Total Essays Submitted	Pass	Fail	Total
25+	10	0	10
20–24	2	0	2
15–19	6	0	6
10–14	11	0	11
0–9	7	3	10
Total	36	3	39

153 On file with the author.
154 On file with the author.
155 On file with the author.

The chi-square for pass rates by essays submitted by third quartile students in 2014 was 10.35844; the chi-square for pass rates by essays submitted by third quartile students in 2013 was 39.0; and the chi-square for pass rates by essays submitted by third quartile students in 2012 was 99.5. With a minimum chi-square value at the 0.05 significance level of 9.49, and a minimum chi-square value at the 0.005 significance level of 14.26, the results for third quartile students, showing that third quartile students who write 10 or more essays passed at a 93.6% rate in 2012, an 89.3% rate in 2013, and at a 79.17% rate in 2014, are also highly significant.[156] Thus, like students overall, including the first and second quartiles, third quartile students were aided by writing and receiving feedback on more essays.

While fourth quartile students did better by submitting more essays, it appeared as if it required more essay writing for that group. Significant improvement in pass rates was not observed except among those who wrote 25 or more essays for submission. The pass rate for fourth quartile students who wrote 25 or more essays tended to approach (and in 2012 to exceed) a 50% pass rate, as compared to overall pass rates for all students ranging between 77% and 82%.[157]

Therefore, the empirical data suggest that there is a range where labor-intensive supplemental bar preparation programs open to all students, particularly those where students are motivated to write substantial numbers of essays and faculty grade substantial numbers of essays in a quick turnaround, are quite productive and helpful to most students. Some students need to be motivated to write enough essays, and some students need to be limited so they do not write too many essays. A program that promises quick feedback to every student who writes between 10 and 35 essays (with encouragement that they submit at least 20 essays) also holds the promise of the greatest opportunity for the greatest range of students to pass the bar examination on the first attempt.

Nevertheless, there may well be limitations on how much of a conclusion we can draw from these results. For example, one could suggest that the number of essays a student submits is highly correlated with work ethic, and thus highly correlated with their law school GPA. This would further suggest that it is whatever other factor made the student a good student that makes it more likely they would pass. It is true that this study does not attempt to control for other factors, such as work ethic,

156 On file with the author.
157 On file with the author.

but it does control somewhat for law school GPA. The third quartile pass rates for the July 2009, 2011, 2012, 2013, and 2014 California Bar Examinations have reached 86.11%, 82.05%, 92.31%, 92.05%, and 77.42% respectively.[158] In the several years before adoption of the program, third quartile pass rates approximated 69%.[159] Similarly, while in the several years before adoption of the program, the fourth quartile pass rates ranged between 20% and 30%,[160] those rates for the July 2009, 2011, 2012, and 2013 California Bar Examinations have reached 50.00%, 42.5%, 45.0%, 35.9%, and 40.6%, respectively.[161]

Still, it cannot be said with certainty that the program, or requiring more essay work, are the sole, or even the primary, contributing factors in the rise of bar passage rates at Chapman. Nevertheless, the analyses that we have done suggest that bar passage has improved and is significantly linked to the programs and the students' work effort at all levels of law school GPA. At a minimum, these results suggest that this is a program that should be looked at as a possible source of ideas for designing bar preparation programs.

Still, no program is perfect, given that it is run by humans, none of whom are perfect. The Chapman program clearly had a tendency to try to deliver too much in terms of services, resulting in the decision to cap the essays that could be submitted. The program still does not have a way to ensure that the students most in need of writing the most essays in fact write them and turn them in. One possible need might be to monitor student essay production on a weekly basis—for those students who are not turning in sufficient essays, send them reminders to increase essay production, or directly meet with those students to urge them, face-to-face, to increase their essay work.

Moreover, the Chapman program could probably benefit from a greater diffusion of effort among the essay graders and among the faculty teaching in the program to ensure a fairer distribution of that effort.

Finally, given the statistical analysis, our message to students can be more tightly honed, so that we can explain with greater clarity how many essays should be written, and why. These results can help us help the students to reach a good balance of effort among class time, study time, outlining, MBE preparation, and essay and performance test writing.

---

158 On file with the author.
159 On file with the author.
160 On file with the author.
161 On file with the author.

As I suspect anyone who spends significant time helping students prepare for the bar examination knows, there are some things we can never control: sudden illnesses, family emergencies, emotional catastrophes, relationship breakups, and other factors that affect a student's performance on the bar examination. We hope that, by adopting programs designed to increase practice and feedback, those uncontrollable occurrences will have less of an impact than they otherwise might.

CONCLUSION

In light of the increase in underpreparedness of law students and decrease in admissions statistics, most law schools that are concerned with bar passage should accept the following if they are going to take truly effective steps to provide their students with the best opportunities to pass the bar examination:

- Unlike traditional academic support programs, bar preparation courses and supplemental bar preparation programs must be open to all students, since a greater fraction of the cohort is less prepared than in past years, and therefore, more students are increasingly at risk on the bar examination.
- Students should be made to feel as though they are all one team, rather than differentiating students based on perceived notions of "risk" or other descriptors.
- Faculty and academic support professionals engaged in providing bar preparation courses and services must both demand extensive work, and be prepared to expend significant time and effort themselves.
- Faculty and academic support professionals engaged in providing bar preparation courses and services must provide opportunities for students to write twenty to thirty-five essays for grading during a supplemental bar preparation program, as well as additional personalized and individual assistance, whether in the form of one-on-one tutoring, responsiveness to a multitude of student questions on substantive law, or live structured classes on multistate subjects and multiple choice questions, with classrooms receptive to student discussion of these multiple choice questions.
- If we expect students to treat bar exam study as a "full-time job," then we must ourselves treat it as a full-time job and more, and be willing to expend

> whatever time is needed to deliver individualized assistance in writing, analysis, and practice to all of our students.

Law teaching, and particularly preparing students for the bar examination, is more than a job. In fact, it is a calling, and a mission. Given the cost of a legal education, we owe no less to our students than to dedicate *whatever time it takes* to help them get ready. As this Article demonstrates, that expenditure of time—whether it is 50 hours a week or 125 hours a week—seems well worth it to each student who benefits from our effort.

There is no one perfect way to prepare students for the bar examination. Unfortunately, as this Article has indicated, there are not all that many published studies detailing the nuts and bolts of programs, and statistically evaluating them. This leaves us with little information to study and compare the effectiveness of various approaches, and it limits our ability to learn from each other in the academy. We would invite others with bar preparation programs to evaluate their programs as Richmond, UDC, and Chapman have done, and to publish their results. This will allow all of us in the academic support community, as well as law school administrators and faculty, to collectively learn from each other and improve our programs and the delivery of these programs to our students. This is a goal of rising importance and concern as we, as law teachers, prepare to deliver programs to students whose preparedness for law school and qualifications for law school differ markedly from what we have seen in the past.

The Cost of Sharing and the Common Law: How to Address the Negative Externalities of Home-Sharing

*Tristan P. Espinosa**

INTRODUCTION

Over the past several years, the "sharing economy" has proven more challenging to regulate than perhaps any other commercial industry in recent decades. An exact definition of the "sharing economy" is hard to pin down, however, the term is typically thought to refer to companies that either "(1) own goods or services that they rent to consumers on a short-term basis, or (2) create peer-to-peer ("P2P") platforms connecting providers and users for short-term exchanges of goods or services."[1] The variety of companies that embody the sharing economy are as numerous as they are creative, and each presents its own set of regulatory needs and challenges. Yet of the companies that comprise the "sharing-economy," the need for regulation is most apparent for companies that provide for home-sharing, such as Airbnb, Inc., HomeAway, Inc., and Couchsurfing International, Inc. Though their respective target demographics differ, each of these home-sharing providers are similar in that they create digital P2P marketplaces that allow users all over the globe to rent and lease empty space in their homes for the short-term. While this practice is economically beneficial in a number of respects (utilization of an untapped resource, financial gain, increased tourism, etc.), oftentimes such benefits come at the expense of others.

When a user of one of the above-referenced home-sharing websites lives in a residential neighborhood and lists their property as a short-term rental, they are essentially commercializing a residential area. Unregulated, this activity causes nuisances in single-family-neighborhoods typically associated with commercial activities, such as noise, traffic, and transients. Such nuisances threaten the integrity of single-family

* J.D., Chapman University Dale E. Fowler School of Law, May 2016.

1 Daniel E. Rauch & David Schleicher, *Like Uber, But for Local Governmental Policy: The Future of Local Regulation of the "Sharing Economy"* 2 (George Mason Law & Econ. Research Paper No. 15-01, 2016).

neighborhoods and the property values of the homes therein, causing outrage amongst the residents in the neighborhood who chose not to rent out space in their homes. But it is not only residential areas that are affected, for even if a user of a home-sharing website lists an apartment for rent short-term, rather than a single-family-home, harm to the general public still results. As one apartment goes up for rent on a home-sharing website, one unit of housing disappears from the regular rental market.[2] In many cities this practice has an exacerbating effect on the housing market, causing availability to fall and the cost of living to rise.[3]

Compelled by the threat that home-sharing poses to single-family neighborhoods and its negative impact on the rental housing market, cities across the United States have attempted to regulate digital home-sharing markets.[4] These regulations are based on traditional, business-to-consumer business models and thus target the actual suppliers of short-term rentals—those who list properties for rent on home-sharing websites—rather than the platform providers, i.e. the websites.[5] However, because home-sharing websites utilize P2P business models, supply of the service is decentralized, rendering regulations based on a business-to-consumer model largely ineffective.[6] This is because the decentralized nature of home-sharing makes it difficult for violators of regulations to be discovered, thereby reducing

---

2 *See generally* L.A. DEP'T OF CITY PLANNING, HOUSING ELEMENT 2013-2021, CHAPTER 1: HOUSING NEEDS ASSESSMENT (Dec. 3, 2013), http://planning.lacity.org/HousingInitiatives/HousingElement/Text/Ch1.pdf [http://perma.cc/5MFQ-G5WF].

3 *Id.*

4 To name just a few, San Francisco, Los Angeles, New York, Portland, Chicago, and Philadelphia are cities that are currently attempting to regulate home-sharing. *See* Marielle Mondon, *S.F. Is Struggling to Make Good on Airbnb Regulation*, NEXT CITY (Mar. 25, 2015), http://nextcity.org/daily/entry/san-francisco-airbnb-regulation-problems [http://perma.cc/3AJP-FD47]; Robert Holguin, *Los Angeles City Leaders Want to Regulate Home-Sharing Websites Like Airbnb*, KABC EYEWITNESS NEWS (Dec. 5, 2014), http://abc7.com/news/la-city-leaders-want-to-regulate-home-sharing-websites-like-airbnb/424126/ [http://perma.cc/WD8Z-KBDD]; Ronda Kaysen, *What's Up Next in New York? Airbnb and Rent Regulation Will Be Hot Topics*, N.Y. TIMES (Dec. 26, 2014), http://www.nytimes.com/2014/12/28/realestate/new-york-airbnb-and-rent-regulation-will-be-hot-topics.html?_r=0 [http://perma.cc/K23B-2QRT]; Steve Law, *Airbnb Resists City Efforts to Regulate It*, PORTLAND TRIB. (Dec. 18, 2014, 8:14 PM), http://portlandtribune.com/pt/9-news/244479-112102-airbnb-resists-city-efforts-to-regulate-it [http://perma.cc/YAB7-P5LH]; Alby Gallun & Ally Marotti, *Hotels to Airbnb Hosts: Pay Up*, CRAIN'S CHI. BUS. (Feb. 14, 2015), http://www.chicagobusiness.com/article/20150214/ISSUE01/302149989/hotels-to-airbnb-hosts-pay-up [http://perma.cc/MLD6-8FAC]; Mike Dunn, *Phila. Lawmakers Move Toward Regulating, and Taxing, Airbnb Room Rentals*, CBS PHILLY (June 1, 2015, 2:05 PM), http://philadelphia.cbslocal.com/2015/06/01/phila-lawmakers-move-toward-regulating-and-taxing-airbnb-room-rentals/ [http://perma.cc/J974-GH6V].

5 *See infra* Part II.

6 *Id.*

incentive to comply. Thus in several cases, even where regulations prohibit home-sharing in a specific neighborhood or area, because there is substantial profit to be made and little chance of discovery, home-sharing continues, unabated.[7]

If regulatory efforts fail, the costs of home-sharing are borne by those who are not involved in its practice ("non-sharers").[8] In single-family neighborhoods, non-sharer residents continue to experience nuisances typically associated with commercial activity, resulting in the loss of enjoyment of their property and a potential decrease in the monetary value of the property.[9] At the same time, non-sharer inhabitants of rental dwellings in the city continue to experience rent increases, causing the cost of living to rise.[10] As these problems continue, the number of aggrieved parties will grow and the aggregate damages will become substantial. As history has shown, once a tipping point is reached, a lawsuit will follow—a lawsuit that may just be the cost-shifting mechanism needed to address the negative externalities caused by home-sharing.

Based on precedent cases involving P2P business models and common-law rules of third-party liability, a class of individual landowners may one day bring and win a monumental lawsuit against home-sharing websites that will change the way home-sharing websites operate within the United States. While

---

7 Examples of regulation failure can be observed most clearly in San Francisco and Los Angeles. *See* Emily Alpert Reyes, *Los Angeles Gives Hosts, Neighbors Mixed Signals on Short-term Rentals*, L.A. TIMES (Feb. 7, 2015, 10:00 AM), http://www.latimes.com/local/california/la-me-adv-illegal-rentals-20150208-story.html#page=1 [http://perma.cc/FWJ7-DYSY]; *see also* Matt Weinberger, *San Francisco Complains It Can't Enforce Its Own Airbnb Law*, BUS. INSIDER (Mar. 23, 2015, 4:41 PM), http://www.businessinsider.com/san-francisco-calls-airbnb-regulations-unenforceable-2015-3 [http://perma.cc/F7J6-3VZS].

8 *See* Steven Leigh Morris, *Airbnb Is Infuriating the Neighbors. Is It Time for New Rules?*, L.A. WKLY. (Jan. 22, 2015, 2:47 PM), http://www.laweekly.com/news/airbnb-is-infuriating-the-neighbors-is-it-time-for-new-rules-5343663 [http://perma.cc/GL67-3ECU]; Benjamin Mueller, *Hearing Pits Tenants Who Denounce Airbnb Against Those Who Profit From It*, N.Y. TIMES (Jan. 20, 2015), http://www.nytimes.com/2015/01/21/nyregion/ hearing-pits-tenants-who-denounce-airbnb-against-those-who-profit-from-it.html [http://perma.cc/KC4V-8NZM].

9 *See* Morris, *supra* note 8; *see also* Walter Hamilton, *Renting Rooms Through Airbnb Riles Fellow Homeowners*, SEATTLE TIMES (Sept. 19, 2013, 6:56 PM), http://www.seattletimes.com/business/renting-rooms-through-airbnb-riles-fellow-homeowners/ [http://perma.cc/KL2S-M5AB].

10 *See* Daniel Hirsch, *Report: Airbnb Cuts into Housing, Should Share Data*, MISSION LOCAL (May 14, 2015, 5:00 PM), http://missionlocal.org/2015/05/report-airbnb-cuts-into-housing-should-give-up-data/ [http://perma.cc/5TB6-2AUS]; Caroline O'Donovan, *The Rent Is Too Damn High: In Search of the Truth About Airbnb's Impact on Housing*, BUZZFEED NEWS (June 9, 2015, 3:59 PM), http://www.buzzfeed.com/carolineodonovan/the-rent-is-too-damn-high-the-truth-about-airbnbs-impact-on#.mqaP1YmG5 [http://perma.cc/X2ZY-P6LD]; *see also* Rachel Monroe, *More Guests, Empty Houses*, SLATE (Feb. 13, 2014, 8:08 AM), http://www.slate.com/articles/business/moneybox/2014/02/airbnb_gentrification_how_the_sharing_economy_drives_up_housing_prices.html [http://perma.cc/H9BM-RR8U].

home-sharing is a recent phenomenon, digital P2P markets have been around since the late 1990s, and have already been the impetus for a pair of pivotal judicial decisions.

In 1999, a class of recording producers brought suit against the infamous Napster Inc.,[11] and in 2004, a class of film producers brought suit against Grokster Ltd., Napster's more sophisticated cousin.[12] Interestingly, the stories of these lawsuits are remarkably similar. In each case, a company utilized a business model based on digital P2P marketplaces,[13] and each company thrived for a time, but at the expense of other entities in their respective industries. Eventually the costs which had been passed on to the other companies in the industry grew so large, it came to a tipping point, and a class-action lawsuit was brought. As a result, both Napster and Grokster were held accountable for the negative externalities each had caused.[14] Napster and Grokster were then left to either abandon their business for fear of future lawsuits, or re-evaluate their business models and conceive methods of doing business lawfully. In other words, Napster and Grokster were compelled by lawsuits to address and mitigate the negative externalities each had caused.

These cases exemplify how the common law can act as a cost-shifting mechanism for the negative externalities of P2P markets, and provide a framework outlining more effective regulations for home-sharing. Despite the fact that legislative regulation fails to shift the costs of harms caused by home-sharing back onto the companies that create them, the costs can still be shifted—and home-sharing can be successfully regulated—if a class of plaintiffs successfully brings suit against a home-sharing company. Once a lawsuit is successful, home-sharing companies will be compelled to re-evaluate their business practices and formulate methods of conducting business that do not expose the company to liability.

This Comment is divided into three parts. Part I details two of the most common negative externalities caused by home-sharing, identifies who bears the costs of those externalities, and discusses the legislative attempts by various

---

11 *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).

12 *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 919 (2005).

13 *Id.*; *see also supra* note 11.

14 *See* Ron Harris, *Napster Offers $1 Billion Settlement*, ABC NEWS (Feb. 20, 2001), http://abcnews.go.com/Technology/story?id=98832 [http://perma.cc/DUY6-KBWA]; *see also* Ben Fritz, *Grokster Plays Nice by Turning Radio Dial*, VARIETY (Nov. 15, 2004, 3:56 PM), http://variety.com/2004/biz/markets-festivals/grokster-plays-nice-by-turning-radio-dial-1117913569/ [http://perma.cc/CFZ6-LYKR]; John Borland, *Last Waltz for Grokster*, CNET (May 30, 2006, 11:10 AM), http://www.cnet.com/news/last-waltz-for-grokster/ [http://perma.cc/J7AU-EJMC].

municipalities to address them. Part II explains why legislative attempts to address negative externalities of home-sharing are ineffective. Part III then offers how, based on precedent P2P cases and common law rules of private nuisance and third-party liability, the common law is an adequate mechanism for shifting the costs of the negative externalities of home-sharing onto the companies that create them, so that these companies may finally be successfully regulated.

I. THE NEGATIVE EXTERNALITIES OF HOME-SHARING

Generally speaking, a negative externality is an indirect cost of a commercial activity that is borne by society or bystanders outside of the industry rather than the commercial enterprise or individuals conducting the activity.[15] The number of negative externalities that result from the unregulated, wide-spread practice of short-term renting made possible by home-sharing websites are numerous and substantial. However, there are two externalities in particular that are most common in cities across the United States: the negative effect of wide-spread home-sharing on residential neighborhoods, and the negative effect of wide-spread home-sharing on the rental housing market.

A. The Effect of Home-Sharing on Residential Neighborhoods

Los Angeles, California has experienced nearly all of the negative externalities associated with home-sharing on residential areas given the density and high cost of living. As is the case in many Los Angeles areas, home-sharing is a popular practice in the neighborhood of Silver Lake.[16] In 2013, Silver Lake was the location of at least 200 listings for short-term rentals on Airbnb.com, ranging from studio apartments for $60 per night, to entire homes complete with swimming pools for $425 per night.[17] Yet despite the numerous home-sharers in the area, many residents were strongly opposed ("non-sharers") to the practice of home-sharing in their neighborhood. In fact, the non-sharers of Silver Lake were so opposed to home-sharing that they eventually petitioned their local government to enact an outright ban on short-term renting through home-sharing websites like Airbnb.com in the neighborhood.[18]

---

15 Thomas Helbling, *What Are Externalities?*, FIN. & DEV. (December 2010), http://www.imf.org/external/pubs/ft/fandd/2010/12/pdf/basics.pdf [http://perma.cc/783F-2JNW].

16 *Will Airbnb Have to Check Out of Silver Lake?*, EASTSIDER (Aug. 14, 2013), http://www.theeastsiderla.com/2013/08/will-airbnb-have-to-check-out-of-silver-lake/ [http://perma.cc/3KG3-8SQA].

17 *Id.*

18 *Id.*

Non-sharers in Silver Lake opposed home-sharing with as much vigor and animosity as they would the development of a commercial short-term rental establishment such as a hotel or inn. They asserted that the "hotel-like room rentals," made available by home-sharing websites like Airbnb.com "bring transients, traffic," and "create potential safety issues."[19] These are legitimate concerns for homeowners because property values are typically higher in quieter, secluded, crime-free areas.[20] But when land is put to commercial use, such as a hotel or retail store, the noise and traffic levels of the area increase as a result of people coming and going, and the transient nature of the establishment can increase the crime rate.[21] Thus, by their nature, commercial uses in residential areas cause the values of the surrounding residential properties to fall, and the loss of value is borne by the residents, not the home-sharing websites.[22]

In an effort to mitigate the negative impact of home-sharing on the neighborhood and restore their properties to their original perceived value, the non-sharers of Silver Lake petitioned the neighborhood council to pass a resolution that would ban all short-term rentals within the neighborhood.[23] At a meeting to discuss the resolution, more than 150 residents of Silver Lake appeared.[24] While there were plenty of non-sharers present to bemoan the parking shortages, increased transients, and excessive noise caused by home-sharing,[25] also present at the hearing were members of "Peers," an Airbnb lobbyist group whose self-proclaimed mission is "to grow the sharing economy, to mainstream it, to tell its story, and to protect it."[26] Ultimately, the non-sharers were outnumbered by the Peers, and the resolution to ban short-term renting on home-sharing websites did not pass.[27]

---

19 *Id.*

20 Mandi Woodruff, *9 Things That Will Trash Your Home's Value*, BUS. INSIDER (May 13, 2013, 9:30 AM), http://www.businessinsider.com/what-hurts-home-value-2013-5?op=1 [http://perma.cc/N2CY-EX35].

21 *See generally* John M. Quigley & Larry A. Rosenthal, *The Effects of Land Use Regulation on the Price of Housing: What Do We Know? What Can We Learn?*, 8 CITYSCAPE: 1 J. POL'Y DEV. & RES. 69 (2005), https://www.huduser.gov/periodicals/cityscpe/vol8num1/ch3.pdf [http://perma.cc/GXF7-8YGA].

22 *Id.*

23 Neal Broverman, *Silver Lakers Want to Ban Airbnb Rentals in Their Neighborhood*, CURBED L.A. (Aug. 14, 2013, 6:16 PM), http://la.curbed.com/archives/2013/08/silver_lakers_want_to_ban_airbnb_rentals_in_their_neighborhood.php [http://perma.cc/N7Y6-XKYN].

24 Zak Stone, *The Battle Over Airbnb Moves to Los Angeles*, CO.EXIST (Sept. 17, 2013, 8:23 AM), http://www.fastcoexist.com/3017486/the-battle-over-airbnb-moves-to-los-angeles [http://perma.cc/LYU4-3YTM].

25 *Id.*

26 *Id.*

27 *Id.*

Regardless of who won the battle of Silver Lake, it is clear that unregulated home-sharing has a costly impact on residential communities. Similar disputes over whether home-sharing should be regulated have taken place not only in other neighborhoods throughout California such as Venice and West Hollywood, but also in cities across the United States including New Orleans, Louisiana, and Portland, Oregon.[28] Thus, it would seem that no matter the city, widespread unregulated home-sharing brings nuisances to residential areas, thereby lowering the values of all homes in the neighborhood, and leading non-sharers to demand regulation. While the story of Silver Lake demonstrates that, for the time being, non-sharers are in the minority, this does not change the fact that the cost of the degradation of the neighborhood is borne by residents who do not participate in home-sharing.

B. Pressure on Housing Market

In addition to the costs that home-sharing places on non-sharing homeowners in single-family neighborhoods, the proliferation of home-sharing also generates costs for renters.[29] Home-sharing websites reduce traditional barriers to entry into the hotel industry, and thus, more and more landlords and leasing companies are converting long-term rental units into permanent short-term rental units or de facto hotels.[30] As a result, the number of rental units available on the market is falling, and the market is shrinking.[31] Such shrinkage has an exacerbating effect on the high cost of living in dense areas such as San Francisco, New York City, and Los Angeles.[32] But just like the cost of lowered property values in single-family neighborhoods, this higher cost of living is borne by those who do not participate in home-sharing.

---

28 *See* Stevie St. John, *Airbnb Is Raising the Ire of WeHo Apartment Managers and Tenants*, WEHOVILLE (Mar. 14, 2014), http://www.wehoville.com/2014/03/14/airbnb-raising-ire-weho-apartment-managers-tenants/ [http://perma.cc/CNE5-AYVK]; *see also* Juliet Bennett Rylah, *WeHo Might Ban Airbnb*, LAIST (Feb. 4, 2015, 1:15 PM), http://laist.com/2015/02/04/weho_considers_banning_airbnb.php [http://perma.cc/U5U7-8N9A]; Robert McClendon, *Battle Brewing over Short-Term Rentals, as Residents Discuss Airbnb*, TIMES-PICAYUNE (May 20, 2014, 9:51 PM), http://www.nola.com/politics/index.ssf/2014/05/battle_brewing_over_bed_and_br.html [http://perma.cc/H34E-K28M]; Elliot Njus, *Portland Tries to Make Peace with Airbnb as 'Sharing Economy' Moves into the Mainstream*, OREGONIAN (Jan. 31, 2014, 5:18 AM), http://www.oregonlive.com/front-porch/index.ssf/2014/01/airbnb-style_vacation_rentals.html [http://perma.cc/7WTK-CRP7].

29 *See* L.A. DEP'T OF CITY PLANNING, *supra* note 2.

30 *See generally* Denise Cheng, *Is Sharing Really Caring? A Nuanced Introduction to the Peer Economy*, OPEN SOC'Y FOUND. (Oct. 2014), http://static.opensocietyfoundations.org/misc/future-of-work/the-sharing-economy.pdf [http://perma.cc/4VRE-E2PK].

31 *See* Hirsch, *supra* note 10; O'Donovan, *supra* note 10.

32 *See* L.A. DEP'T OF CITY PLANNING, *supra* note 2, at 1–3.

In some respects, the practice of home-sharing is fairly consistent with the practice of running a hotel. Generally speaking, the success of any given hotel can be attributed to its reputation and visibility.[33] Hotels spend hundreds of thousands of dollars on amenities and employees in order to gain the reputation of a clean, comfortable, and safe hotel.[34] In addition, hotels spend significant sums of money on advertising in order to increase visibility and draw guests. Successful home-sharing relies on similar techniques. Just like a hotel, home-sharers must establish their reputation, and then advertise their short-term rental properties in order to draw guests. But where hotels have money to spend on amenities and advertising, the average homeowner or renter does not.

If in fact a homeowner or renter had a spare room and was willing to rent it short-term, the search for a short-term tenant could be challenging and ineffective. Advertising for the room would be done either on community bulletin boards, newspapers, or word-of-mouth. Granted, the emergence of Craigslist made advertising easier and more effective (as anyone with an internet connection gained the ability to broadcast an advertisement capable of reaching unlimited viewers), but as the breadth of the advertisement increased, so did the risk for hosts and guests.[35] Once the advertisement spreads beyond the scope of the neighborhood, would-be hosts and guests have no way to vet one another.[36] Therefore, prior to the recent rise of home-sharing websites, for most prospective home-sharers advertising a residential property as a short-term rental either failed to reach enough prospective guests or it posed an unacceptable degree of risk, and thus home-sharing occurred on a much smaller scale.[37]

---

33 *See generally* Pedro Colaco, *10 Success Tips on Online Visibility for Independent Hotels*, HOTEL BUS. REV., http://hotelexecutive.com/business_review/2120/10-success-tips-on-online-visibility-for-independent-hotels [http://perma.cc/DAP9-UKT5]; Vanessa Horwell, *How to Market Your Hotel Today for Success Tomorrow*, HOTEL BUS. REV., http://hotelexecutive.com/business_review/2139/how-to-market-your-hotel-today-for-success-tomorrow [http://perma.cc/4EBE-THMJ].

34 *See* Sam Trotter, *How Much Does it Cost to Build a Hotel – 2015*, BOUTIQUE HOSPITALITY MGMT. (Feb. 11, 2015), http://www.boutique-hospitality.com/how-much-does-it-costs-to-build-a-hotel-2015/ (stating midscale hotels spend on average $95,600 on building and site improvements; full service hotels spend roughly $193,600; and luxury hotels and resorts spend roughly $392,600) [https://perma.cc/3VJB-3L26].

35 David C. Wyld, *Renter Beware: Craigslist is Fast Becoming the Go-to Site for Rental Property, But the Lack of Trustworthiness Makes the Prospect of Renting Via the Internet a Very Risky Proposition Indeed*, WEB.ARCHIVE (June 7, 2012) https://web.archive.org/web/20160115133914/https://www.escrow.com/news/Articles/craigslist_is_fast_becoming_the_go-to_site_for_rental_property/16 [http://perma.cc/WP2H-W5HM].

36 *Id.*

37 *Airbnb in the City*, N.Y. ST. OFF. ATT'Y GEN. (Oct. 2014), http://www.ag.ny.gov/pdfs/Airbnb%20report.pdf [http://perma.cc/BZD3-7ZXY].

Presently, however, home-sharing websites like Airbnb.com have essentially eliminated these problems, thereby greatly reducing traditional barriers to entry to the hotel/home-sharing industry for individuals and commercial enterprises alike. Through user rating systems, home-sharing websites like Airbnb.com create a substitute for trust that reduces the risk of home-sharing for both hosts and guests.[38] Hosts can see which guests have the highest reputations as respectful guests, and guests can see which hosts have the best reputation for providing well-kept rooms and amenities.[39] This manufactured trust drastically reduces costs for homeowners seeking to list their property for rent, as their reputation becomes established through user reviews.

The cost of advertising is likewise eliminated, as home-sharing websites make it possible for home-sharers to be globally visible for free.[40] Through their sophisticated user interfaces, home-sharing websites allow any listed property to be viewed by any potential guest at any time when they use the website's search function. Thus, the user who seeks to rent out space in his or her home need not invest any more in advertising than the cost of a few pictures. Accordingly, home-sharing websites have substantially reduced the cost of entry into the home-sharing/hotel industry for both individuals seeking to self-employ, and commercial entities seeking to establish de facto hotels.[41]

Lower barriers to entry to the hotel industry result in conversion of residential units into rental accommodations on a much larger scale than ever before.[42] For instance, in Los Angeles (and in other cities as well) whole units, as opposed to a spare bedroom within a unit or a shared unit, dominate the listings on home-sharing websites.[43] Of all the Airbnb listings in Los Angeles, sixty-four percent are for entire units, while thirty-two percent are for private rooms, and four percent are for shared rooms.[44] Of the entire-unit listings, six percent are rented out by what can be classified as "leasing companies," which are property owners that

---

38 *See generally* Wyld, *supra* note 35.

39 Cheng, *supra* note 30, at 5.

40 *See generally How It Works*, AIRBNB, https://www.airbnb.com/help/getting-started/how-it-works [http://perma.cc/Z48L-SLJ6].

41 Cheng, *supra* note 30, at 17.

42 *Id.*; *see also* Tim Logan, Emily Alpert Reyes & Ben Poston, *Airbnb and Other Short-Term Rentals Worsen Housing Shortage, Critics Say*, L.A. TIMES (Mar. 11, 2015, 3:00 AM), http://www.latimes.com/business/realestate/la-fi-airbnb-housing-market-20150311-story.html#page=1 [http://perma.cc/HBC7-WNTQ].

43 *See* Roy Samaan, *Airbnb, Rising Rent, and the Housing Crisis in Los* Angeles, LAANE: A NEW ECONOMY FOR ALL (Mar. 2015), http://www.laane.org/wp-content/uploads/2015/03/AirBnB-Final.pdf [http://perma.cc/6C6J-E737].

44 *Id.* at 18.

list two or more whole units at a time.[45] While these leasing companies represent a minority share of the market, they actually account for thirty-five percent of all the revenue generated by Airbnb in Los Angeles.[46]

Global Homes and Condos ("Global") is one such leasing company. Global describes itself as "a full service vacation rental management company,"[47] and is known as "the most prolific host" in Los Angeles, listing at least seventy-eight whole units as short-term rentals on home-sharing websites in a cluster that spans the border between Santa Monica and Venice.[48] By using home-sharing websites, Global is able to pit "tourist dollars against rental dollars," and consistently finds that it can generate significantly more revenue by converting its long-term rental stock into short-term rental listings on home-sharing websites than if it were to lease the properties long term.[49]

Meanwhile, the city of Los Angeles suffers from a deficit of rental housing, needing an additional 5300 units of rental housing per year to meet demand.[50] The Mayor and City Council of Los Angeles are currently working to make the availability of rental housing a priority by requiring developers to set aside units for affordable housing in exchange for permitting other development. The City is also working to preserve the number of rental housing units on the market by "adopting a 'no net loss' policy that ensures subsidized units don't disappear when buildings are demolished or replaced."[51] Measures like these demonstrate that the City is spending tax dollars and other municipal resources to not only ensure that new units of rental housing will be added to the market, but current units will remain available. Entities like Global, however, which make commercial use of home-sharing websites, directly hinder the City's goal of keeping rental housing units on the market, and the City (i.e. taxpayers and renters) pays the costs in two ways.[52] First, as more long-term rental units are converted into permanently listed short-term rentals, the cost of living in the

---

45 *Id.*

46 *Id.*

47 *Id.*

48 *Id.*

49 *Id.* at 20.

50 The Times Editorial Board, *L.A. Has a Serious Housing Crisis and It's Time for City Officials to Do Something About It*, L.A. TIMES (Jan. 11, 2015, 5:00 AM), http://www.latimes.com/opinion/editorials/la-ed-affordable-housing-part-1-20150111-story.html [http://perma.cc/N2HK-XG9S]; *see also* Logan, Reyes & Poston, *supra* note 42.

51 The Times Editorial Board, *supra* note 50.

52 *See* Tim Logan & Emily Alpert Reyes, *Airbnb Cuts Ties with Vacation-Rental Firms in Los Angeles,* L.A. TIMES (Apr. 3, 2015, 5:41 PM), http://www.latimes.com/business/la-fi-airbnb-rift-20150404-story.html [http://perma.cc/EG4S-Z3MH].

area rises.[53] Second, as more of the City's tax dollars are spent on ensuring the supply of rental housing, less is available for other municipal needs.

The costs generated by home-sharing that are being borne by the City of Los Angeles are common throughout several other cities in the United States. In response, many cities have attempted to regulate home-sharing.[54] As discussed *infra,* the effectiveness of such regulation remains to be seen. However, it is readily apparent from the regulation efforts that, just like the negative externalities home-sharing imposes on single-family neighborhoods, the costs that home-sharing imposes on the city are also being borne by those who do not participate in home-sharing.

In sum, as home-sharing becomes more widely used throughout neighborhoods and cities in the United States, negative externalities result, the costs of which fall on homeowners in single-family neighborhoods where home-sharing is particularly prevalent, and cities where rental housing is in short supply. These externalities are substantial, leading homeowners to petition local government for the prohibition of home-sharing, and compelling cities to devote additional tax dollars to maintaining adequate levels of rental housing. Thus, the externalities created by home-sharing create a clear demand for regulation, and unless regulation can effectively shift the cost of those externalities back onto the home-sharing industry, those not involved in home-sharing will continue to pay.

II. INEFFECTIVE REGULATIONS

Given that home-sharing generates substantial negative externalities, there is little doubt that the industry needs to be regulated. Unsurprisingly, several municipalities have tried. However, current attempts at regulation are based on normative business-consumer ("B2C") business models, and as such, these regulations target the supplier of services. Thus, current regulatory attempts have all targeted those who supply space for rent (hosts) rather than the home-sharing websites themselves. However, the digital P2P marketplaces utilized by home-sharing websites thwart normative regulation methods that are effective on traditional commercial enterprises. Digital P2P marketplaces reduce the effectiveness of supplier-targeting regulation because such regulation is only successful if hosts police themselves, or if neighbors blow the whistle. Moreover, neither self-policing nor

53 *Id.*
54 *Id.*

whistleblowing is occurring because there is little incentive for hosts to self-police, there is little opportunity for neighbors to whistle-blow, and there are few ways to actually enforce regulations even when whistleblowing occurs. Accordingly, nearly every attempt to regulate home-sharing, from city-wide to neighborhood specific, has failed (with one exception discussed *infra*), leading to the conclusion that a different cost-shifting mechanism should be called upon to effectively mitigate the negative externalities of home-sharing.

Airbnb.com and many other home-sharing websites employ a P2P marketplace or "platform."[55] These marketplaces "act as a meeting point between providers and customers to transact over individual services,"[56] thereby enabling individuals to monetize skills and assets within their possession.[57] The concept of a P2P marketplace is not new, but thanks to ever-increasing internet access and ever-falling utilization costs, companies like Airbnb can use the internet to organize and distribute essential market information (such as where consumers are, what they will pay, whether they can be trusted, etc.) necessary to create a thriving, digital, P2P marketplace.[58] As the market thrives, the responsible website takes a commission of all transactions occurring within its digital marketplace. Thus, companies like Airbnb have turned P2P platforms into the backbones of their operations: they allow users to monetize resources (such as a spare room) at a rate they would not be able to before, and for that they take a percentage of the revenue.[59]

While the use of P2P platforms creates resource utilization, as stated before, it also creates a challenge from a regulatory perspective. Until recently, most large companies operated using a B2C platform, which is one commercial producer/provider selling goods or providing services to several consumers (like a hotel chain and its guests), or business-to-business ("B2B") platform, where companies sell goods to secondary vendors who sell the goods directly to the end consumer.[60] Such companies can be easily regulated because they are the initial and/or sole producers of the product or service. Therefore, a regulation that targets the producer/provider will be effective because the producer/provider is the company, which has complete control

---

55 Cheng, *supra* note 30, at 8.

56 *Id.* at 2.

57 *Id.*

58 *Id.*

59 James Corbett, *The Peer-to-Peer Economy—A Turning Point in Human History*, WALDEN LABS SOLUTIONS IN SELF-RELIANCE (Apr. 8, 2015), http://waldenlabs.com/peer-to-peer-economy/ [http://perma.cc/82UK-X7J4].

60 Cheng, *supra* note 30, at 9.

over the product/service. For instance, if a hotel (provider) conducts business in a way that generates a nuisance to nearby landowners or disrupts a city's rental housing market, the *hotel* will be the target of any necessary regulation. The hotel will then comply with the regulation because, as the producer *and* the commercial establishment, its infractions will be visible, reportable, and therefore punishable.

Companies that utilize P2P platforms, however, decentralize control over their goods and services, and move commercial activity into residential homes.[61] The company provides the general rules for users, but it is the *user* that provides the actual services to consumers, and does so from the privacy of the user's own dwelling.[62] In that sense, companies such as Airbnb that employ P2P platforms are not the providers of the services rendered on its website. Users are not employees or agents of the company, but rather are business partners or "micro-entrepreneurs" making independent business decisions with little influence from the company facilitating the transaction.[63] Therefore, when regulators seek to impose regulations on home-sharing using traditional methods that target the producer/provider, the regulations do not target a company like Airbnb, but rather target the *users* of the website, as they are the actual providers of the service. However, because the users are providing services from their homes, their infractions are far less visible than those of a commercial establishment, and thus, regulations that target the users of home-sharing websites are largely ineffective.

Currently, the most common forms of home-sharing regulations are zoning codes, ordinances, and Homeowner Associations' Covenants, Conditions, and Restrictions ("CC&Rs"). Regardless of whether these regulations existed before the advent of home-sharing websites or were enacted as a response, they all suffer from the same fatal flaw: they target the user of the website and not the website itself. The following hypothetical sheds light on the problem.

Assume Louis Landowner discovers that people in his city are making great money by listing their spare rooms on Airbnb.com. Landowner decides to investigate, so logs onto Airbnb.com and creates a profile. Instantly he is presented with a geographically tailored statistic of the average revenue other users in his area are generating monthly by listing their

61 *Id.* at 8.
62 *Id.* at 9.
63 *Id.*

properties on Airbnb.com. Seeing a lucrative opportunity, Landowner lists a spare bedroom in his house on Airbnb.com. He heeds the admonition on Airbnb's website to check his local laws and regulations and discovers that his city (like many) has an ordinance prohibiting rentals for less than thirty days in residential areas.

Unless Landowner is extremely scrupulous and willing to police himself, the ordinance will have no deterring effect standing alone. Moreover, even if Landowner is afraid of violating prohibitive zoning ordinances, if he types his own region and arbitrary dates into Airbnb's search engine, a map will appear, showing all the listings available in his area for those dates and their prices. Thus Landowner will see that no one is deterred by the ordinance, but rather people are generating revenue by violating an ordinance that no one is enforcing. Because Landowner is now incentivized *not* to self-police, the prohibitive regulation is ineffective to prevent Landowner from engaging in short-term renting.

Host-based regulations fail not only because there is a lack of incentive for the host to self-police, but also because home-sharing is hard to detect, making whistleblowing nearly impossible. Returning to the hypothetical, suppose Landowner has listed a spare bedroom in his home on Airbnb.com for a reasonable price. Landowner receives a "request"[64] from Gary Guest to rent his spare room. Landowner accepts the request and a pleasant rental experience follows. Of course, there is no alarm sounding informing city officials that Landowner is engaging in a prohibited land use. If no one witnesses and reports the activity to the city, there cannot even be an attempt at enforcing the ordinance. But even assuming a neighbor witnesses guests coming and going from Landowner's home, there is little likelihood that such activity would be reported. To a neighbor, the individual coming and going could just as likely be a visiting friend or family member as an Airbnb guest, so a neighbor is unlikely to report a fellow landowner unless there are other indications of home-sharing occurring.

Furthermore, the inability of city officials to investigate alleged home-sharers, even once home-sharing has been reported, further proves that whistle blowing is an ineffective means of regulating home-sharing. Continuing the hypothetical, assume

---

64 When an Airbnb guest wants to stay at a listing, they select the listing and click a box entitled "request." Airbnb's server sends a notification to the owner with the option to accept or reject the potential guest. *See generally* AIRBNB, www.airbnb.com [http://perma.cc/7SKN-YU3X].

Nathan Neighbor, who lives across the street from Landowner, somehow learns that Guest is actually a short-term renter from Airbnb.com. He calls the local officials and states that he believes Landowner is engaged in a prohibited land use—short-term renting. A city official arrives, knocks on Landowner's door, and asks Landowner if he is renting his room short-term to Guest. Landowner says "no." Absent any additional evidence that Landowner is renting out his room short-term on Airbnb.com, this is likely the end of the investigation.

For many municipalities and neighborhoods across the United States, this hypothetical is not far from what actually occurs when anti-home-sharing residents attempt to blow the whistle on their neighbors. In Los Angeles for instance, short-term rentals violate zoning ordinances and are generally subject to fines if discovered,[65] yet just as in the above-hypothetical, enforcement is scarcely called upon and largely ineffective when it is.[66] One spokesman from the Building Department of Los Angeles stated that "it is extremely difficult to prove someone is illegally renting out a home."[67] Upon being notified, a building department official could knock on the door of the alleged short-term rental location and ask if the owner is renting short-term, but if the owner denies it, that is the end of the investigation.[68] To pursue the matter further, someone from the Building Department would need to solicit a search warrant from a judge to investigate for "serious violations [of a zoning ordinance] that threaten life, limb or property."[69] The unlikelihood of seeking and obtaining such a warrant for every alleged short-term rental is obvious, and considering the fact that thousands of L.A. residents still list their units on Airbnb today, it appears home-sharers are aware of the unlikelihood that they will be discovered and fined.[70] In sum, because home-sharing is popular, profitable, and difficult to prove, zoning regulations that target users and rely on self-policing and whistleblowing are ineffective to actually regulate home-sharing.

Preexisting user-targeting regulations such as zoning codes are not the only regulations that fail to effectuate meaningful

---

65 Deputy Director of Planning Alan Bell, *Short Term Rentals*, EXECUTIVE OFFICES L.A. DEP'T CITY PLAN. (Mar. 19, 2014), http://cityplanning.lacity.org/code_studies/misc/shortterm rentals.pdf [http://perma.cc/2PNN-RLNK].

66 Emily Alpert Reyes, *Los Angeles Gives Hosts, Neighbors Mixed Signals on Short-term Rentals*, L.A. TIMES (Feb. 7, 2015, 10:00 AM), http://www.latimes.com/local/california/la-me-adv-illegal-rentals-20150208-story.html#page=1 [http://perma.cc/3BZ8-6NA5].

67 *Id.*

68 *Id.*

69 *Id.*

70 Samaan, *supra* note 43.

regulation of home-sharing. On the contrary, San Francisco has shown that even legislation specifically crafted to regulate home-sharing also fails.[71] Like Los Angeles, San Francisco has experienced a substantial shrinkage of its rental housing market as a result of home-sharing.[72] Perhaps since San Francisco is "ground-zero" for home-sharing (as it is the birthplace of Airbnb as well as the location of its headquarters),[73] it is one of the first cities to pass legislation specifically to address the effects of home-sharing on the rental housing market.

In October 2014, San Francisco's Board of Supervisors approved, and the Mayor signed into law, a bill aimed at regulating home-sharing within the city, commonly referred to as the "Airbnb Law."[74] David Chiu, President of the Board, stated that the law is an attempt at "a balanced solution that protects housing from hotel conversion while allowing some flexibility for residents to help them afford to stay in their homes."[75] In a nutshell, the Airbnb Law legalizes short-term rentals inasmuch as they were prohibited by the City's former zoning code, with some caveats:[76] only primary residential units (units occupied by the permanent resident for at least 275 days out of the year) may be listed on home-sharing platforms as short-term rentals; listing a property for rent when the host is not present is limited to ninety days out of the year; and hosts are required to register with the city planning department and obtain a permit in

---

71 *See* Jay Barmann, *Airbnb Law Impossible to Enforce, Says Agency Tasked with Enforcement*, SFIST (Mar. 23, 2015, 4:30 PM), http://sfist.com/2015/03/23/airbnb_law_impossible_to_enforce_sa.php [http://perma.cc/H82B-UF8Q]; *see also* Matier & Ross, *'No way of Enforcing' Airbnb Law, S.F. Planning Memo Says*, S.F. CHRON. (Mar. 22, 2015), http://www.sfchronicle.com/bayarea/matier-ross/article/No-way-of-enforcing-Airbnb-law-S-F-planning-6151592.php [http://perma.cc/A5VD-ZWLY].

72 *See* Rachel Swan, *Protesters Accuse Airbnb of Desecrating San Francisco's Neighborhoods*, S.F. WKLY. (Oct. 27, 2014, 11:25 AM), http://www.sfweekly.com/thesnitch/2014/10/27/protesters-accuse-airbnb-of-killing-san-franciscos-neighborhoods [http://perma.cc/7R37-NGFE]; *see also* Carolyn Said, *Window into Airbnb's Hidden Impact on S.F.*, S.F. CHRON. (June 2014), http://www.sfgate.com/business/ item/Window-into-Airbnb-s-hidden-impact-on-S-F-30110.php [http://perma.cc/PAK2-LF9C]; Dara Kerr, *Sen. Feinstein Urges San Francisco Not to Pass 'Airbnb Law'*, CNET MAG. (Oct. 20, 2014, 7:28 PM), http://www.cnet.com/news/sen-feinstein-urges-san-francisco-not-to-pass-airbnb-law/ [http://perma.cc/9V83-JE8Z].

73 Lisa Davis, *To BnB – or Not?*, CAL. LAW. (Nov. 2014), https://ww2.callawyer.com/Clstory.cfm?eid=937933&wteid=937933_To_BnB_-_or_Not? [http://perma. cc/9APZ-VHR9].

74 Dara Kerr, *Sen. Feinstein Urges San Francisco Not To Pass 'Airbnb Law'*, CNET MAG. (Oct. 20, 2014, 7:28 PM), http://www.cnet.com/news/sen-feinstein-urges-san-francisco-not-to-pass-airbnb-law/ [http://perma.cc/9V83-JE8Z].

75 Dara Kerr, *San Francisco Mayor Signs Law Making Airbnb Legal*, CNET MAG. (Oct. 28, 2014, 1:25 PM), http://www.cnet.com/news/san-francisco-mayor-makes-airbnb-law-official/ [http://perma.cc/574A-HHZU].

76 Stephen Fishman, *Overview of Airbnb Law in San Francisco*, NOLO, http://www.nolo.com/legal-encyclopedia/overview-airbnb-law-san-francisco.html [http://perma.cc/5C9U-R9SV].

exchange for a fifty-dollar fee every two years.[77] Additionally, the Airbnb Law requires that prospective hosts register their activity with the City's Planning Department.[78] While at first blush this legislation appears promising, upon closer inspection it bears the same fatal flaw as zoning ordinances that prohibit short-term rentals: it targets users and relies on self-policing and whistleblowing to be effective. Unsurprisingly then, since the Airbnb Law was enacted, San Francisco residents and city officials alike have described it as "a mess."[79]

Because the Airbnb Law relies on self-policing, it fails in the same fashion as the zoning ordinances that preceded it. For home-sharers, the registration process is so cumbersome that compliance is difficult and unappealing. The registration process mandates that every host interested in listing their property on a home-sharing website fill out an application; provide a number of documents as proof of permanent residency;[80] present a Business Registration Certificate to the planning department; present proof of liability insurance covering at least $500,000; present a signed affidavit agreeing to abide by all conditions of the short-term residential rental ordinance; and last but not least, present and a fifty-dollar check made out to the San Francisco Planning Department.[81] Due to the sheer intensity of the registration process, the incentive to participate is low, and home-sharers are unlikely to police themselves into compliance. The fact that only about two percent of home-sharers have even attempted to comply with the new regulations suggests that this is true. As of March 2015, there were at least 6000 short-term rentals operating in San Francisco listed on various home-sharing websites (5000 of which were listed on Airbnb.com), and of those hosts, only 159 have applied for the mandatory registration.[82]

The Airbnb Law is further ineffective because, just like with ordinances, the entity in charge of enforcement, the San Francisco Planning Department, lacks the ability to effectively enforce the Law.[83] In order to enforce the Airbnb Law, the Planning Department would need some way to track and locate

---

77 *Id.*

78 *See generally supra* Part I; Fishman *supra* note 76.

79 Matier & Ross, *supra* note 71.

80 Caleb Pershan, *Get Ready To Register Your Airbnb and Follow All the New Rules Starting Next Month*, SFIST (Jan. 19, 2015, 9:50 AM), http://sfist.com/2015/01/19/get_ready_to_register_your_airbnb_w.php [http://perma.cc/CX3P-Q8K6].

81 *Id.*

82 Carolyn Said, *S.F. Airbnb Law off to Slow Start; Hosts Say It's Cumbersome*, SFGATE (Mar. 3, 2015, 1:52 PM), http://www.sfgate.com/business/article/S-F-Airbnb-law-off-to-slow-start-hosts-say-6110902.php [http://perma.cc/KU38-RGCN].

83 Matier & Ross, *supra* note 71.

hosts that are noncompliant. But to do so it would need to be able to cross-reference its record of registered hosts with hosts on home-sharing websites to discover the identities and locations of non-register hosts. The only entity capable of accurately collecting and reviewing the names and locations of all hosts on its website are the home-sharing websites themselves, but for the time being, they do not cooperate with city officials.[84]

Additionally, the Planning Department claims it would need home-sharing companies to monitor their sites and actually prohibit users from accepting more than ninety days worth of guest requests for rentals in multi-dwelling buildings in San Francisco, [85] but home-sharing websites decline to do this as well. Given that the San Francisco Planning Department needs meaningful cooperation from home-sharing websites to effectively enforce the new Airbnb Law, without such cooperation, the law is just as impotent as the preexisting zoning code it was designed to replace.[86]

The problems of self-policing and whistleblowing that frustrate the effectiveness of city-enacted regulations also prevent regulation of home-sharing on a smaller scale. Homeowners Associations ("HOAs"), with few exceptions, are equally incapable of regulating home-sharing as municipalities because, just like municipalities, HOA regulations target users of home-sharing websites. As demonstrated above, when a regulation targets users, its success is tied to the users' willingness to self-police or third parties' ability to blow the whistle. While the smaller size of an HOA compared to a municipality can reduce some barriers to enforcement, for the most part, HOA regulations targeting home-sharing still fail.

When a landowner purchases property governed by an HOA, he agrees to abide by the CC&Rs. A common restriction in CC&Rs is a prohibition on short-term renting; thus most HOAs make it a finable offense for one of its members to rent space in their properties for less than thirty days. But still, the target of the regulation is the host, and just like zoning ordinances or specially crafted legislation, the regulation relies on self-policing and whistle-blowing. Accordingly, before any regulation can occur, a neighbor must report the offending property owner and an HOA official must actually investigate the claim. The size of neighborhoods compared to the size of cities gives HOAs an advantage in that the HOA has fewer properties to police than a

84 *Id.*
85 *Id.* at 2.
86 *Id.*

municipality, but generally speaking, that advantage is still insufficient to overcome inherent problems with user-based regulations. However, a minority of HOAs have demonstrated that with the right infrastructure and extreme vigilance, they can overcome the barriers to whistleblowing and enforce their prohibitions on home-sharing to some degree. Take for example, the case of The Mark Condominium Association in downtown San Diego.[87]

Thomas Stevens lived in a condo in a high-rise run by The Mark Condominium Association in downtown San Diego.[88] At the time Stevens bought his condo, he agreed to the CC&Rs (as is always a condition of purchasing a dwelling controlled by an HOA).[89] The CC&Rs of the condominium prohibited rentals of less than 90 days,[90] yet Stevens, either in ignorance or disregard of the prohibition, decided to list his condo on a home-sharing website.[91] Stevens was eventually discovered by his HOA when one of his guests revealed to a receptionist at the building that she was a short-term renter.[92] The HOA then fined Stevens $350.[93] Apparently this was but a slap on the wrist to Stevens, who reportedly pocketed $2,500 from the week-long rental which resulted in the fine.[94] Perhaps Stevens continued to somehow remain ignorant of the specifics of the CC&Rs after his fine, or perhaps simple math (Stevens' large profit margin despite the fine) is a better explanation for why Stevens continued to list his condo on home-sharing websites. However, Stevens was eventually sued by The Mark.[95] Initially, Steven tried what many home-sharers are likely to do—he claimed his guests were friends or family members, but to no avail.[96] While the frequency of Stevens' rental activities were disputed in litigation, a Superior Court Judge ultimately found for The Mark, and concluded that Stevens was in breach of his contract (the CC&Rs) with The Mark.[97] The court awarded the condominium

---

87 Jonathan Horn, *Man Who Rented out Condo Fined $106K*, U-T SAN DIEGO (Oct. 24, 2014, 4:55 PM), http://www.utsandiego.com/news/2014/oct/24/airbnb-vrbo-mark-rent-steelers-gaslamp-condos/?#article-copy [http://perma.cc/G6P7-9GGC].

88 *Id.*

89 *Id.*

90 *Id.*

91 *Id.*

92 *Id.*

93 *Id.*

94 *Id.*

95 *Id.*; *see also* Ariel Bedell, *Short-Term Vacation Rentals and Homeowners Associations (HOAs)*, LOFTIN FIRM, P.C. (Nov. 3, 2014), http://www.loftinfirm.com/blog/2014/11/short-term-vacation-rentals-and-homeowners-associations-hoas.shtml [http://perma.cc/C6BL-2Q49].

96 Horn, *supra* note 87.

97 *Id.*

roughly $16,000 in costs, and $90,000 in attorneys' fees for breach of contract.[98] If the math was not simple before, it certainly is now: Stevens' home-sharing activities earned him a few thousand dollars, but in the end it cost him over a hundred thousand, and Stevens had to sell his condo to pay for the ordeal.[99]

While Stevens' story may be a cautionary tale for some home-sharers, it is unlikely to deter the majority of homeowners from home-sharing because there are two characteristics of The Mark that are unique to high-rise style HOAs that make enforcement of anti-home-sharing regulations possible. The first characteristic is the dense, vertical layout of a condominium style HOA. As one general manager of a high-rise condominium pointed out, "you're not going to keep anything secret in a vertical village."[100] First, management is likely to be working in the lobby for several hours a day and is likely to take notice of any unusual increase in new faces or non-residents coming and going with luggage. Second, the residents all use the same parking structure, elevators, hallways, lobby, and common-areas, making it much easier for whistleblowing neighbors to be aware of short-term guests coming and going than in typical low density residential areas.

The second characteristic unique to condominium-style HOAs is the apartment-like management system. Unlike typical HOAs, which are policed by a board of elected, volunteer homeowners, high-rise condominium HOAs like The Mark are policed by paid managerial staff.[101] Since they are paid to keep the condominium functioning smoothly for all members, condominium managers have the time and motivation to vigilantly watch for activities such as home-sharing that threaten the quiet enjoyment (and thereby the value) of the condos. A general manager of one condominium complex in downtown San Diego stated he "checks sites like Airbnb every two weeks to see if people are advertising their units," and checks those websites even more frequently during times of increased tourism in the city.[102] Unlike these downtown high-rise condominiums, most neighborhood HOAs are not patrolled by paid managerial staff, and thus they are unable to go to such lengths to investigate for home-sharing.

---

98 *Id.*
99 *Id.*
100 *Id.*
101 *Id.*
102 *Id.*

While the HOA of a high-rise condominium complex may be in an advantageous position to weed out short-term rentals, they are the exception. Neither of the two characteristics that overcome enforcement difficulties are found in typical, sprawling, single-family-home style HOAs. Unlike The Mark and similarly situated HOAs, most HOAs are still barred from enforcing anti-home-sharing regulations by a lack of self-policing and whistleblowing.

Whether the regulation of home-sharing is citywide or neighborhood specific, if such a regulation targets hosts, it is unlikely to be effective. The majority of cities and HOAs do not have the resources or ability to monitor hosts regularly, and neither do neighbors. Because there is no enforcement, and the potential for revenue is great, users are not incentivized to self-police. Therefore, regulatory attempts thus far have resulted in little to no change in the home-sharing industry; the costs of the negative externalities are still fully borne by those outside of the industry. This epic failure of legislative regulation suggests that another cost-shifting tool is needed to address the negative externalities generated by the proliferation of home-sharing across the United States.

III. USING NUISANCE LAW TO TARGET WEBSITES AND EFFECTIVELY REGULATE HOME-SHARING

As discussed above, home-sharing generates substantial negative externalities, the cost of which are currently borne by individuals and entities who do not participate in home-sharing. Meanwhile, the P2P nature of the home-sharing industry frustrates traditional methods of regulatory enforcement, making regulatory attempts to mitigate the negative impacts ineffective. But where regulations fail, the common law can succeed. Recent case law regarding digital P2P platforms shows that common law rules of fault-based liability can be used to hold the creators of P2P platforms liable for the damages caused by third parties using their platforms.[103] Thus the common law acts as a cost-shifting mechanism for negative externalities: when a company generates substantial negative externalities, if the company is found liable, it must pay the damages—i.e. the cost of the negative externalities. Furthermore, once liability has been established, the company will be compelled to implement new business methods that insulate the company from liability. In other words, the company will stop producing negative

---

103 *See generally* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

externalities, or else it will pay the cost of them in court. Therefore, in the event that legislative action fails to regulate an industry, the common law can be used to shift the costs of the negative externalities caused by home-sharing away from the general public and onto the cost-generating industry.

The cases of *A&M Records, Inc. v. Napster, Inc.* and *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* provide the framework for applying rules of fault-based liability to digital P2P platforms. In 1999, Napster, Inc. created a P2P platform that allowed users to share music, and in 2001, Grokster, Ltd. created a P2P platform that allowed users to share music and movies.[104] The practices of music sharing and movie sharing caused a negative externality—wide-spread copyright infringement—and for a time the cost of the externality (lost profits) was borne by music and movie producers. However, once these companies were taken to court, the cost of copyright infringement was shifted from music and movie producers onto Napster and Grokster respectively.

In 1999, Shawn Fanning developed one of the first digital P2P platforms, Napster, Inc.—a file-sharing service that made it fast and simple for users to share music over the Internet.[105] With the help of a few programmers, Fanning launched his software and incorporated Napster, Inc.[106] Within months, user numbers skyrocketed, billions of songs were being shared, and Napster generated substantial revenue through venture capitalists' investments. Unfortunately for Napster, however, the negative externalities generated from music sharing were substantial enough to compel those affected by them to take action,[107] and less than a year after its creation Napster, Inc. was sued by the RIAA (Recording Industry Association of America) for copyright infringement.[108]

At the trial court level, Napster was enjoined from operating based on claims of copyright infringement.[109] Eventually appearing before the Ninth Circuit Court of Appeals,[110] Napster defended its liability by citing *Sony Corp. of America v. Universal City Studios, Inc.*, a case in which Sony was sued for its sale of

---

104 Richard Nieva, *Ashes to Ashes, Peer to Peer: An Oral History of Napster*, FORTUNE MAG. (Sept. 5, 2013, 9:00 AM), http://fortune.com/2013/09/05/ashes-to-ashes-peer-to-peer-an-oral-history-of-napster/ [http://perma.cc/8F5L-7L3E]; *see also Grokster, Ltd.*, 545 U.S. at 919.

105 Nieva, *supra* note 104.

106 *Id.*

107 *Id.*

108 *Id.*

109 *Id.*

110 *Id.*

Videocassette Recorders ("VCRs").[111] To give a brief history, when VCRs became available to the general public, several copyright owners of television programs sued Sony for copyright infringement, arguing that by distributing a product that allows consumers to record and re-watch television programs, Sony was contributorily infringing on their copyrights.[112] Simply put, the Supreme Court of the United States ruled that because the VCR was equally capable of being used by consumers for noninfringing purposes, sales of VCRs to the public did not constitute contributory infringement of copyrights.[113]

The Ninth Circuit distinguished Napster's software from the VCR, pointing out the VCR "did not distribute taped television broadcasts," but rather merely allowed users to watch them at a different time, whereas the technological process of Napster's software actually involved duplicating and subsequently distributing copyrighted material to the general public.[114] The Ninth Circuit ultimately upheld a modified injunctive order and mandated Napster remove all infringing material from its servers.[115] By 2002, Napster ceased doing business as a music-sharing company,[116] however, the company since has been bought and now conducts legitimate business as Rhapsody. Thus in the end, the judicial system was able to shift the cost of the negative externalities caused by file-sharing back on the company that controlled the practice, and the company then found a business practice that eliminated those externalities.

Though Napster was the first company to use digital P2P platforms with disregard for the negative impacts on third parties, they were far from the last. Grokster, Ltd., emerged on the heels of Napster in 2001, and like Napster, Grokster used a P2P platform to enable users to exchange not only music, but movie files as well.[117] Grokster was nearly identical to Napster in purpose—allowing users to freely share movies and music files over the Internet—but Grokster employed an essential "technological tweak" that distinguished itself from the music-sharing pioneer from a liability perspective.[118] Napster's

---

111 *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019 (9th Cir. 2001).

112 *See generally* Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

113 *Id.* at 455.

114 *See Napster, Inc.*, 239 F.3d at 1010.

115 *Id.*

116 *Id.*

117 David McGuire, *At a Glance:* MGM v. Grokster, WASH. POST (June 27, 2005, 12:37 PM), http://www.washingtonpost.com/wp-dyn/content/article/2005/05/03/AR2005050301028.html [http://perma.cc/AYH6-TPAN]; *see also* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 923 (2005).

118 McGuire, *supra* note 117.

software allowed users to search through each other's computers and share copyrighted music with one another, but in the process, each music file shared would pass through Napster's servers electronically. In the eyes of the Ninth Circuit, this gave Napster a degree of control over copyrighted material after it was sent from a sender and before it arrived on the receiver's computer. This control was a significant factor in finding Napster liable for contributory copyright infringement.[119] However, Grokster's software "abandoned centralized servers, allowing users to connect directly with each other."[120] So unlike Napster, Grokster maintained no control over the files being sent using its software and therefore believed it could not be viewed as the distributor of copyrighted material and would not be held liable for copyright infringement as Napster was.

This belief was in fact shared by the District Court for the Central District of California when Grokster was eventually sued by a number of copyright holders claiming that Grokster "knowingly and intentionally distributed their software to enable users to reproduce and distribute the copyrighted works."[121] The District Court held that since Grokster retained no control over the activities of its users, and because the file-sharing software could be used for noninfringing purposes, it was protected from liability based on the Supreme Court's ruling in the *Sony* case.[122]

The case was ultimately appealed to the United States Supreme Court, which granted certiorari and reversed the rulings of the District Court and Court of Appeals, finding Grokster liable for contributory copyright infringement.[123] One of the many factors that led the Court to its decision included the fact that Metro-Goldwyn-Mayer ("MGM") had "commissioned a statistician to conduct a systematic search [using Grokster's software], and his study showed that nearly 90% of the files available for download on [Grokster's network] were copyrighted works."[124] Additionally, Grokster conceded its awareness that users typically employed its software primarily to download copyrighted files, since MGM had previously notified Grokster of roughly eight million copyrighted files that could be obtained using its software.[125] Discovery also showed that Grokster adamantly promoted and marketed itself as software that

---

119 *Id.*
120 *Id.*
121 *See Metro-Goldwyn-Mayer Studios Inc.*, 545 U.S. at 921.
122 McGuire, *supra* note 117.
123 *See Metro-Goldwyn-Mayer Studios Inc.*, 545 U.S. at 919.
124 *Id.* at 922.
125 *Id.* at 923.

enables users to download copyrighted works, and Grokster made no effort to filter copyrighted material from the network or otherwise prohibit the sharing of copyrighted files.[126] The Court found that overall, the facts indicated that Grokster was not a mere passive creator of a digital P2P platform that allowed for possible infringement, but rather, it had "clearly voiced the objective that recipients use it to download copyrighted works."[127]

Despite these findings, Grokster attempted to argue that "because it was the users themselves who searched for, retrieved, and stored the infringing files," Grokster was like Sony and could not be said to have materially contributed to its user's copyright infringement.[128] The Court disagreed, stating that the lower courts misinterpreted the *Sony* rule to mean "that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties' infringing use of it."[129] Rather, the Court clarified that "nothing in *Sony* requires courts to ignore evidence of intent if there is such evidence, and the case was never meant to foreclose rules of fault-based liability derived from the common law."[130] Ultimately, because Grokster "showed itself to be aiming to satisfy a known source of demand for copyright infringement," Grokster never "attempted to develop filter tools or other mechanisms to diminish the infringing activity," and "the commercial sense" of Grokster's enterprise turned on high-volume infringing use, the Court could infer Grokster's intent to induce and encourage its user to directly infringe on the plaintiff's copyrights, and concluded by stating that Grokster's "unlawful objective [was] unmistakable."[131]

The Supreme Court's decision in *Metro-Goldwyn-Mayer* can be applied to home-sharing to the extent that it provides a frame-work for analyzing the liability of P2P platform creators. Although *Metro-Goldwyn-Mayer* revolved around a copyright dispute, the Supreme Court's decision was based on "rules of fault-based liability derived from the common law" that go beyond copyright law.[132] Thus, through *Metro-Goldwyn-Mayer*, the Supreme Court iterated a general rule ("the MGM rule") regarding P2P networks: when a cause of action can establish third-party liability, the fact that a P2P platform is capable of

126 *Id.* at 926.
127 *Id.* at 924.
128 *Id.* at 928.
129 *Id.* at 934.
130 *Id.* at 934–35.
131 *Id.* at 939–40.
132 *Id.* at 934–35.

lawful use, standing alone, will not shield the creator of the platform from liability. If the P2P platform's primary intent is to facilitate unlawful activity, the party who creates and has the power to regulate the platform can be held liable based on a common law cause of action for the damages caused by third-party use of the platform. Since home-sharing websites are similar to Grokster in that they create and have the power to regulate their P2P networks, the rule from Grokster can be applied to analyze whether home-sharing websites can be liable for the negative externalities caused by third-parties activities on their websites.

By combining the MGM rule with nuisance law, home-sharing websites can conceivably be held liable for damages caused by the unlawful activity of third parties using their platforms. Like the common law cause of action for contributory copyright infringement, the common law cause of action for private nuisance allows a plaintiff to hold a defendant liable for the unlawful acts of third parties. Before *Metro-Goldwyn-Mayer*, a home-sharing website may have been able to claim that because its P2P platform is equally capable of lawful use, it could not be liable for a claim of private nuisance. However, after *Metro-Goldwyn-Mayer*, the fact that a P2P platform is capable of lawful use is not a bar to a plaintiff's recovery from a defendant for third-party torts, when the action is based on a common law cause of action. If a plaintiff can show that the primary intent of a home-sharing P2P platform is to facilitate unlawful home-sharing, the home-sharing website itself could be held liable for the damages caused by the unlawful home-sharing of third-parties.

As stated by the Supreme Court of California, liability for private nuisance arises when a plaintiff can establish "interference with the plaintiff's use and enjoyment" of their property.[133] And while the law recognizes that "[l]ife in organized society . . . involves an unavoidable clash of individual interests," the law will also recognize "liability for damages . . . in those cases in which the harm or risk to one is greater than he ought to be required to bear under the circumstances."[134] Furthermore, the Restatement of Torts, Second, provides that "the fact that other persons contributes to the nuisance is not a bar to the defendant's liability,"[135] and "one is subject to liability for a nuisance caused by an activity, not only when he carries on the

133 San Diego Gas & Electric Co. v. Superior Court, 920 P.2d 669, 696 (Cal. 1996).
134 *Id.*
135 RESTATEMENT (SECOND) OF TORTS § 840(e) (AM. LAW INST. 2006).

activity but also when he participates to a substantial extent in carrying it on."[136]

Given that courts across the U.S. have enunciated the well-established tenet of private nuisance law, which states that a defendant can be held liable for contributing to the nuisance, assisting in the creation of nuisance,[137] controlling that which creates the nuisance,[138] participating in the nuisance,[139] and even *instructing* others to create a nuisance,[140] it cannot be gainsaid that nuisance law allows for a plaintiff to recover from a defendant for the tortious actions of third-parties—much like the laws of copyright expounded upon by the Supreme Court in *Metro-Goldwyn-Mayer*. Accordingly, if a plaintiff can establish all of the elements of private nuisance, under the MGM rule, that plaintiff may be able to not only bring a cause of action against a home-sharing company for private nuisance, but actually recover damages for the nuisances caused by third-parties—the users.

To establish a prima facie case for private nuisance, a plaintiff must establish: (1) the defendant committed an act;[141] (2) the act was a substantial invasion of the plaintiff's interest in the private use or enjoyment of his land;[142] and (3) the invasion was unreasonable under the circumstances of the particular case.[143] Analyzing each of these elements in turn reveals that if a class of landowners become so inclined—conceivably motivated by the perpetual nuisances of short-term rentals in their neighborhoods—they could establish a prima facie showing of private nuisance against a home-sharing website like Airbnb.com.

---

136 *Id.* § 834; *see also* Cty. of Santa Clara v. Atlantic Richfield Co., 40 Cal. Rptr. 3d 313, 325 (Cal. Ct. App. 2006) (stating "liability for nuisance does not hinge on whether the defendant owns, possesses or controls the property, nor on whether he is in a position to abate the nuisance; the critical question is whether the defendant *created or assisted in the creation of the nuisance*") (quoting City of Modesto Redevelopment Agency v. Superior Court, 13 Cal. Rptr. 3d 865, 872 (Cal. Ct. App. 2004), as modified on denial of reh'g (June 28, 2004)).

137 *Cty. of Santa Clara*, 40 Cal. Rptr. 3d at 325; Shurpin v. Elmhirst, 195 Cal. Rptr. 737, 740–41 (Cal. Ct. App. 1983).

138 City of Greenwood v. Martin Marietta Materials, Inc., 299 S.W.3d 606, 621 (Mo. Ct. App. 2009); Rosenfeld v. Thoele, 28 S.W.3d 446, 452 (Mo. Ct. App. 2000).

139 Abbatiello v. Monsanto Co., 522 F. Supp.2d 524, 541 (S.D.N.Y. 2007); *see also* Penn Cent. Transp. Co. v. Singer Warehouse & Trucking Corp., 447 N.Y.S.2d 265, 266 (N.Y. App. Div. 1982).

140 California Dept. of Toxic Substances Control v. Payless Cleaners, College Cleaners, 368 F.Supp 2d. 1069, 1081 (E.D. Cal. 2005) (stating "[n]uisance liability also extends to defendants who create 'a system that causes hazardous wastes to be disposed of improperly, or who instruct users' to do so") (citing Selma Pressure Treating Co. v. Osmose Wood Preserving Co., 271 Cal. Rptr. 596 (Cal. Ct. App. 1990)).

141 RESTATEMENT (SECOND) OF TORTS § 824.

142 San Diego Gas & Electric Co. v. Superior Court, 920 P.2d 669, 696 (Cal. 1996); RESTATEMENT (SECOND) OF TORTS § 822.

143 *San Diego Gas & Electric Co.*, 920 P.2d at 696; RESTATEMENT (SECOND) OF TORTS § 822 comment (c).

First, the class could assert that Airbnb participated to a substantial extent in the act of home-sharing by creating a P2P platform that instructs and allows third-parties (users) to list their properties for rent short term. While the act of unlawful home-sharing is directly done by the third-party that lists their property for rent on Airbnb.com, as stated above, the laws of private nuisance state that one who substantially contributes to an unreasonable invasion can also be held liable. Thus, the fact that Airbnb.com is not the party listing the property for rent unlawfully would not defeat the assertion that Airbnb.com has committed an act for the purposes of making a prima facie showing of private nuisance.

Second, the class could establish that Airbnb's act of instructing and allowing users to create short-term rentals was a substantial invasion of their respective interests in the private use and enjoyment of land by pointing to the negative externalities caused by home-sharing on residential neighborhoods. For instance, if the plaintiff class included residents of Silver Lake, Los Angeles, the class could point to the increased traffic, noise, transients, and subsequent effects on property values of the neighborhood, as facts sufficient to establish that, by enabling unlawful home-sharing, Airbnb has substantially invaded their interest in the private use and enjoyment of their land.

The last hurdle the plaintiff-class would have to leap over would be the establishment of Airbnb's invasion of their interests as unreasonable.[144] When determining whether an invasion of an interest is unreasonable, courts consider "whether the gravity of the harm outweighs the social utility of the defendant's conduct."[145] As is apparent from the language, this test is a fact-based inquiry, and in general, is "to be determined by the trier of fact in each case."[146] Conceivably then, a class of landowners could succeed in establishing Airbnb's invasion as unreasonable by making an offer of proof as to the aggregate monetary diminishment of properties owned by members of the class as a result of home-sharing facilitated by Airbnb, and by offering objective, fact-based reports that show the negative impact of unregulated home-sharing on the cost of living in dense areas. The diminishment of property values would speak to the gravity of harm caused by Airbnb, while the reports of Airbnb's negative impact on cost of living in dense areas would point out a lack of social utility in Airbnb's actions.

---

144 *San Diego Gas & Electric Co.*, 920 P.2d at 696.
145 *Id.* at 697.
146 *Id.*

Because the common-law tort of nuisance allows for certain contributors to the nuisance to be held liable for the unreasonable invasions of third-parties, if a plaintiff class is one day successful in pleading all the elements of private nuisance, the plaintiff class could then argue that the MGM rule should be applied, for just like Napster and Grokster, Airbnb is the creator of a P2P network that results in tortious action. Accordingly, a court will then be able to consider whether the same factors of fault-based liability that led to Grokster being held liable in *Metro-Goldwyn-Mayer* are present in home-sharing companies like Airbnb.

Under the MGM rule in *Metro-Goldwyn-Mayer*, the Court concluded that Grokster could be held liable for torts of third-parties using its platform because its primary intent was to facilitate unlawful activity. The Court reached this conclusion by finding that three factors were present: (1) Grokster was aiming to satisfy a demand for unlawful activity (copyright infringement); (2) Grokster did not attempt to reduce the amount of unlawful activity that took place in its network; and (3) the more activity that took place on Grokster's network, the more profitable the company became, and most of the activity was unlawful. Thus if the same three factors can be proven of a home-sharing website such as Airbnb, like Grokster, that home-sharing website could be held liable for the torts of third-parties using its platform.

To continue to use Airbnb as an example, a plaintiff class of landowners could make a strong argument that the second two factors that gave rise to the fault-based liability of Grokster's P2P network under the MGM rule are present in Airbnb's P2P network as well. First, Airbnb does not attempt to reduce the amount of unlawful activity taking place on its network. Airbnb knows or has reason to know that home-sharing is prohibited in several areas, but yet Airbnb makes no substantial effort to limit its potential to be used by people living in those areas. For example, if Airbnb so desired, it could prohibit users from posting a short-term rental located in places like The Mark Condominiums, or prohibit users from listing properties in violation of San Francisco's Airbnb Law, but it does not. Thus, by continuing to make its platform available to all landowners everywhere, without limitation, Airbnb is declining to reduce the amount of unlawful activity taking place on its network.

It could be argued that because Airbnb has content on its website encouraging users to consult their leases, HOAs, and local regulatory agencies, it does in fact attempt to limit the amount of unlawful activity taking place on its website. However, the content can only be found by clicking on a small link titled

"FAQs for Housing" at the very bottom of Airbnb's webpage, while the words "List Your Property" appear in large, colorful font in the center of the page.[147] Furthermore, at no point in the listing process is the user re-directed to the page with the content that encourages hosts to check with the various regulatory entities.[148] In light of these circumstances, the fact that Airbnb warns users to check with local regulations may carry little weight. Therefore, a class would most likely still be able to establish that Airbnb does not limit the amount of unlawful activity on its website, despite the fact that at some point it encourages users to check local regulations.

Second, a plaintiff class could assert that, like Grokster, the more activity that takes place on Airbnb's network, the more profitable it becomes, since Airbnb takes a commission from every transaction occurring on its website. Furthermore, after propounding extensive discovery, the class would also likely be able to assert that the majority of short-term listings on Airbnb's website are unlawful in one way or another (violative of city ordinance, HOA regulation, lease agreement, etc.), for as discussed *supra*, there were nearly 5000 unlawful units listed on Airbnb in March 2015 in San Francisco alone.[149] Indeed, the plaintiffs in *Metro-Goldwyn-Mayer*, were able to establish the majority of the activity taking place on Grokster's network was illegal by hiring a statistician to determine the percentage of file downloads on Grokster's network that were copyrighted files. Perhaps the future class could even hire the same statistician. Thus, with the help of a detailed investigation, a plaintiff asserting a claim of private nuisance could establish that, like Grokster, the more activity that occurs on Airbnb's network, the more profitable it becomes, and most of the activity is unlawful.

The biggest challenge for a class of landowners using the MGM rule to assert a claim of private nuisance against a home-sharing company like Airbnb would be to establish that, like Grokster, Airbnb is aiming to satisfy a demand for unlawful activity. Though not impossible, the success of that argument would depend on whether the class can establish that despite Airbnb's efforts to encourage users to check with local laws and regulations, Airbnb is still encouraging users in restricted areas to list their properties for rent on Airbnb.com. The class may be able to succeed if it can show that Airbnb still targets restricted home-owners through its marketing campaigns. Accordingly, if a

147 *See generally* AIRBNB, *supra* note 64.
148 *Id.*
149 Said, *supra* note 82.

plaintiff can show that Airbnb solicits and induces homeowners or lessees to violate regulations and list their properties on Airbnb.com, a plaintiff could establish that, like Grokster, Airbnb is aiming to satisfy a demand for unlawful activity.

In sum, because the common law tort of private nuisance can be used to hold a defendant liable for the torts of third-parties, using the MGM rule, a court could find Airbnb liable for private nuisance. Under the MGM rule, the mere fact that Airbnb can be used for lawful activity does not bar defendants from recovery. Airbnb created the platform, and has the power to regulate it. Thus if a court determines all the elements of private nuisance are met and the primary purpose of Airbnb's P2P network is to facilitate unlawful activity, a court could hold Airbnb liable for the damages caused by the users of its website.

CONCLUSION

Home-sharing is a rapidly growing new industry that provides for utilization of an often unused resource (space), but the negative externalities that result are numerous and substantial. In communities where home-sharing is prevalent, landowners experience invasions of their property interests typically associated with commercial activities. Meanwhile, the cost of living for the city as a whole rises, as units of rental housing are converted into permanent short-term rentals, reducing the overall supply and driving the price of those remaining units upward. Because the costs of these externalities are currently borne by those outside the home-sharing industry there is a demand for regulation, but due to challenges presented by digital P2P platforms, regulatory methods both new and old that are designed to address such externalities fail to shift the costs of the negative externalities onto the home-sharing industry. However, where legislative regulations fail, the common law can succeed. Once aggregate damages reach a tipping point, a plaintiff class of landowners may bring a lawsuit for private nuisance against home-sharing companies themselves, and using the rule of P2P platform liability stated by the U.S. Supreme Court in *Metro-Goldwyn-Mayer*, that class may just prevail. If so, the defendant home-sharing website will be forced to account for the negative externalities caused by the industry, or cease to do business in the manner in which they currently operate. As such, the common law will have provided the mechanism for shifting the costs of home-sharing back to the industry.

The Gamification of Legal Education: Why Games Transcend the Langdellian Model and How They Can Revolutionize Law School

Daniel M. Ferguson[*]

INTRODUCTION

In winter of 2009–2010, a bizarre phenomenon swept through advanced countries: more than eighty million children, teens, and adults interrupted their first-world lives to harvest crops, raise livestock, and tend to the fields.[1] Farming—once considered a tedious, mundane activity—erupted as the latest pop culture sensation in the social networking game *Farmville*.[2] During their spare time, people across the world employed themselves as virtual agriculturalists for no tangible benefit. They sowed virtual plants in virtual fields with virtual chickens for virtual pay. They did it without compensation, and some even spent real money to do it.[3]

The success of *Farmville* highlights an important phenomenon relevant to educators everywhere: an activity can be amusing even if the subject matter of the activity is not.[4] Game developers have learned to tap into this phenomenon, turning even monotonous tasks into stimulating games. They call this process gamification.[5]

---

* J.D., Chapman University Dale E. Fowler School of Law, May 2016. I wish to express my gratitude to Professors Richard Faulkner and Carolyn Larmore for their assistance and feedback, and to everyone else who supported and inspired me throughout the writing process.

1 Griffin McElroy, *FarmVille Community Surpasses 80 Million Players*, ENGADGET (Feb. 20, 2010, 5:30 PM), http://www.engadget.com/2010/02/20/farmville-community-surpasses-80-million-players [http://perma.cc/JT7V-YJGL].

2 *See generally FarmVille*, ZYNGA, https://zynga.com/games/farmville [http://perma.cc/KKJ5-WMWV].

3 *See Guide to Farm Bucks*, ZYNGA, https://support.zynga.com/article/farmville-2/Guide-to-Farm-Bucks-en_US [http://perma.cc/LV2Y-7FGX].

4 *See* GoogleTechTalks, *Fun Is the Future: Mastering Gamification*, YOUTUBE, at 5:20 (Nov. 1, 2010), https://youtu.be/6O1gNVeaE4g (noting that "fun, and the theme of the things that are fun, are actually not connected").

5 *See, e.g.*, Janna Anderson & Lee Rainie, *The Future of Gamification*, PEW RES. CTR. (May 18, 2012), http://www.pewinternet.org/2012/05/18/the-future-of-gamification/ [http://perma.cc/8DRM-H89Q]. There is considerable debate over the use of the word "gamification." *See, e.g.*, *id.* ("Gamification is a horrible made-up word. Just say games. Just say gaming interfaces. Just say game-design thinking.").

Gamification is particularly relevant to legal education today. Students, graduates, and professors alike tend to agree that law school can be profoundly unpleasant. As the old adage about law school goes: first they scare you to death, then they work you to death, then they bore you to death.[6] But surely it does not have to be this way. If the makers of *Farmville* can transform the mindless chores of virtual farming into an exciting, addictive activity, then law school professors can turn legal pedagogy into an enjoyable, captivating experience.

Since the introduction of the current legal education system by Harvard Law Professor Christopher Langdell in the 1870s,[7] commentators have flung considerable critiques at the American legal education system.[8] Some 140 years later, the critiques remain unanswered, the system has changed little, and the criticisms continue to mount.[9] And as each year passes without any significant change, it seems things have only worsened.[10]

This Article recommends the use of gamification to transform legal education. Part I of this article introduces the concept of gamification and explains the aspects of games relevant to legal educators. Part II summarizes the issues with legal education today that gamification is particularly apt to address. Part III sets forth three solutions to legal education's shortcomings inspired by gamification.

I. WHAT IS GAMIFICATION?

Gamification is the use of game thinking and game mechanics to engage audiences and solve problems.[11] "Game thinking is the idea of thinking of problem solving through the

---

6 *See, e.g.*, Marcia Gelpe, *Professional Training, Diversity in Legal Education, and Cost Control: Selection, Training and Peer Review for Adjunct Professors*, 25 WM. MITCHELL L. REV. 193, 206 n.40 (1999).

7 Thomas C. Grey, *Langdell's Orthodoxy*, 45 U. PITT. L. REV. 1 (1983).

8 *See* John O. Sonsteng et al., *A Legal Education Renaissance: A Practical Approach for the Twenty-First Century*, 34 WM. MITCHELL L. REV. 303, 319 (2007).

9 *Id.*

10 *See generally id.*; Debra S. Austin, *Killing Them Softly: Neuroscience Reveals How Brain Cells Die from Law School Stress and How Neural Self-Hacking Can Optimize Cognitive Performance*, 59 LOY. L. REV. 791, 825 (2013); Paul Campos, *The Crisis Of American Law School*, 46 U. MICH. J.L. REFORM 177, 214 (2012); William D. Henderson & Rachel M. Zahorsky, *The Law School Bubble: How Long Will It Last If Law Grads Can't Pay Bills?*, A.B.A. J. (Jan. 1 2012), http://www.abajournal.com/magazine/article/the_law_school_bubble_how_long_will_it_last_if_law_grads_cant_pay_bills [http://perma.cc/8KXD-APAK]; Lawrence S. Krieger, *Institutional Denial About the Dark Side of Law School, and Fresh Empirical Guidance for Constructively Breaking the Silence*, 52 J. LEGAL EDUC. 112 (2002); Susan Stuart & Ruth Vance, *Bringing a Knife to the Gunfight: The Academically Underprepared Law Student & Legal Education Reform*, 48 VAL. U. L. REV. 41 (2013).

11 *See* GoogleTechTalks, *supra* note 4, at 3:29.

prism of games."[12] Game mechanics are the building blocks of games, such as levels, points, and leaderboards.[13]

Gamification works by creating challenges that otherwise may not exist, focusing our efforts to achieve clear goals.[14] Gamification then acknowledges when we complete challenges, activating the reward centers in our brains[15] and "motivat[ing] us to participate more fully in whatever we're doing."[16]

A. The History and Future of Gamification

Gamification has been traced back to at least 1896 when Sperry & Hutchinson ("S&H") began offering Green Shield Stamps to retailers.[17] Retailers distributed the stamps as bonuses with purchases, and customers could redeem the stamps for merchandise from a catalogue or an S&H Green Stamps shop.[18]

Throughout the twentieth century, many organizations followed suit. Some of the most famous examples of gamification in the private sector include airline mileage programs, and the McDonald's Monopoly game, both of which use elements of games to enhance customer engagement and loyalty. But companies also use gamification in the workplace to train employees. Commercial airlines, for instance, use flight simulators to train pilots and reward them for the quality of their performance.[19] A study from the Colorado Denver Business School found that "employees trained on video games learned more factual information, attained a higher skill level and retained

---

12 Christopher Carosa, *Exclusive Interview: Gabe Zichermann on How Game-Like Techniques Can Motivate Behavior*, FIDUCIARY NEWS (March 17, 2015), http://fiduciarynews.com/2015/03/exclusive-interview-gabe-zichermann-on-how-game-like-techniques-can-motivate-behavior [http://perma.cc/7A62-R4NA]; *see also* Karl Kapp, *Playing with the Definition of "Game Thinking" for Instructional Designers*, KAPP NOTES (April 16, 2014), http://karlkapp.com/playing-with-the-definition-of-game-thinking [http://perma.cc/966Y-WJ65] ("Game thinking, from an instructional game designer's perspective, is approaching the design of a learning event from the perspective of learner actions and activities that lead to a meaningful outcome while navigating some sort of risk.").

13 Carosa, *supra* note 12.

14 *See, e.g.*, JANE MCGONIGAL, REALITY IS BROKEN: WHY GAMES MAKE US BETTER AND HOW THEY CAN CHANGE THE WORLD 22–23 (2011).

15 *Id.* at 47 ("By accomplishing something that is very hard for us, like solving a puzzle or finishing a race, our brains release a potent cocktail or norepinephrine, epinephrine, and dopamine. These three neurochemicals in combination make us feel satisfied, proud, and highly aroused."); *see also id.* at 124.

16 *Id.*

17 KEVIN ROEBUCK, CUSTOMER LOYALTY PROGRAMS: HIGH-IMPACT STRATEGIES - WHAT YOU NEED TO KNOW: DEFINITIONS, ADOPTIONS, IMPACT, BENEFITS, MATURITY, VENDORS 52 (2012).

18 *Id.*

19 *See* Lydia DePillis, *Flights of Fancy: Inside the Intense World of Virtual Pilots*, WASH. POST (Dec. 20, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/12/20/flights-of-fancy-inside-the-intense-world-of-virtual-pilots [http://perma.cc/3TE6-GG84].

information longer than workers who learned in less interactive environments."[20] Gamification is also used to make better products. In Windows' "Language Quality Game," Microsoft employees earn points and compete for high scores for assessing localized versions of the Windows operating systems in their free time.[21] Analysts estimate that in 2015, more than 70% of Global 2000 organizations "will have at least one gamified application,"[22] and by 2018, the gamification market is expected to be worth $5.5 billion, with an annual compound growth of around 67% per year.[23]

Scientific researchers use gamification to aid in scientific discovery. On Planethunters.org, hundreds of thousands of players aided in the discovery of extrasolar planets by classifying light curves from stars monitored by the Kepler space telescope.[24] Additionally, researchers at the University of Washington created a game, *Fold.it*, to grapple with the mysteries of protein folding.[25] Forty-six thousand gamers logged on to *Fold.it*, and solved a fifteen-year-old AIDS problem in ten days.[26] Scientists hope to use the model of the protein generated by *Fold.it* to develop drugs that could hinder the reproduction process of HIV in humans.[27]

In Sweden, government authorities turned speeding tickets into a game. Each person who passes a speeding camera while going under the speed limit is automatically entered into a lottery to win the proceeds of the tickets given by the camera to those driving over the speed limit.[28] The game produced a 22%

---

20 Rachel Emma Silverman, *Latest Game Theory: Mixing Work and Play*, WALL ST. J. (Oct. 10, 2011), http://www.wsj.com/articles/SB10001424052970204294504576615371783795248.

21 Oliver Chiang, *When Playing Videogames at Work Makes Dollars and Sense*, FORBES (Aug. 9, 2010), http://www.forbes.com/2010/08/09/microsoft-workplace-training-technology-videogames.html [http://perma.cc/7K23-8CMS].

22 Press Release, Gartner, Gartner Says by 2015, More than 50 Percent of Organizations That Manage Innovation Processes Will Gamify Those Processes, (Apr. 12, 2011), http://www.gartner.com/newsroom/id/1629214 [http://perma.cc/V4VH-DZPT].

23 Press Release, MarketsandMarkets, Gamification Market Worth $5.5 Billion by 2018, PR NEWSWIRE (June 4, 2013), http://www.prnewswire.com/news-releases/gamification-market-worth-55-billion-by-2018-210042381.html [http://perma.cc/P2DB-C57A].

24 Chris J. Lintott et al., *Planet Hunters: New Kepler Planet Candidates from Analysis of Quarter 2*, 145 ASTRONOMICAL J. 1 (2013), http://iopscience.iop.org/1538-3881/145/6/151/pdf/1538-3881_145_6_151.pdf [http://perma.cc/9ZM4-MFUU].

25 Dean Praetorius, *Gamers Decode AIDS Protein that Stumped Researchers for 15 Years in Just 3 Weeks*, HUFFINGTON POST (Sept. 19, 2011, 3:37 PM), http://www.huffingtonpost.com/2011/09/19/aids-protein-decoded-gamers_n_970113.html [http://perma.cc/JEZ4-U32M].

26 Anderson & Rainie, *supra* note 5.

27 Praetorius, *supra* note 25.

28 *'Gamifying' the System to Create Better Behavior*, NAT'L PUB. RADIO (Mar. 27, 2011, 4:34 PM), http://www.npr.org/2011/03/27/134866003/gamifying-the-system-to-create-better-behavior [http://perma.cc/R4NV-AHJJ].

decrease in the average speed among drivers, enhancing driver and pedestrian safety.[29]

In the education sector, gamification is making a roaring entrance. Educators everywhere are utilizing the power of games to engage students and inspire learning. In Minnesota, for example, third grade teacher Ananth Pai transformed his classroom into a gamer's paradise: "he collected the best games for math, reading, vocabulary, geography and other subjects available online and from game creators and created a digital profile for every kid in his class. Suddenly, kids were engaged—absorbed, actually, in getting to the games' next levels."[30] In four and a half months, his students moved from a mid-third grade level to a mid-fourth grade level.[31] Elsewhere in the education sector, higher education projects have sprung up around gamification, including Penn State's Educational Gaming Commons.[32] But perhaps, the most well-known example of gamification in education is Salman Khan's "Khan Academy", which seeks "to provide a free world-class education for anyone, anywhere."[33]

B. What Makes a Game?

At the core of gamification are, of course, games. Although gamification often turns processes into complete games—such as military war games—gamification can simply use elements of games without the entire game structure. Regardless, an analysis of games provides a useful lens through which to view the benefits of gamification.

There are many competing definitions for what constitutes a game,[34] but one accepted definition of a game is "a system in which players engage in an artificial conflict, defined by rules,

---

29 *See* Charlie Sorrel, *Swedish Speed-Camera Pays Drivers to Slow Down*, WIRED (Dec. 6, 2010, 7:17 AM), http://www.wired.com/2010/12/swedish-speed-camera-pays-drivers-to-slow-down/ [http://perma.cc/V5CG-QBD8].

30 Beth Hawkins, *Teacher Ananth Pai's Do-It-Yourself Tech Effort Pays Big Dividends for Students*, MINNPOST (Nov. 13, 2012), http://www.minnpost.com/learning-curve/2012/11/teacher-ananth-pais-do-it-yourself-tech-effort-pays-big-dividends-students [http://perma.cc/X7L6-XH9K].

31 *Ananth Pai: Engaging Students Through Scalable Game Based Curriculum*, INSPIRED TO EDUCATE (Aug. 27, 2012), http://inspiredtoeducate.net/inspiredtoeducate/ananth-pai-engaging-students-through-scalable-game-based-curriculum/ [http:// perma.cc/W9RM-XXWG].

32 *See, e.g.*, *Educational Gaming Commons*, PA. ST. U., 2012, http://gaming.psu.edu [http://perma.cc/5C9B-C2B4].

33 *About Khan Academy*, KHAN ACADEMY, https://www.khanacademy.org/about [http:// perma.cc/M6WH-MDSY]. For background on the Khan Academy, see Khan Academy, *Salman Khan Talk at TED 2011 (from ted.com)*, YOUTUBE (Mar. 9, 2011), https://www.youtube.com/watch?v=gM95HHI4gLk [hereinafter *Salman Khan TED Talk*].

34 KARL M. KAPP, THE GAMIFICATION OF LEARNING AND INSTRUCTION: GAME-BASED METHODS AND STRATEGIES FOR TRAINING AND EDUCATION 6–7 (2012).

that results in a quantifiable outcome."[35] Using this definition, this section analyzes games through their component parts.

C. Artificial Conflict

Games use artificial conflicts to challenge players to overcome unnecessary obstacles. Artificial conflict enables the use of abstraction and gives players permission to fail.

Reality poses serious difficulties in the context of learning, namely the distraction of extraneous variables, and the difficulty of creating specific situations. Through the use of abstraction, "[g]ames remove elements of reality to keep the player focused on the essence of the game. Removing extraneous factors keeps the game moving and the player involved."[36] For instance, in the game *Microsoft Flight Simulator*, players can focus on the goal of the game—i.e., piloting the aircraft—without having to worry about other variables involved in real life flying—e.g., maintenance of the plane, turbulence, and the risk of serious bodily injury or death. Abstraction makes it easier to grasp concepts found in the real world. Further, "[reality] presents the ultimate possible specificity—each situation it poses is unique. Consequently, each single experience in reality can only be used to derive conclusions about that one unique situation."[37] Game creators have control of the game and use abstraction to determine the elements that players encounter, rather than leaving the elements to the whims of reality.

Moreover, players in a game know that the obstacles faced are artificial, thus, evoking a different reaction in the player than if the obstacles were real. "When we're afraid of failure or danger, or when the pressure is coming from an external source, extreme neurochemical activation doesn't make us happy. It makes us angry and combative, or it makes us want to escape and shut down emotionally."[38] Games are, by design, solvable, and provide players with a safe environment to operate in which failure is an option. Failure is a crucial part of learning that no learning environment should do without.[39]

---

35 KATIE SALEN & ERIC ZIMMERMAN, RULES OF PLAY: GAME DESIGN FUNDAMENTALS 80 (MIT Press, 2004).

36 KAPP, *supra* note 34, at 27.

37 Jonathan H. Klein, *The Abstraction of Reality for Games and Simulations*, 36 J. OPERATIONAL RES. SOC. 671, 675 (1985), http://www.jstor.org/stable/pdf/2582262.pdf?acceptTC=true [http://perma.cc/TSD2-U3DF].

38 MCGONIGAL, *supra* note 14, at 32.

39 *See* Benedict Carey, *Why Flunking Exams Is Actually a Good Thing*, N.Y. TIMES MAG. (Sept. 4, 2014), http://www.nytimes.com/2014/09/07/magazine/why-flunking-exams-is-actually-a-good-thing.html?_r=2 [http://perma.cc/T544-Z4WN]; Anne Sobel, *How Failure in the Classroom Is More Instructive than Success*, CHRON. HIGHER EDUC. (May 5,

Failure in a game entails minimal consequences. This encourages players to explore different options for success. In many games, players are permitted to fail multiple times until they succeed. If a player fails too much, some games have built in mechanisms to provide hints or decrease difficulty so that success always seems achievable with sufficient time and effort.

1. Rules

The rules of a game define the boundaries of the environment in which the player is engaged. The rules of a game include the goals, and limits to how the game may be played. Often, rules in a game are altered within the context of two different types of levels: game levels and playing levels.

Game levels are segmented pieces of a larger game, allowing players to progress from one level to the next as they move toward the end goal of the game. Each game level contains its own manageable set of goals which the player seeks to accomplish. Goals give games a focus and a purpose, and generate a method for measuring the success of a player. "But goals have to be well structured and sequenced to have sustained meaning and to motivate players to achieve those goals."[40] Game levels provide a useful framework in which to create reasonable goals.

A playing level is "the degree of difficulty the player chooses when he or she first enters the game."[41] With different playing levels, games challenge players with various levels of experience at appropriate difficulties. At their best, games are neither too easy nor too hard. They place players at the edge of their skill level. And when gamers are engaged at the limits of their abilities, they attain a state of mind which psychologists refer to as the "flow" state.[42] Flow is "the satisfying, exhilarating feeling of creative accomplishment and heightened functioning."[43] Flow promotes effective learning, but it is also psychologically fulfilling. "When you are in a state of flow, you want to stay there: both quitting *and* winning are equally unsatisfying outcomes."[44] The experience of flow is part of what makes games so addicting.[45]

2014), http://chronicle.com/article/How-Failure-in-the-Classroom/146377/ [http://perma.cc/DB9M-TFR6]; *see also* Warren Binford, *How to Be the World's Best Law Professor*, 64 J. LEGAL EDUC. 542, 543 (2015).

40 KAPP, *supra* note 34, at 29.

41 *Id.* at 37.

42 *See generally* MIHALY CSIKSZENTMIHALYI, BEYOND BOREDOM AND ANXIETY: THE EXPERIENCE OF PLAY IN WORK AND GAMES (1975).

43 MCGONIGAL, *supra* note 14, at 35 (quoting CSIKSZENTMIHALYI, *supra* note 42, at xiii).

44 MCGONIGAL, *supra* note 14, at 24 (emphasis in original).

45 *Id.* at 42–43.

2. Quantifiable Outcome

Another critical aspect of games is the quantifiable outcome. A quantifiable outcome allows the player to adjust his or her behavior based on previous outcomes, to make success more likely in the future. Games always generate quantifiable outcomes as end-of-game feedback by designating winners and losers, but many games provide feedback through the duration of the game as well.

In game design circles, feedback that is continuous, engaging, and effective is described as "juicy feedback."[46] Juicy feedback can drastically improve a player's performance.

> Real-time data and quantitative benchmarks are the reason why gamers get consistently better at virtually any game they play: their performance is consistently measured and reflected back to them, with advancing progress bars, points, levels, and achievements. It's easy for players to see exactly how and when they're making progress.[47]

Juicy feedback informs players on the success of their performance and induces them to try harder.

When quantifiable outcomes are positive, they are often accompanied with a reward. Rewards—e.g., medals, experience points, and badges—reinforce successful behaviors and promote positive emotions by acknowledging a player's hard work.[48]

II. LEGAL EDUCATION TODAY

A. Limited Engagement and Applied Learning

The primary pedagogical tool in legal education is the case method, whereby students extract legal principals through analysis of court decisions.[49] The case method is generally accompanied by Socratic dialogue in which professors induce students to learn the legal principles involved on their own. The case method is important because it teaches students how to think like a lawyer.[50] The Socratic method is important because it "motivate[s] students to reason rather than recite."[51] In combination, these methods prepare students for the analysis of court decisions in legal practice. But they teach only a fraction of the skills required for successful legal practice, and their use as

---

46 KAPP, *supra* note 34, at 36.

47 MCGONIGAL, *supra* note 14, at 157.

48 *See* KAPP, *supra* note 34, at 51–74; MCGONIGAL, *supra* note 14, at 28.

49 Sonsteng et al., *supra* note 8, at 325.

50 *See generally* WILLIAM M. SULLIVAN, ET AL., EDUCATING LAWYERS: PREPARATION FOR THE PROFESSION OF LAW (2007).

51 Sonsteng et al., *supra* note 8, at 325.

the primary pedagogical tool for legal education is hardly defensible.[52]

Professors may stick with these methods because they provide a simple way to engage students—to involve them in the learning process and to motivate them to improve. The case method and Socratic dialogue force students to apply knowledge learned in the course, and applied learning is well-known to be an effective way of understanding and retaining information.[53] But these methods are inefficient because only one or two students can engage with the professor at a time. All of the other students experience passive learning. Even worse, time constraints force many professors to limit engagements to a few minutes per student, once or twice per semester. At this rate, an average student engages with a professor for maybe ten to twenty minutes across the entire semester. This illustrates a serious deficiency with student engagement.

Further, the case method is often used ineffectively. Professors sometimes engage students "through the arbitrary and ruthless questioning about cases and legal principles that are often subtle, minor, and obscure."[54] Some professors rely on classroom discussion as a check that students are completing the assigned reading, rather than using discussion to advance learning objectives—clearly an inefficient use of resources. And when professors are harsh on their end of the dialogue, "the fear of being publicly criticized and humiliated for an incorrect answer can be incapacitating, rendering some students mute or unwilling to take risks in their discourse."[55] The negative impact of such unnecessary stress on the learning environment is well documented.[56]

Legal textbooks and casebooks mimic this engagement deficiency. They contain the raw material from which students

---

52 *See, e.g.*, Stephen M. Feldman, *The Transformation of an Academic Discipline: Law Professors in the Past and Future (or Toy Story Too)*, 54 J. LEGAL EDUC. 471, 482 (2004) (reviewing critiques of the ineffectiveness of the case method); David D. Garner, *Socratic Misogyny?—Analyzing Feminist Criticisms of Socratic Teaching in Legal Education*, 2000 BYU L. REV. 1597, 1610–11 (2000) (criticizing the Socratic method as an inefficient way to convey large amounts of information).

53 *See* Gerald F. Hess, *Heads and Hearts: The Teaching and Learning Environment in Law School*, 52 J. LEGAL EDUC. 75, 102 (2002) ("Students learn better when they are actively engaged in the learning process."); Binford, *supra* note 39, at 11–12.

54 Sonsteng et al., *supra* note 8, at 337.

55 Robin S. Wellford-Slocum, *The Law School Student-Faculty Conference: Towards a Transformative Learning Experience*, 45 S. TEX. L. REV. 255, 271 (2004).

56 *See* Austin, *supra* note 10, at 825 ("The impact of stress on law student cognition includes deterioration in memory, concentration, problem-solving, math performance, and language processing. Curiosity is dampened, and creativity is diminished. A paralysis sets in, limiting motivation and the ability to break out of repetitive behavior patterns. Research has shown that hippocampi shrink in size in people with major depression.").

attempt to passively understand legal reasoning, but without many opportunities for applied learning. This is unlike most, if not all, other academic areas. A standard math textbook, for instance, contains dozens of practice problems in a variety of formats that accompany each and every lesson.[57] Legal textbooks often provide a few questions after each lesson or case, but these questions are insufficient in quantity and quality, leading most students to purchase supplemental texts to overcome this deficiency. At the very least, this creates an inconvenience. And at its worst, this creates barriers to learning through confusion, stress, and misdirection. Further, legal textbooks bind themselves to a single medium—i.e., text—neglecting the benefits of a multimedia approach—e.g., increased understanding, retention, and recall.[58] In short, legal education provides little opportunity for engagement and applied learning.

B. Minimal Feedback

Because engagement and applied learning are so sparse in legal education, students suffer from a lack of feedback. Generally, students receive feedback only through minimal classroom engagement and a single grade on a single final examination. Students, therefore, have little opportunity to improve.

For students participating in a dialogue with the professor, only some feedback directly relates to course objectives—many engagements focus on the facts of a particular case rather than the law or legal reasoning. But even when feedback is effective and relevant, it is infrequent. Feedback gained through the classroom experience amounts to little more than a few brief interactions with a professor per semester.

All of the students not currently participating in the dialogue "are expected to listen, silently answer the questions being asked of their peers, and determine whether their potential response was appropriate based on the professor's response to the student . . . ."[59] In this way, students receive no direct feedback. If observing students incorrectly understand the material, they have little opportunity to understand why.

---

57 For example, see generally RICHARD G. BROWN ET AL., ALGEBRA: STRUCTURE AND METHOD, BOOK 1 (2000).

58 *See, e.g.*, Fred Galves, *Will Video Kill the Radio Star? Visual Learning and the Use of Display Technology in the Law School Classroom*, 2004 U. ILL. J.L. TECH. & POL'Y 195, 203 n.26 (2004).

59 Linda S. Anderson, *Incorporating Adult Learning Theory into Law School Classrooms: Small Steps Leading to Large Results*, 5 APPALACHIAN J.L. 127, 135 (2006).

Some professors attempt to engage the whole class with "clicker questions," where each student answers multiple-choice questions with a wireless remote.[60] Answers are individually anonymous, but the aggregate results of student responses are revealed. Generally, a short discussion on the results follows. Unfortunately, only a few classrooms utilize multiple choice clicker questions. But even in these classrooms, only a few questions are asked and often not until the end of the class. In this way, feedback is sparse and delayed.

Students also receive feedback via examination scores. But law school examinations are an inaccurate measure of student understanding:

> timed essay exams are almost exclusively the only method of testing. A single method of testing does not utilize a variety of learning and problem-solving methods and ignores underlying character attributes that are important predictors of a student's success as a lawyer. The system of timed essay exams unfairly benefits students who write well, while not rewarding those who may have an advantage in an oral examination setting.[61]

Moreover, because examination scores are an inaccurate measure of skills and knowledge, students shift their focus "from the objectives of the course to being prepared for the final test."[62]

Further, examination scores consist of a single grade. This one grade provides little information for students to use to adjust their future performance. Additional feedback specifying what the student did right and wrong is hard to come by, if available at all. But even if examination feedback is detailed and accurate, it is too infrequent to be effective. When students receive scores from a final examination, they have already completed the course. Students have no immediate incentives to make adjustments to their understanding. Even in courses with a midterm examination, students receive, at best, feedback on some small subset of material from the first half of the course before they take their final examination.

---

60 *See, e.g.*, Martha Neil, *Move Over Socratic Method, 'Clicker' Offers Law Profs New Option to Monitor Student Progress*, A.B.A. J. (Nov. 17, 2010, 3:00 PM), http://www.abajournal.com/news/article/move_over_socratic_method_clicker_offers_law_profs_new_option_to_monitor_st [http://perma.cc/4XZW-R8HZ]; Winnie Hu, *Students Click, and a Quiz Becomes a Game*, N.Y. TIMES (Jan. 28, 2008), http://www.nytimes.com/2008/01/28/education/28neck.html?_r=0 [http://perma.cc/HR6X-V92D].

61 Sonsteng et al., *supra* note 8, at 346.

62 Anderson, *supra* note 59, at 136.

C. Nominal Personalization

Another issue facing students in law school classrooms is one-size-fits-all teaching. Professors cannot teach to each and every student. They can teach to the top of the class, to the bottom of the class, or, more likely, to somewhere in the middle. At any given time, therefore, the class is either too fast or too slow for most students.

Compounding the issue of classroom pace is "the failure to recognize students' pre-existing knowledge."[63] Students today come from vastly different backgrounds with different sets of knowledge about the world. The failure to take this into account means that professors never teach to the level of any one student. This is important because an individual's pre-existing knowledge "can significantly affect how a student remembers, organizes, and interprets the curriculum."[64]

Further, students learn in different ways. Some prefer visual over auditory learning; some prefer active over passive learning; others prefer intuitive reasoning over logical reasoning.[65] These factors, too, are not taken into account. Students are subject to the teaching style of their professors, like it or not.

While attending a live class enables a professor to partially "customize" or "personalize" the instruction for the students present, any "personalized" instruction that can be said to come from attending a live class concludes at the end of class. Personalized learning does not follow a student home; it is not available when a student attempts practice problems on her own, or when reviewing material for study. Moreover, personalized instruction from class is rarely catalogued for reference. If a student misses a piece of information because of absence, misunderstanding, or simply zoning out, she has limited ability to retrieve the information later.

The worst consequence of the lack of personalization is what Salman Khan, founder of the Khan Academy, calls "Swiss cheese learning."[66] Swiss cheese learning is the idea that students almost always pass courses with holes in their knowledge, and yet they are forced to move on.[67] Even if a student scores a 95% on an examination, the score indicates that he or she does not understand 5% of the material. For instance, a law school

---

63 Sonsteng et al., *supra* note 8, at 395.

64 *Id.*

65 *See generally* Richard M. Felder & Linda K. Silverman, *Learning and Teaching Styles in Engineering Education*, 78(7) ENG'G EDUC. 674, 674 (1988).

66 SALMAN KHAN, THE ONE WORLD SCHOOLHOUSE: EDUCATION REIMAGINED 85 (2013).

67 *Id.*

student might be able to pass a Civil Procedure course, even if she has little understanding of the discovery process, so long as she has a decent understanding of other aspects of Civil Procedure. This is a horrifying fact for institutions that purport to transform students into professionals. No student should be able to pass a course without 100% comprehension of the relevant material.

The problem of Swiss cheese learning is further compounded because concepts in law school build on one another. If a student does not understand the foundational material, he or she stands no chance of mastering the secondary or tertiary material that flows from it.[68]

D. Limited Options

Another issue with the current legal education system is limited options for students. Students must choose from select courses that happen to be offered at their school, taught by professors that students do not choose.

Law schools only offer courses taught by professors employed at each school. This happens because law schools use live courses, and professors can only be in one physical place at a time. Professors must compete with other professors at that school to teach any given course. But statistically speaking, no matter which law school a student attends, the best professor(s) for any given course can most likely be found at some other school. Therefore, students rarely learn from the best professors; this creates significant opportunity costs.

Apart from choosing from a limited number of professors, students also must choose from a limited number of courses. Students rarely take courses outside of their particular law school. This means that students miss out on the opportunity to take specialized courses that might advance their careers. But they also tend to miss out on courses that could provide the basic foundation for entering the legal profession. Many commentators agree that law school does not provide individuals with enough skills or experience to be successful lawyers.[69] A 2009 report

---

68 *See id.* at 83.

69 *See, e.g.*, Erwin Chemerinsky, *Rethinking Legal Education*, 43 HARV. CIV. RTS.-CIV. LIBERTIES. L. REV. 595, 595 (2008) ("[T]he reality is that few law students graduate from law school ready to practice law."); *see also* John M. Burman, *Oral Examinations as a Method of Evaluating Law Students*, 51 J. LEGAL EDUC. 130, 132 (2001) ("[T]he required curriculum at many, if not most, American law schools virtually ignores at least half of the fundamental skills every lawyer should have."); William P. Quigley, *Introduction to Clinical Teaching for the New Clinical Law Professor: A View from the First Floor*, 28 AKRON L. REV. 463, 469 (1995) (quoting Chief Justice Warren E. Burger: "The law schools

compiled a list of twenty-six skills that are important to effective lawyering,[70] and an analysis of the list reveals that traditional law school does not teach nineteen of these skills.[71] "Live client clinics may or may not afford some opportunities to develop [some of these missing skills]," but the remaining skills "may be absent from law school entirely."[72] Further, enrollment in clinical courses is extremely limited.[73] This highlights a shocking truth about the effectiveness of law school.

E. Soaring Expense

One of the most pervasive problems facing law students today is the rising cost of attending law school. The cost of tuition in higher education has increased about 8% per year since at least the 1950s.[74] In 2013, the average tuition at a private law school was $41,985.[75] This figure does not include room and board. The average cost of borrowing money for law school was estimated at $216,406 for 2013 graduates.[76]

These costs are significant enough alone, but a weak job market compounds the issue for law school graduates. Data from the ABA on the class of 2013 reveals that nine months after graduation, only 57% of graduates whose employment status was known were employed in full-time, long-term positions requiring bar admission.[77] Projections for the next decade suggest that less than 48% of graduates of ABA-accredited law schools will get

---

of this country on their part have superbly trained students in legal principles and analysis but the question is whether that is enough. In my view that is not enough.").

70 Marjorie M. Shultz & Sheldon Zedeck, *Final Report: Identification, Development and Validation of Predictors for Successful Lawyering* 25 (Sept. 2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1353554.

71 *See* Susan Swaim Daicoff, *Expanding the Lawyer's Toolkit of Skills and Competencies: Synthesizing Leadership, Professionalism, Emotional Intelligence, Conflict Resolution, and Comprehensive Law*, 52 SANTA CLARA L. REV. 795, 823–24 (2012). Some of the skills not explicitly covered by most legal educators include: organizing and managing one's own work, organizing and managing others (staff/colleagues), stress management, creativity/innovation, strategic planning, building relationships with clients, and community involvement and service. *See id.* at 822–24.

72 *Id.* at 824 n.127.

73 *Id.* at 824 n.126.

74 *See Tuition Inflation*, FINAID, http://www.finaid.org/savings/tuition-inflation.phtml [http://perma.cc/AY7A-89F5].

75 *Tuition Tracker*, LAW SCHOOL TRANSPARENCY, http://www.lawschooltransparency.com/reform/projects/Tuition-Tracker [http://perma.cc/3J5F-NZP2].

76 Debra Cassens Weiss, *Legal Education Cost Is Even Higher than First Estimated, Transparency Group Says*, A.B.A. J. (May 7, 2012, 2:37 PM), http://www.abajournal.com/news/article/legal_education_cost_is_even_higher_than_first_estimated_transparency_group [http://perma.cc/4P8U-RXQK].

77 *American Bar Association Releases Class of 2013 Law Graduate Employment Data*, A.B.A. (Apr. 9, 2014), http://www.americanbar.org/news/abanews/aba-news-archives/2014/04/american_bar_associa4.html [hereinafter *ABA 2013 Employment Data*] [http://perma.cc/M98Z-3KZ3].

legal jobs.[78] In short, a law degree is expected to be a significant negative investment for most students.[79]

F. Nebulous Credentials

Even if a student manages the debt load that comes with three years of full-time professional education, he or she enters the job market with inaccurate and incomplete measures of skill and knowledge. Grades say little about the skills required for any given job. Grades merely identify who performed better or worse on assessments that generally amount to a single exam or paper. Students' grades are often distilled down to a single GPA or class rank that omits indicators on the strengths and weaknesses of an individual on particular legal topics. Further, a variety of factors are not taken into account when computing GPA because students are not directly graded on such factors, including communication skills, leadership skills, and work ethic.

Finally, the Juris Doctor degree makes no differentiation between individuals in a highly segmented profession. Employers must attempt to assess for themselves the abilities of a candidate employee in any given field; employers cannot rely solely on the degree. This creates significant transaction costs for employers, and makes it difficult for legal professionals to offer proof of their skills.

III. SOLUTIONS

Law schools already utilize games to motivate, engage, and assess students. CALI awards[80] and class rank engender competition between students. "Cold-calling" maintains engaged discussions and promotes preparedness for class. Examinations, whether multiple choice questions or essays based on fact patterns, act as games. In fact, nearly all applied learning methods can be classified as a game. But these games tend to be basic and poorly designed. To gamify legal education is simply to acknowledge these facts, and then to draw upon the massive body of knowledge from the game development community to enhance legal education.

The following solutions are intended to inspire the use of well-designed games to invigorate the law school experience. The first solution tackles the lack of engagement and feedback in law

---

78 Campos, *supra* note 10, at 214.

79 *Id.* at 207.

80 The Center for Computer-Assisted Legal Instruction Excellence for the Future Award (CALI Award) "is given to the highest scoring student in each law school class at many law schools." *CALI Excellence for the Future Awards*, CENTER FOR COMPUTER-ASSISTED LEGAL INSTRUCTION EXCELLENCE, http://www.cali.org/content/cali-excellence-future-awards [http://perma.cc/YPT5-LDYK].

school, and offers simple ways to incorporate games into existing classrooms. The second solution goes a step further by also addressing limited personalization and course offerings, and suggests a more radical change using games in and out of the classroom. The third solution takes a carte blanche approach to reform, in an attempt to also solve the cost and credential issues, by gamifying law school from the ground up.

A. Solution #1: More, Better Games Inside and Outside the Classroom

In most law school classrooms today, professors teach through some variation of the case method with Socratic dialogue. With this system, each student rarely engages with the professor, and students receive minimal feedback. By supplementing the traditional classroom experience with game thinking and game mechanics, professors could immediately increase student involvement and motivation, provide more opportunities for applied learning, and give students an accurate portrait of their understanding.

The Proposal:	**Gaming Elements:**
- Audience response systems - Engagement with each student - Applied learning - Low-risk testing - Public or anonymous scoring - Games in the classroom - Applied learning - Contextual learning	- Leaderboards - Competition - Collaboration - Progress tracking - Feedback - Replay
	Benefits: - Engagement - Motivation - Performance indicators

A simple way to implement gamification in the classroom is with the use of audience response systems ("ARS"). ARS enables professors to pose ungraded questions to each student in the classroom, an instant advancement over the traditional classroom dialogue. And, research shows that low-risk testing is one of the most effective learning methods.[81] The "clicker questions" many professors now use are a type of ARS.[82] But ARS should be used in greater frequency and with more game elements. ARS questions could be interspersed throughout lectures to maintain continuous engagement, or clumped into

81 *See* Binford, *supra* note 39, at 545–46.

82 *See, e.g.*, LegalEDweb, *"Using Technology for Engagement and Assessment" Sydney Beckman, Duncan School of Law*, YOUTUBE (Oct. 9, 2014), https://youtu.be/5GqthSPjG0M?list=PLLxxzZq76ixxbd_KFvJYVxyezP8rxvQpY.

groups of questions for more comprehensive examinations. Instead of specialized "clickers" that offer limited functionality, ARS can operate through a web-based application that students can access on their laptops or smartphones.[83]

Every multiple-choice question asked of a student is, in effect, a rudimentary game. But, more gaming elements can be added to ARS to enhance student engagement and motivation. If web-based ARS tracked students' answers throughout a class, the application could chart each student's level of comprehension in real time. ARS could award "points" to generate positive emotional feedback. Points could be awarded on a simple basis, such as "+1" for correct answers and "–1" for incorrect answers, or on a more complex basis accounting for the difficulty of each question and the novelty of the material being tested.

Further, each time a student answers incorrectly, ARS could generate a detailed analysis of the question and answer for each student to review on her own screen. At the end of each class, or throughout the semester, the application could generate progress reports with "juicy feedback," identifying areas of difficulty for each student and suggesting relevant resources for review.

Public scoreboards could enhance the ARS experience. "Clicker questions" are usually answered anonymously, but a twist on this format could create friendly competition in the classroom. For instance, the application might publicly broadcast the top ten players on a leaderboard. Or, a random group of students might be selected to have their scores publicly revealed—similar to the "on call" method of class participation. Or, teams of students could compete with aggregate point totals. If a professor chooses to keep scoring anonymous, the application could still display to each student how his or her score compares to the average classroom score.

Further, these questions should be available to students for replay after class. This would be particularly useful for students when reviewing for graded examinations. During replay, students could review all of the ARS questions, or some subset of the questions, such as those the student answered incorrectly before, or those questions marked as challenging by the professor.

Another gaming element that could be adapted for ARS is a "count down" timer. A timer would add a sense of urgency and excitement to each question, induce students to practice quick thinking, and ensure the class moves at a reasonable pace.

---

83 *See, e.g.*, POLL EVERYWHERE, http://www.polleverywhere.com [http://perma.cc/9JRK-QR3B].

ARS could be used for a variety of examination types beyond a multiple-choice format. For example, in an Evidence course, students could watch videos of a witness examination in court and press a button to register objections to opposing counsel's questions. Again, students could compete on teams—for example, as prosecutors or defense counsel—and professors could follow the activity with an analysis of the merits of the objections. In an even more complex iteration of this scenario, the examining attorney and the witness could be played by live actors (perhaps students from a mock trial team), with the professor acting as the judge and students acting as the witness's counsel. During questioning, if a critical mass of students votes to object, one student who votes for the objection would have to stand up, object, and argue with opposing counsel. The professor would sustain or overrule the objection, award points for successful arguments, and deduct points for meritless objections.

Beyond ARS, professors can use a number of games and game-like pedagogies to enhance student engagement, motivation, and applied learning. Many professors have already adopted games in their classrooms to meet these goals. Professor Jennifer Rosato, currently the Dean and Professor of Law at DePaul University College of Law, created a number of games for her Civil Procedure Course, including one called "Buffalo Creek Family Feud" to "teach certain discovery rules relating to depositions, interrogatories, and requests for production of documents."[84] This game revolves around simulated litigation between two families.[85] Professor Rosato chooses six contestants with three students on each team.[86] She then poses a series of short-answer questions to each team, such as: "What is the proper way to obtain documents from the insurance company?"[87] She awards points based on the quality of the responses and the authority offered in support.[88]

The late Professor James Brown, Emeritus Professor at the George Washington University Law School, developed a semester-long game for his Land Development Law course to help students "understand the problems [of the construction and land development business] in their true context rather than as isolated, disconnected episodes."[89] He designed his game to

---

84 *See generally* Jennifer L. Rosato, *All I Ever Needed To Know About Teaching Law School I Learned Teaching Kindergarten: Introducing Gaming Techniques into the Law School Classroom*, 45 J. LEGAL EDUC. 568, 569–70 (1995).

85 *Id.* at 575.

86 *Id.*

87 *Id.* at 575–76.

88 *Id.* at 576.

89 James M. Brown, *Simulation Teaching: A Twenty-Second Semester Report*, 34 J.

"provide effective training in negotiations, legislative drafting, legal writing for lay audiences, client counseling, motions practice, ethical problems . . . ; and in discovery practice, in conducting a trial, in 'working up' witnesses; and for various types of appearances before administrative bodies and legislative committees, while laying a sound substantive foundation."[90]

Games like these are beneficial to the classroom experience because they provide incentives for achievement, increase student confidence, encourage cooperation, demonstrate the relevance of the material, and improve doctrinal and professional skills and values.[91] Supplementing standard lecture courses with in-class games and ARS would significantly upgrade the mostly passive environment that many students experience in classrooms today.

B. Solution #2: Games in a Flipped Classroom

Law school classrooms today suffer from a lack of personalized learning and a lack of choice for students. Even in a classroom designed like Solution #1—with increased engagement and feedback with ARS and other games—students are forced to learn at a pace decided by their professor. Further, students can choose only from the courses offered by their school, taught by the professors employed by their school. But, if the bulk of basic learning were conducted outside the classroom with online lectures and interactive games, learning could be personalized for students, professors could focus on active learning inside the classroom, and schools could offer more courses to students.

The Proposal:	**Gaming Elements:**
- Flipped classroom - No in-class lecturing - Focus on applied learning - Online course supplement created by teams of collaborators - Video lectures from professors around the country - Online activities and assessment - Personalized programs	- Leaderboards - Competition - Collaboration - Progress tracking - Feedback - Replay - Extra challenges - Rewards/Badges - Game levels
	Benefits: - Personalized learning - More courses to offer - Higher quality education - Career readiness

LEGAL EDUC. 638, 638 (1984)..

90 *Id.* at 639–40; *see also* Donald B. King, *Simulated Game Playing in Law School: An Experiment*, 26 J. LEGAL EDUC. 580, 580 (1974) (discussing game playing as an educational technique in a commercial law course).

91 *See* Rosato, *supra* note 84, at 570–72.

The first step in moving basic learning outside the classroom is "flipping" the classroom. In a flipped classroom, lectures are posted online as videos for students to watch outside of class.[92] A number of teachers across the education spectrum have been using flipped classrooms for years, including law school professors.[93] Moving lectures online and outside the classroom has many benefits over keeping lectures in classrooms. First, it gives students the opportunity to watch and listen to lectures at their own pace. If students fail to understand material the first time around, they can watch a lecture again without having to ask the professor to repeat the material in class and using other students' time. Second, it enables professors to use class time more efficiently with interactive discussion, simulations, and other games in the classroom. The professor can focus on engagement, motivation, and applied learning.

A more advanced flipped classroom goes a step further by adding online, interactive games and assessments for students to play outside the classroom. An excellent example of this idea in action is Khan Academy software.[94] After students watch videos on the website, an application tests them on the material to ensure understanding.[95] ARS questions like those suggested in Solution #1 can be used in this way.

While interactive programs cannot engage in complex Socratic dialogues with students, they can provide less complex quizzing for students. In effect, the program does much of the work that a professor might normally perform in a classroom. This is the promise of technology: "to liberate teachers from those largely mechanical chores so that they have more time for human interactions."[96]

An interactive program like the Khan Academy goes a step further than just asking questions and providing answers. By tracking student progress, the program can identify areas of difficulty for students.[97] The program can then take the students

---

92 *See* KHAN, *supra* note 66.

93 For example, Professor William R. Slomanson flipped his Civil Procedure course. *See* William R. Slomanson, *Blended Learning: A Flipped Classroom Experiment*, 64 J. LEGAL EDUC. 93, 95 (2014); LegalEDweb, *"Why Flip? & Macro Design" William Slomanson, Thomas Jefferson School of Law*, YOUTUBE (Nov. 6, 2014), https://youtu.be/Yo4eT17ZPmg?list=PLLxxzZq76ixxbd_KFvJYVxyezP8rxvQpY. Professor Deborah Threedy flipped her Contracts course. LegalEDweb, *"Flipping Contracts: The Making of the Videos" Debora L. Threedy, S.J. Quinney College of Law*, YOUTUBE (Nov. 6, 2014), https://youtu.be/b68yaH_k72w?list=PLLxxzZq76ixxbd_KFvJYVxyezP8rxvQpY.

94 *See* KHAN ACADEMY, https://www.khanacademy.org [http://perma.cc/3BJW-NR59]; *see also* COURSERA, coursera.com [http://perma.cc/EDF5-PWEJ].

95 *See Salman Khan TED Talk*, *supra* note 33.

96 *See* SALMAN KHAN, *supra* note 66, at 123.

97 *See Salman Khan TED Talk*, *supra* note 33.

through another review of the material the student struggled with, and even inform the instructor where the class—or a particular student—encounters trouble.[98]

Additionally, the Khan Academy software awards badges, points, and other rewards for achievements.[99] Virtual badges and points cost almost nothing to produce, but go a long way towards motivating students and encouraging learning efforts.[100] Virtual rewards can be given for simply watching video lectures and completing short assignments. Badges can be awarded publicly online to encourage competition between students. Further, rewards can easily be structured to encourage students to complete extra challenges. These challenges could be games played between students or extra missions above and beyond the assigned materials.

If the program is complex enough, it could track each individual's knowledge base across her student career to avoid unnecessary review of material already learned and to provide extra explanation for novel material. For example, if a student takes Criminal Procedure before Constitutional Law, then the Criminal Procedure program could spend extra time explaining selective incorporation of the Bill of Rights through the Fourteenth Amendment. This saves time, ensures understanding, and keeps students focused on the relevant material.

Further, by providing continuous, complex assessments, an interactive program would eliminate "Swiss cheese" learning. Khan Academy does this by requiring each student to correctly answer ten multiple-choice questions on every topic before moving on to the next topic. An interactive program used in law school should do the same, testing students on every part of the material covered in the course as opposed to the few select topics that are typically covered on a law school examination.

An interactive program would also eliminate the time professors spend checking to see that students have read or reviewed the required materials. Professors could require students to reach certain checkpoints in the program before they attend class. The program would easily identify and report to professors any student who has not completed the material. This would increase accountability and prevent students from coming to class unprepared.

---

98 *Id.*
99 *Id.*
100 *See infra* Section I.B.

Professors might work alone in posting lectures and quizzes online, but if professors shared materials online, redundancy would be avoided. In the current model, hundreds of professors across the nation prepare for and deliver similar lectures every day. At some schools, the lecture is given more than once where there are multiple sections of the same course. And the process is repeated over and over every year. This is wasteful because, in theory, a lecture needs to be given only once so that it can be recorded and shared on the Internet forever—at least until an update is needed.

Even more, professors could collaborate with software companies, video game developers, and other professors to develop a high-quality product. The result could be bundled up and sold alongside textbooks as a virtual course supplement. This would subject the product to market forces, increase the quality of legal education, and enable students to hear lectures from the best professors in the field.

If much of the work traditionally performed by a professor were moved to online content, in-class professors would not need as much time to teach the same material. A professor could spend more time focusing on activities that can only be performed live, in the classroom. Or, schools could simply retain some of the extra time and have classes meet less often.

Additionally, schools could offer a wider variety of courses to reach the niche interests of students. Because professors would be relieved of many traditional duties, schools should feel more comfortable with adjunct faculty stepping into the classroom and teaching specialized courses. The professor would only have to conduct active-learning exercises in the classroom and to create and grade examinations. Exercises and exams could even be provided to the professor in a teaching kit accompanying the virtual course. Further, because less work would be involved for the professor, correspondingly lower pay could make small class sizes financially palatable for specialized courses.

Finally, because fewer resources would be spent on preparing for lecture-based courses, schools would be free to spend more resources on preparing students for the practice of law. This could be achieved through in-class activities in existing courses, or by providing additional clinical courses.

By flipping the classroom and using virtual course supplements, law schools could increase course offerings and enable personalized learning.

C. Solution #3: Starting from Scratch

Law schools today put enormous cost pressures on students, and at the end of a three-year study, students receive a diploma and a transcript that says little about their ability to practice law in an increasingly diverse profession. If legal educators moved every aspect of legal education online that could reasonably be moved online, the cost of those components would instantly reduce to near zero—drastically lowering the expense of law school to students. Furthermore, if the credentialing roles of law schools were decoupled from the teaching roles of law schools, each individual could be credentialed separately on a range of skills instead of being lumped together in a one-size-fits-all J.D.

The Proposal:	**Gaming Elements:**
- Standalone virtual courses - Students dictate their own pace - No direct professor oversight - Peer-to-peer tutoring - Course connects students, professors, and professionals for social learning - Decoupled credentials - Customized credentials - Microcredentials - Game-based assessment - Peer-based assessment - Comprehensive, diverse assessment	- Leaderboards - Competition - Collaboration - Progress tracking - Feedback - Replay - Extra challenges - Rewards/Badges - Game levels - Playing levels
	Benefits: - Lower cost - Customized education - Accurate credentials

The first aim of Solution #3 is to lower the cost of legal education by moving much of the experience online. An online program cannot perform many aspects of legal education. Computers cannot engage students in Socratic dialogue, grade written briefs or examinations, or conduct clinical courses.[101] But, Solution #2 attempts to demonstrate that much of the work of a lecturing law school professor can be performed by a virtual course supplement. Solution #3 takes this idea as far as it will go by moving lecture-based courses entirely online. The cost of an online course to students would be significantly less than a live, in-person course.

The initial cost of developing online courses could be expensive. Basic online courses cost about $15,000 to produce.[102] Complex online courses would cost much more. If the course is

101 Not yet, at least. *See generally* RAY KURZWEIL, THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY (2005).

102 *See* JEREMY RIFKIN, THE ZERO MARGINAL COST SOCIETY: THE INTERNET OF THINGS, THE COLLABORATIVE COMMONS, AND THE ECLIPSE OF CAPITALISM 117 (2014).

deeply interactive and designed by a team of professors, software engineers, and game designers, the cost could easily rise into the hundreds of thousands of dollars. But once the course is developed, an online course can be shared online as an information technology good.

Information technology goods are important because they have near-zero marginal cost reproduction.[103] With near zero-marginal costs of reproduction, information technology goods can be instantly copied and shared with anyone connected to the internet at almost no cost. A number of industries have been revolutionized by near-zero marginal costs—for example, the music industry—and many more will follow, including legal education.[104]

So, although the upfront cost of a single online course could be significant, and many competing online courses would likely be developed, the costs can be spread across all of the students taking that course across the nation in any given year. For example, assuming a complex online Contracts course costs $500,000 to produce, and assuming five different groups develop competing Contracts courses, then the total cost of the courses would be $2.5 million. But these costs could be spread amongst the 40,000 or so law students who take Contracts every year.[105] At this rate, an entire online course would cost approximately $62.50 per student.[106] Further, the online courses could be used year after year, lowering the cost even more.[107]

Specialized courses—e.g., Estate and Gift Taxation—would cost more for students as virtual courses because the cost would be distributed among fewer students than a foundational course like Contracts. But, costs can be minimized if the courses are less complex or updated less often.

---

103 The marginal cost of reproduction of a good is the cost of producing one additional unit of that good. *Id.* at 3–4. When something is written onto a computer as source code—i.e., when it becomes an information technology good—then it can be duplicated by simply copying and pasting that source code. The cost of copying and pasting source code is the cost of running a computer for a few seconds or minutes. And because the cost of running a computer for a few seconds or minutes is near zero, the cost of reproducing an information technology good is near-zero.

104 *See generally* RIFKIN, *supra* note 102.

105 *See* Elizabeth Olson & David Segal, *A Steep Slide in Law School Enrollment Accelerates*, N.Y. TIMES (Dec. 17, 2014, 7:04 AM), http://dealbook.nytimes.com/2014/12/17/law-school-enrollment-falls-to-lowest-level-since-1987/?r=0 [http://perma.cc/EEC2-5MRL] (noting that 37,924 students started law school in 2014).

106 Of course, this assumes that the costs would be evenly distributed amongst the competing courses, and that the products would be sold without profit. But even assuming that taking these factors into account would double the price of the product, the price would still only be around the price of a law school textbook.

107 This assumes that the overhead costs of running the course and the costs of updating and upgrading the course would not significantly add to the cost.

Offering virtual courses to a massive number of students online might seem implausible, but the idea is hardly novel. A number of higher education courses are already offered over the internet, and the trend even has its own name: Massively Open Online Courses ("MOOCs").[108] Sebastian Thrun, a professor from Stanford, and Peter Norvig, a Google employee, together offered their first MOOC on Artificial Intelligence in 2011.[109] A total of 160,000 students from 190 countries signed up for the course, astonishing Professor Thurn. "Having done this, I can't teach at Stanford again," Thrun said.[110] "I feel like there's a red pill and a blue pill, and you can take the blue pill and go back to your classroom and lecture your 20 students. But I've taken the red pill, and I've seen Wonderland."[111] Thrun went on to start his own online university, Udacity, to provide a quality education for every young person in the world.[112] Law school professors, too, should be inspired by the possibility of teaching thousands of students at a time through virtual courses.

In addition to lower cost, Solution #3 enhances personalization by ditching the format of traditional courses—the bi-weekly, hour-long sessions with a single professor over a four-month semester. Instead, students would take virtual courses at their own pace without direct oversight by a professor.

Law school today is structured around learning within a particular period of time. By decoupling the traditional law school course schedule from the learning experience, students can learn at their own pace. In this way, students advance if and when they reach a specified level of mastery, rather than a specified period of time. So, if a student fails to understand a certain subject matter, he or she is not forced—or even permitted—to move on to the next topic. Instead, the student can keep working on a topic either by watching the lecture again, or by replaying the interactive games. If the student continues to have trouble with the material, the program can connect him or her with a student tutor who mastered the material. The student tutor would be rewarded with points or badges for assisting, and gain a deeper understanding of the material.[113]

---

108 Tamar Lewin, *Instruction for Masses Knocks Down Campus Walls*, N.Y. TIMES (Mar. 4, 2012), http://www.nytimes.com/2012/03/05/education/moocs-large-courses-open-to-all-topple-campus-walls.html?_r=0 [http://perma.cc/XS65-YJDU].

109 *Id.*

110 *Id.*

111 *Id.*

112 RIFKIN, *supra* note 102, at 114–15.

113 *See* Binford, *supra* note 39, at 11 (noting that "teaching generally produces the highest rate of long-term retention").

Further, courses could be offered at varying levels of difficulty—i.e., different playing levels. A course completed on easy, medium, or hard would demonstrate "proficiency," "mastery," or "excellence," respectively. Students could customize their learning profiles by reaching for "mastery" and "excellence" with courses relevant to their career paths, while general education and exploratory courses could be taken at a "proficiency" level.

Online courses also make it feasible to break up courses into smaller, distinct parts that do not fit traditional course structures. Most law schools, for instance, offer "Legal Research and Writing" that covers a wide variety of material. This course could be broken up into "Legal Research" and "Legal Writing." "Legal Writing" could be further divided into "Persuasive Legal Writing" and "Objective Legal Writing." And "Legal Citation" could be separated from "Legal Research." Another course could focus on issue spotting, another on fact gathering, and another on the analysis of appellate court opinions via the case method. Law schools already teach these concepts, but bundled together in an unorganized concoction. By separating the elements of legal education into distinct courses, each concept can be individually developed and assessed.

Individuals outside the academic sphere could also develop virtual courses. Law firms, for example, could develop courses on case management or litigation basics. The courses could be offered to all students, and firms could require students to take such courses as a condition of employment. In this way, firms could reduce the costs of employee training, share knowledge with others in the legal profession, and bolster the public image of their firm.

Because virtual courses remove the complex, live interaction often found in a law school classroom—e.g., Socratic dialogue and other social engagement—other aspects of law school would have to compensate. One way to keep social interaction in legal education is to keep some courses as live courses, such as clinical courses. A greater focus on clinical courses would also add to the educational experience. But, clinical courses do not generally focus on learning through Socratic dialogue. Therefore, in addition to increasing clinical courses, law schools could create a course with small class sizes dedicated solely to Socratic dialogue to kick-start the law school experience. The course should not focus on the material being learned, but rather on the method of learning. In this way, students could continue to reap the benefits of Socratic dialogue and the case method—i.e., learning

to think like a lawyer—without worrying about keeping pace with the material.

Another way to maintain social interaction with legal education is to couple virtual courses with live activities. Because students would take courses at their own pace, live exercises would have no defined schedule. As students reach certain checkpoints in their online courses, the program could add them to a queue to participate in live exercises. Live exercises would vary in size and type—they might be small exercises with other students, one-on-one sessions with professors, or large simulations with many participants. Live exercises might be omitted when courses are taken at the "proficiency" level, and increased in frequency when taken at the "excellence" level. But course creators should try to minimize or eliminate the need for professor involvement in live exercises to keep costs down. For example, in one exercise students would receive a hypothetical voicemail from a potential client.[114] Students would be assigned to create questions to ask the client in a future interview. After constructing questions on their own, students would meet in small groups to share and discuss their ideas. After the discussion, they could collaborate on a set of questions to present to a professor for grading. Or, the virtual course could utilize peer-to-peer grading for even greater efficiency.

Peer-to-peer grading is often used in MOOCs to grade assignments that require human eyes to evaluate, such as short-answer problems. In peer-to-peer grading, after students submit their own answers for an assignment, they are tasked with grading the submissions of about five other students who are also taking the course.[115] To reduce bias, grading is anonymous and the distribution of submissions for grading is random.[116] The final grade given to students is the median of the peer-assessed grades.[117] A number of studies have demonstrated the accuracy of peer-to-peer grading.[118]

At the end of a course, a final examination should be administered to ensure students have met course goals relative to the mastery levels of the course. While assessments during the

---

114 This example is borrowed from Professor Victoria Duke. *See* LegalEDweb, *"Bringing Exercises in Large Classes" Victoria Duke, Indiana Tech Law School,* YOUTUBE (Oct. 9, 2014), https://youtu.be/5jz7pSWbylw?list=PLdfvq_luev5uf2aUUkJOcJb0YFIIBMrhy.

115 Chris Piech et al., *Tuned Models of Peer Assessment in MOOCs*, STAN. UNIV., http://web.stanford.edu/~cpiech/bio/papers/tuningPeerGrading.pdf [http://perma.cc/SW9P-5DNL].

116 *Id.*

117 *Id.*

118 *See* RIFKIN, *supra* note 102, at 115–16; Piech, *supra* note 115.

course would be taken without oversight, strict oversight should be utilized in the final examination to deter cheating throughout the course. Law schools could have a dedicated room and staff member to administer examinations on demand, since students would move at their own pace. To prevent students from sharing questions and answers with future test-takers, one of two solutions might be adopted: either a new national examination could be created once a month and administered contemporaneously,[119] or a few dozen examinations would be available and administered randomly.[120]

The grade on the examination, however, should not show up on a transcript as the definitive sign of how much a student knows. Rather, it should test whether the student can meet the requirements for a particular level of mastery. The assessment would, in effect, certify that the student completed the online course at a particular level of mastery. Students should be able to retake the final examination as many times as they want at any level of mastery. This way, students would continue to learn the material if they have not met course goals, rather than simply assigning a letter grade and forcing them to move on to another topic. Moreover, students could return to earlier courses and complete them at higher levels of mastery.

Course assessments should be standardized across the country—or across each state—and graded by a central authority, just like the Law School Admissions Council does for the LSAT. This would eliminate the uncertainty that comes with current transcripts, and decrease the importance of which law school a student attends.

A variety of credentials could then be created to match the diversity of the profession. Credentials would vary by level of mastery, number, and type of course requirements. Some credentials might require dozens of courses, while others might only require ten. Some might require Mock Trial or Federal Income Tax, and others not at all. Some might require excellence across the board, and others mere proficiency. The result would be credentials that would accurately indicate the breadth of an individual's knowledge for potential employers. Further, it would enable students to intricately customize their law school experience.

---

119 In this way, the examination would not be perfectly "on demand," but it would nonetheless be available for a student to take within one month of finishing the course.

120 Of course, if the same few dozen examinations are administered over and over, students would still be able to share questions and answers—especially over the internet. But, any student who studies the answers to a few dozen examinations is likely to have met course objectives regardless.

Finally, courses should be offered, and encouraged, for law school graduates. Graduates looking to change jobs and enter new legal fields could have access to courses to acquire particular credentials. And online courses could substitute for MCLE credits, making it easier for lawyers to stay updated with relevant legal knowledge.

With these changes, law schools could drastically reduce the cost of legal education and focus on social learning that online courses cannot provide. Students would graduate with significantly less student debt, ready to enter the legal profession with a customizable set of credentials that accurately reflects the particulars of each individual's abilities.

CONCLUSION

The Langdellian model is long broken and in dire need of repair. From the lack of engagement, to minimal feedback, to limited course offerings, to nebulous credentials, to the mountains of debt piled on students, the legal education system fails the very people it intends to serve. Gamification is fit to solve each of these problems.

Games motivate us to engage with our work; they provide meaning to our experiences; and they challenge us to overcome obstacles. Games even motivate some of us to virtually farm *for free*. Gamification takes queues from these lessons by using game thinking and game mechanics to engage audiences and solve problems.

Law school is already a loose collection of games. Aside from lecturing, nearly all pedagogy is gaming. Legal educators, therefore, are already in the business of game development. Why not look to game developers for help?

Em"BARK"ing on the Journey to Expand Recovery of Damages for the Loss of a Companion Animal

*Jade McKenzie**

INTRODUCTION

When Tootsie, a two-year-old Maltese dog, was diagnosed with a respiratory disorder requiring corrective surgery, her owner desperately feared for the safety and well-being of her beloved pet.[1] The veterinarian advised the dog's owner of the risks associated with such a procedure and the importance of withholding all food and water for twenty-four hours following surgery.[2] Contrary to her own instructions, the veterinarian proceeded to feed Tootsie a food mixture merely two hours after the surgery, causing Tootsie to aspirate the mixture into her lungs, and ultimately resulting in her premature death.[3] When Tootsie's owner was informed of this tragedy, the veterinarian attempted to conceal the fact that it was her own negligence that caused Tootsie's death.[4] Due to the current state of the law in California, the court refused to award any type of emotional distress damages to sufficiently compensate Tootsie's owner for the negligent killing of her precious dog, leaving her with nothing but heartache.[5]

Tootsie's owner is only one of many individuals who are forced to endure the loss of man's best friend without any compensation to acknowledge the emotional impact of such a tragic event. In *Carbasho v. Musulin*, a West Virginia Supreme Court decision, a woman who witnessed the death of her pet dog was only permitted to recover the dog's fair market value after he

---

* J.D., Chapman University Dale E. Fowler School of Law, May 2016; B.A., California Polytechnic State University, San Luis Obispo, 2013. I would like to thank Professor Kenneth Stahl for his thoughtful guidance throughout the development of this Comment; the Editors of the *Chapman Law Review* for their hard work in the publication process; and my mother, Liddy, and father, Ken, for their unconditional love and support.

1 McMahon v. Craig, 97 Cal. Rptr. 3d 555, 558 (Ct. App. 2009).

2 *Id.*

3 *Id.* at 558–59.

4 *Id.* at 559.

5 *Id.* at 564.

was struck and killed by a negligently driven vehicle while the two of them were taking a walk.[6] It is the unfortunate reality that the vast majority of individuals who suffer the loss of a pet must undergo severe pain and suffering without receiving compensation for their emotional distress. In fact, the majority of courts refuse to allow plaintiffs to recover non-economic emotional distress damages arising from the injury to or death of a companion animal; rather, the judiciary is stuck in an antiquated mode of viewing animals as if they were any other form of inanimate personal property, limiting recovery to their fair market value.[7]

Although the role that companion animals play in American society has been gradually transitioning away from mere property and is becoming more akin to that of a family member, the judiciary has failed to keep pace with this change.[8]

> Today, 63% of all American households have one pet, 45% have more than one. In fact, there are more pets in America than there are citizens (360 million pets, 290 million people). Americans will spend upwards of $36 billion pampering those pets this year, an amount nearly equal to the amount Americans spend on toys and candy *combined* . . . . Beyond question, many Americans love their cats, their dogs, their birds, as well as they love their children. But like the children of the pre-industrial revolution, the [judiciary] chooses to categorize those pets as nothing more than chattel.[9]

What were once treated as items of personal property, used solely for economic purposes, are now providing societal benefits to humans, such as companionship, affection, and emotional fulfillment. Despite judicial recognition of such a significant change, courts continue to label companion animals as personal property, thereby prohibiting plaintiffs from recovering emotional distress damages when they are forced to grieve the loss of a pet.[10] The unconditional love and companionship that pet owners derive from their furry friends creates an emotional dependence that persists even after the animal's death, just as it would upon the death of a family member, and this relationship

---

6 Carbasho v. Musulin, 618 S.E.2d 368, 371 (W. Va. 2005) ("[D]ogs are personal property and damages for sentimental value, mental suffering, and emotional distress are not recoverable for the negligently inflicted death of a dog.").

7 Steven M. Wise, *Recovery of Common Law Damages for Emotional Distress, Loss of Society, and Loss of Companionship for the Wrongful Death of a Companion Animal*, 4 ANIMAL L. 33, 50 (1998).

8 Sabrina DeFabritiis, *Barking up the Wrong Tree: Companion Animals, Emotional Damages and the Judiciary's Failure to Keep Pace*, 32 N. ILL. U. L. REV. 237, 245 (2012).

9 *Carbasho*, 618 S.E.2d at 372 (Starcher, J., dissenting) (internal citations omitted).

10 *Id.*

should be afforded better recognition by the law.[11] One of the most crucial roles of the judiciary is to adapt to society's changing attitudes and to formulate remedies that account for such changes. Nevertheless, while courts have acknowledged the emotional bond that often exists in the relationships between people and their pets, the current state of the law fails to adequately address this change, leaving many aggrieved plaintiffs without a legal remedy.[12]

While courts have historically refused to recognize the recovery of emotional distress damages associated with the injury to or death of a companion animal, some states have recently begun to recognize a plaintiff's ability to recover non-economic damages as a result of the intentional injury to a companion animal.[13] Among these states is California, which recently held in *Plotnik v. Meihaus* that "a person's intentional injuring or killing a pet will support recovery of damages for intentional infliction of emotional distress," reasoning that the strong emotional connection that exists between a human and a companion animal indicates that recovery for emotional distress damages is warranted in particular situations.[14] Although courts are certainly taking steps in the right direction, limiting the potential recovery of emotional distress damages to cases involving intentional conduct leaves countless plaintiffs, such as Tootsie's aggrieved owner, without a sufficient remedy. This Comment will address the need for expanding California's recognition of non-economic emotional distress damages to include recovery for the loss of a companion animal due to the *negligent* conduct of another.

Although California has allowed for the recovery of emotional distress damages when a pet has been intentionally injured or killed, this rule should similarly apply to the negligent injuring or killing of a companion animal. A plaintiff may recover under a theory of negligent infliction of emotional distress in

---

11 *Id.*

12 *See, e.g.*, Hendrickson v. Tender Care Animal Hosp. Corp., 312 P.3d 52, 54–55 (Wash. Ct. App. 2013) (recognizing human-animal bond, but refusing to award emotional distress damages for the negligent death or injury to a pet).

13 *See* Richardson v. Fairbanks N. Star Borough, 705 P.2d 454, 456 (Alaska 1985) (stating that the court is willing to recognize a cause of action for intentional infliction of emotional distress for the intentional killing of a pet); Gill v. Brown, 695 P.2d 1276, 1278 (Idaho Ct. App. 1985) (holding that plaintiffs are entitled to recover emotional distress damages for the intentional killing of their pet donkey); Burgess v. Taylor, 44 S.W.3d 806, 809–12 (Ky. Ct. App. 2001) (recognizing the court's ability to award emotional distress damages when defendant sold plaintiff's pet horses to a slaughterhouse without her knowledge).

14 Plotnik v. Meihaus, 146 Cal. Rptr. 3d 585, 600–03 (Ct. App. 2012).

certain situations involving the death or injury of a family member;[15] however, California has refused to find a defendant liable for this cause of action when the case involves negligent conduct towards an animal. While it is concededly true that the loss of a family member is likely to result in greater hardship than the loss of a companion animal, it is virtually undisputed that the death of a pet is considered to be a traumatic event that will also lead to significant emotional devastation. Due to the analogous nature of these relationships based upon the grief that accompanies either loss, such protection should be granted in the latter situation as well as the former. The state's failure to adapt to modern views regarding companion animals leaves numerous plaintiffs without an adequate remedy when they suffer the loss of their beloved pet. Courts have repeatedly acknowledged the special relationship that often exists between humans and companion animals, yet there have been no efforts to alter the law to provide a sufficient remedy when this relationship has been destroyed in situations involving negligence. Moreover, emotional distress damages are compensatory in nature, and thus serve to make the plaintiff whole in cases where a person has been the victim of another's wrongful conduct. As such, whether a person's conduct is intentional or negligent should be irrelevant when awarding emotional distress damages. In making this determination, the focus should be on the plaintiff's recovery rather than the defendant's actions.

In this Comment, Part I will address the history of the classification of nonhuman animals as property, and will discuss the enactment of statutes and judicial interpretations concerning the recovery of damages for the loss or destruction of personal property. Part II will discuss the current state of the law pertaining to the availability of emotional distress damages, particularly in California, and how states have applied these damage awards to cases involving the negligent harm to a companion animal. Finally, Part III will identify the issues associated with the lack of recognition of such damages and will propose a solution by suggesting that California allow a plaintiff to recover emotional distress damages for the negligent, as well as the intentional, injury to or death of a companion animal.

---

15 *See, e.g.*, Stump v. Ashland, Inc., 499 S.E.2d 41, 52 (W. Va. 1997) (allowing claim of negligent infliction of emotional distress after truck crashed into house resulting in homeowners' deaths).

I. ANIMALS AS PROPERTY AND AVAILABLE DAMAGES

Historically, and still to this day, all animals have been considered the personal property of humans.[16] As a result, when a person suffered the loss of a companion animal, the available damages were initially limited to the fair market value of the animal.[17] Due to the tragic nature of such an event and the emotional suffering that often accompanies the loss, courts began to recognize that this limited remedial scheme was vastly insufficient. In an effort to adequately compensate these individuals, many courts now allow additional damages to be recovered, including medical expenses and, in some cases, emotional distress damages.[18] While California has recently expanded the availability of emotional distress damages for the loss of a companion animal, many plaintiffs are still left without a sufficient remedy, resulting in the need for further expansion.[19]

A. Animals as Personal Property

The emerging debate between scholars and animal rights advocates over the proper classification of animals has led to many changes in the way both society and the legal system view companion animals. Ranging from civil liability to criminal prosecution, the law's treatment of injury to or death of a companion animal has been drastically altered in recent years, and continues to change. While animal rights have significantly increased over the past few centuries, the continuing classification of animals as personal property has left countless animals and their human counterparts without a proper avenue for relief.

There currently exist three basic categories of property recognized in the American legal system—real property, personal property, and intellectual property.[20] Personal property is "physical, moveable, and has a limited physical existence," and as such, animals have historically fallen under this broad classification.[21] Some scholars believe that the justification for

---

16 David Favre, *Living Property: A New Status for Animals Within the Legal System*, 93 MARQ. L. REV. 1021, 1026 (2010).

17 William C. Root, *"Man's Best Friend": Property or Family Member? An Examination of the Legal Classification of Companion Animals and Its Impact on Damages Recoverable for Their Wrongful Death or Injury*, 47 VILL. L. REV. 423, 423–24 (2002).

18 *See* Leith v. Frost, 899 N.E.2d 635, 641 (Ill. App. Ct. 2008) (modifying trial court judgment to award damages in the amount that plaintiffs paid in veterinarian bills, rather than fair market value); *see also Gill*, 695 P.2d at 1278 (awarding emotional distress damages for intentional killing of pet).

19 *Plotnik*, 146 Cal. Rptr. 3d at 603–04.

20 Favre, *supra* note 16, at 1025.

21 *Id.* at 1026.

the legal status of animals as property is based both in theology, and on the inferior status of nonhuman animals.[22] This type of classification has resulted in both procedural and substantive hurdles for animals and their advocates, such as the inability of an animal to sue on its own behalf, the denial of rights and privileges that are afforded to humans, and of course, a plaintiff's inability to recover damages for the wrongful death or injury of a pet.[23] These concerns have prompted a series of arguments urging for a change in the legal classification of animals as property. While some scholars argue that a fourth category of property should be created to accommodate for the unique characteristics possessed by animals, others advocate for a change in their property status altogether, arguing that animals should be afforded the status of "legal personhood."[24]

In his article entitled *The Legal Thinghood of Nonhuman Animals*, Steven Wise, President of the Center for the Expansion of Fundamental Rights in Boston, argues that although the "legal thinghood" of animals is derived primarily from ancient law and primitive legal systems, when legal rules no longer reflect current values, such rules must be reconsidered.[25] He addresses the fact that the earliest examples of law clearly demonstrate legal ownership of nonhuman animals, but that these theories of law were founded upon notions of "divine power" as opposed to justice.[26] Modern legal theory, he argues, has essentially replaced this method of law, and requires a consideration of normative principles and scientific discoveries that have since been

---

22 Derek W. St. Pierre, *The Transition from Property to People: The Road to the Recognition of Rights for Non-human Animals*, 9 HASTINGS WOMEN'S L.J. 255, 261 (1998) ("The first has a theological basis, established in the Bible. In Genesis, man is given 'dominion over the fish of the sea, and over the birds of the air, and over the cattle, and over all the earth, and over every creeping thing that creeps upon the earth.' A second justification rests in the 'inferior' status of non-human animals. Historically, non-human animals were viewed as lacking a 'soul,' a 'mind,' a 'will,' or whatever attribute it was thought makes humans uniquely human.").

23 BRUCE A. WAGMAN ET AL., ANIMAL LAW: CASES AND MATERIALS 51 (4th ed. 2010).

24 Steven Wise, *The Legal Thinghood of Nonhuman Animals*, 23 B.C. ENVTL. AFF. L. REV. 471, 472 (1996); *see also* CAROL B. MATLACK, WE'VE GOT FEELINGS TOO!: PRESENTING THE SENTIENT PROPERTY SOLUTION *passim* (Barbara K. Lawing & April Turner eds., 2006) (arguing for a new category of property referred to as "sentient property"); Favre, *supra* note 16, at 1021–22 (arguing for a new category of property referred to as "living property"); Susan J. Hankin, *Not a Living Room Sofa: Changing the Legal Status of Companion Animals*, 4 RUTGERS J.L. & PUB. POL'Y 314, 379 (2007) (arguing for a new category of property referred to as "companion animal property").

25 Wise, *supra* note 24, at 473–74. "As every legal rule has its unique history, an understanding of this history is instrumental in the reconsideration to which every legal rule eventually becomes subjected." *Id.* at 474.

26 *Id.* at 543.

founded.[27] Due to the fact that the foundations of ancient laws are no longer applicable and have been fundamentally destroyed, the application of these laws "violates modern notions of fundamental principles of justice."[28] Wise argues that "scientific discovery has created new views of life and of nature and decisively undermined the hierarchical cosmologies that once underpinned the transcendence of human over nonhuman animals," and as such, "legal values, principles, and rights are not inherently limited to human beings, but entitle at least some nonhuman animals to transcend their historical legal thinghood and to draw equally upon these sources for legal personhood . . . ."[29]

Notwithstanding the numerous scholars who are in support of this view,[30] the harsh reality is that animals continue to be classified as personal property and are treated as such with respect to the law. Nevertheless, while these animals are considered to be the personal property of humans in all fifty states,[31] many changes have taken place to accommodate for the previously mentioned hardships that this classification places on animals. In 1867, Henry Bergh founded the first American Society for the Prevention of Cruelty to Animals ("ASPCA") in New York, which was aimed at promoting the interests of animals in being free from unnecessary pain and suffering.[32] Since that time, hundreds of local humane societies have been established across the country in an attempt to advocate for an increase in animal rights.[33] Additionally, every state has adopted its own anti-cruelty laws designed to prevent the mistreatment of animals, and as of 2009, forty-six states and the District of Columbia had at least one felony anti-cruelty law.[34] Specifically, California has enacted more than 100 statutes pertaining to the treatment of animals.[35] Among these is California Penal Code section 597, enacted in 1872 and aimed at preventing cruelty to

---

27 *Id.* at 543–44.

28 *Id.* at 475.

29 *Id.* at 545–46.

30 *See generally* Jessica Berg, *Of Elephants and Embryos: A Proposed Framework for Legal Personhood*, 59 HASTINGS L.J. 369 (2007); Carter Dillard, *Empathy with Animals: A Litmus Test for Legal Personhood?* 19 ANIMAL L. 1 (2012); Christopher D. Seps, Note, *Animal Law Evolution: Treating Pets as Persons in Tort and Custody Disputes*, 2010 U. ILL. L. REV. 1339.

31 WAGMAN ET AL., *supra* note 23, at 74.

32 Favre, *supra* note 16, at 1028.

33 *Frequently Asked Questions*, ASPCA, http://www.aspca.org/about-us/faq/how-many-aspcas-are-there [http://perma.cc/6BHZ-KZ36].

34 WAGMAN ET AL., *supra* note 23, at 91–92.

35 *Animal Legal & Historical Center*, MICH. ST. U., https://www.animallaw.info/statutes/us/california?page=2 [http://perma.cc/7UH9-P2BW].

animals, which states that "every person who maliciously and intentionally maims, mutilates, tortures, or wounds a living animal, or maliciously and intentionally kills an animal, is guilty of a crime,"[36] and defines an animal as "every dumb creature."[37]

Furthermore, in 2012, the Oregon Court of Appeals issued a ruling in *State v. Nix* that classified nonhuman animals as "victims" for the purpose of prosecuting under Oregon anti-cruelty statutes, essentially expanding the recognition of animal rights in the state.[38] In *Nix*, the defendant was found to be in possession of dozens of emaciated horses and goats and was ultimately convicted of twenty counts of second-degree animal abuse.[39] The court held that even though the animals were still considered to be the personal property of the defendant, each of the twenty neglected farm animals was a separate victim.[40] In reaching this conclusion, the court reasoned that "none of the provisions upon which defendant relies . . . expressly or implicitly provides that the victim of a violation of the animal neglect statutes is a person" and that "even though animals usually are the property of persons, there is a broader public interest in their health, care, and well-being that requires vindication when they are neglected."[41] However, on March 5, 2015, the Supreme Court of Oregon vacated this landmark decision for lack of jurisdiction, holding that the State did not have authority to appeal the misdemeanor judgment and, as a result, both the court of appeals and the supreme court lacked judicial power to issue opinions.[42] Although the decision has been vacated, the court's rationale in issuing such a ruling indicates its willingness to expand animal rights and potentially recognize that animals should be classified as more than mere property.

While there has been a significant increase in the recognition of animal rights and interests on both the statutory and institutional level, there still exists a large concern associated with the ability of plaintiffs to recover emotional distress damages for the loss of their pet. These concerns are primarily due to a companion animal's continued legal status as property. Although courts have recognized that the distinct nature of an

---

36 CAL. PENAL CODE § 597 (West 2016).

37 People v. Baniqued, 101 Cal. Rptr. 2d 835, 840–41 (Ct. App. 2000).

38 State v. Nix, 283 P.3d 442, 449 (Or. Ct. App. 2012), *vacated*, 345 P.3d 416 (Or. 2015) ("[T]he individual animal identified in each count of second-degree animal neglect for which defendant was found guilty qualified as a separate victim . . . .").

39 *Id.* at 443.

40 *Id.* at 449.

41 *Id.* at 446–48.

42 State v. Nix, 345 P.3d 416, 424 (Or. 2015).

animal necessitates the creation of rules to acknowledge its unique status,[43] the ability to recover non-economic damages in situations where an animal has been intentionally or negligently killed or injured is still severely lacking.

B. Recovery for Damage to Personal Property

While an individual who suffers the loss of a companion animal may generally recover the fair market value of the animal, this nominal value is clearly insufficient when considering the overall purpose of civil recovery. Legal remedies are designed to compensate a plaintiff for the defendant's wrongful conduct; in determining the type of compensation that should be awarded, it is crucial to look at the nature of the injury and provide compensation that will make the plaintiff whole. In many cases involving injury to a companion animal, however, a plaintiff is not made whole absent an award of emotional distress damages.

In a lawsuit involving tortious conduct, there are two general types of damages that a plaintiff may be able to recover: punitive damages and compensatory damages. The United States Supreme Court has defined punitive damages as "private fines intended to punish the defendant and deter future wrongdoing," whereas compensatory damages "redress the concrete loss that the plaintiff has suffered by reason of the defendant's wrongful conduct."[44] In other words, compensatory damages are generally thought of as those that serve to make the plaintiff whole, and include both economic and non-economic damages. While economic damages "compensate plaintiffs for tangible injuries" and often refer to measurable amounts such as lost earnings or medical expenses, non-economic damages "compensate plaintiffs for intangible injuries such as pain and suffering, loss of companionship, and emotional distress."[45]

In lawsuits arising from the loss or destruction of personal property, California has generally limited the measure of damages to the fair market value of the property at the time of the loss or destruction,[46] refusing to allow the recovery of

---

43 *See* Morgan v. Kroupa, 702 A.2d 630, 633 (Vt. 1997) ("[M]odern courts have recognized that pets generally do not fit neatly within traditional property law principles. . . . Instead, courts must fashion and apply rules that recognize their unique status.").

44 Cooper Indus., Inc. v. Leatherman Tool Grp., Inc., 532 U.S. 424, 424 (2001).

45 Victor E. Schwartz & Emily J. Laird, *Non-economic Damages in Pet Litigation: The Serious Need to Preserve a Rational Rule*, 33 PEPP. L. REV. 227, 230 (2006).

46 23 CAL. JURISPRUDENCE 3D DAMAGES § 69 (2015).

non-economic damages in such cases. Due to an animal's property classification, courts have historically extended this limitation to situations where an animal has been the victim of intentional or negligent injury or death.[47] However, several states, including California, now recognize that "[p]ets are no longer exclusively treated as property with regard to damages" and have consequently expanded the available recovery in such lawsuits.[48] Indeed, California's state legislature has acknowledged the availability of additional damages in animal-related lawsuits by codifying this change in California Civil Code section 3340, which states that: "[f]or wrongful injuries to animals being subjects of property, committed willfully or by gross negligence, in disregard of humanity, exemplary damages may be given."[49] Although this type of allowance has commonly referred to the recovery of punitive damages in cases involving intentional injury,[50] or an award of economic damages, such as reasonable medical expenses relating to the injury or death of the animal, very recently courts have begun awarding non-economic damages, such as damages for emotional distress.[51] In doing so, courts have focused on the property's actual and intrinsic value and the injury to the plaintiff, stating that "harm may be caused to a person's emotional well-being by malicious injury to that person's pet as personal property," but continuing to acknowledge that damages for sentimental value are not recoverable.[52] As a result, many states have started to take a step in the right direction by allowing the recovery of additional damages when a person's pet has been injured or killed.

II. CURRENT STATE OF THE LAW

Every state has recognized that nonhuman animals possess sentient traits and qualities that inherently distinguish them

---

47 *See, e.g.*, Johnson v. Douglas, 723 N.Y.S.2d 627, 628 (App. Div. 2001) (dismissing plaintiff's claim for emotional distress damages based upon negligent or malicious killing of dog because of its property classification); Goodby v. Vetpharm, Inc., 974 A.2d 1269, 1274 (Vt. 2009) (holding that the measure of damages for death of pet cats was fair market value prior to death less fair market value after death).

48 JUDICIAL COUNCIL OF CAL., CIVIL JURY INSTRUCTION, CACI No. 3903O (2016).

49 CAL. CIV. CODE § 3340 (West 2016).

50 Burgess v. Taylor, 44 S.W.3d 806, 813 (Ky. Ct. App. 2001) (finding that the trial court did not abuse its discretion in awarding $75,000 in punitive damages).

51 *See* Martinez v. Robledo, 147 Cal. Rptr. 3d 921, 927 (Ct. App. 2012) (stating that an injured pet owner's recovery of costs incurred in treatment and care is an appropriate measure of damages); Kimes v. Grosser, 126 Cal. Rptr. 3d 581, 586 (Ct. App. 2011) (allowing plaintiff to present bills incurred to save pet cat in recovering reasonable and necessary costs); *see also* Womack v. Von Rardon, 135 P.3d 542, 546 (Wash. Ct. App. 2006) (holding that malicious injury to a pet can support a claim for emotional distress damages).

52 *Womack*, 135 P.3d at 546.

from other forms of property. As a result, courts are now changing their approach when confronted with cases involving an injury to an animal, and often will treat companion animals as more than mere property by allowing their owners to receive additional forms of compensation. Some states, including Washington,[53] Kentucky,[54] Alaska,[55] Idaho,[56] Florida,[57] Louisiana,[58] and Connecticut,[59] have already acknowledged the availability of emotional distress damages based on the intentional injury to a companion animal. Until 2012, California had refused to make such a determination, limiting the available remedies in cases involving the injury to or death of an animal to economic damages.[60] In a landmark decision, however, the California Court of Appeal for the Fourth District changed the state's view and held that a person who intentionally kills or injures an animal may be liable for emotional distress damages.[61]

A. *Plotnik v. Meihaus*: A Landmark Change in California Law

In 2003, plaintiffs David and Joyce Plotnik moved into a home with their two children and their miniature pinscher dog, Romeo, next door to the Meihaus family.[62] In the six years following their move, the plaintiffs and the defendant, John Meihaus, Jr., developed a hostile relationship consisting of countless adverse encounters between the two families.[63] This relationship came to an end on April 9, 2009, when Romeo ran into the Meihaus' backyard after hearing a loud banging noise coming from their property.[64] After his dog began barking, David Plotnik heard a loud squeal and subsequently saw Romeo rolling down the slope of the yard.[65] When Mr. Plotnik entered the Meihaus' yard, Mr. Meihaus was holding a bat, shouting at Mr. Plotnik "to be more courteous and get [his] dogs to stop

---

53 *See id.*

54 *See Burgess*, 44 S.W.3d at 812.

55 *See* Richardson v. Fairbanks N. Star Borough, 705 P.2d 454, 456 (Alaska 1985).

56 *See* Gill v. Brown, 695 P.2d 1276, 1278 (Idaho Ct. App. 1985).

57 *See* La Porte v. Associated Indeps., Inc., 163 So. 2d 267, 269 (Fla. 1964).

58 *See* Brown v. Crocker, 139 So. 2d 779, 781 (La. Ct. App. 1962).

59 *See* Liotta v. Segur, No. CV020347756S, 2004 WL 728829, at *1 (Conn. Super. Ct. Mar. 15, 2004).

60 *See* Kimes v. Grosser, 126 Cal. Rptr. 3d 581, 586 (Ct. App. 2011) (limiting damages to fair market value when defendant shot and killed pet cat); McMahon v. Craig, 97 Cal. Rptr. 3d 555, 565 (Ct. App. 2009) (refusing to award emotional distress damages when veterinarian negligently killed pet dog).

61 Plotnik v. Meihaus, 146 Cal. Rptr. 3d 585, 603 (Ct. App. 2012).

62 *Id.* at 591–92.

63 *Id.*

64 *Id.* at 592.

65 *Id.*

barking."[66] Meihaus' striking of Romeo caused the dog to have difficulty walking, and ultimately required Romeo to undergo surgery to repair his right rear leg.[67]

The court acknowledged the availability of an award for emotional distress damages as a result of the defendant's conduct, holding that "California law allows a pet owner to recover for mental suffering caused by another's intentional act that injures or kills his or her animal."[68] In doing so, the court recognized that other states have acknowledged a pet owner's ability to "recover for mental suffering caused by another's wrongful acts resulting in the pet's injury or death" and focused on the strong attachment that may exist between a person and a pet.[69] The court quoted the 1889 California Supreme Court case *Johnson v. McConnell*, noting that "there are no other domestic animals to which the owner or his family can become more strongly attached, or the loss of which will be more keenly felt."[70] In determining the award of damages, the court individually addressed the plaintiffs' separate causes of actions for trespass to personal property, negligent infliction of emotional distress, and intentional infliction of emotional distress. Basing its decision on the property status of the animal, the court found that the defendant was liable for emotional distress damages under the plaintiffs' trespass claim.[71] Consequently, the court refused to allow additional emotional distress damages based on the claim for intentional infliction of emotional distress, simply stating that "[a]llowing recovery for the same conduct here would amount to double recovery."[72]

In denying the plaintiffs' request for emotional distress damages based on their negligence claim, the court adopted its previous holding in *McMahon v. Craig*, which held that "a pet owner could not recover damages for emotional distress or loss of companionship based on a veterinarian's negligent treatment that resulted in a dog's death."[73] However, *Plotnik* is easily distinguishable from *McMahon* because the claim in *McMahon* involved negligence in the veterinarian context, whereas the injury in *Plotnik* involved the conduct of a neighbor. The court in *McMahon* addressed the difficulty in creating a rule that imposes

66 *Id.* at 593.
67 *Id.*
68 *Id.* at 591.
69 *Id.* at 600.
70 *Id.* (quoting Johnson v. McConnell, 22 P. 219, 220 (Cal. 1889)).
71 *Id.* at 599–601.
72 *Id.* at 605.
73 *Id.* at 598 (citing McMahon v. Craig, 97 Cal. Rptr. 3d 555, 564 (Ct. App. 2009)).

liability on veterinarians who have negligently injured or killed a person's pet as a result of medical treatment or care, stating that such a rule would raise serious policy concerns pertaining to increased insurance rates or decreased availability of veterinarian care.[74] Allowing the recovery for the negligent injury to a pet outside of the context of veterinary care does not implicate the same policy considerations and, therefore, should have been afforded greater weight in the court's analysis in *Plotnik*. Nevertheless, the court's decision to award the plaintiffs emotional distress damages based on the defendant's intentional conduct demonstrates the affirmative steps that the judiciary is taking to find a proper balance between an animal's property status and its emotional connection with humans in determining the availability of damages in similar situations.

B. The Lack of Recovery in Cases Involving Negligence

While many states, such as California, have unequivocally determined that a plaintiff may recover emotional distress damages for the intentional injuring or killing of a companion animal, the recovery for cases involving a defendant's negligent conduct is still severely lacking. Based primarily on the level of culpability in cases involving negligence and the absence of any maliciousness or ill-will that often accompanies intentional acts, courts have unanimously concluded that an individual may not recover emotional distress damages for the injury to or death of a pet. Nevertheless, California has recognized that a plaintiff may recover emotional distress damages for cases involving negligence in other contexts, and such recognition should be expanded to include cases involving harm to companion animals.

The claim of negligent infliction of emotional distress is a controversial cause of action that has been interpreted in a variety of ways among the various states. The California Supreme Court has analyzed this claim by reference to two theories of recovery—the bystander theory and the direct victim theory.[75] Under the bystander theory, damages for emotional distress are recoverable when the plaintiff:

> (1) is closely related to the injury victim; (2) is present at the scene of the injury-producing event at the time it occurs and is then aware that it is causing injury to the victim and, (3) as a result suffers emotional distress beyond that which would be anticipated in a disinterested witness.[76]

---

74 *See McMahon*, 97 Cal. Rptr. 3d at 564.

75 Gu v. BMW of N. Am., LLC, 33 Cal. Rptr. 3d 617, 622 (Ct. App. 2005).

76 Thing v. La Chusa, 771 P.2d 814, 815 (Cal. 1989).

The California Supreme Court has further elaborated on this theory by stating that "[a]bsent exceptional circumstances, recovery should be limited to relatives residing in the same household, or parents, siblings, children, and grandparents of the victim."[77] Due to the fact that a companion animal is generally not considered to be a family member of a household, California courts have never found negligent infliction of emotional distress under the bystander theory in situations involving companion animals. Under the direct victim theory, the California Supreme Court has emphasized that a finding of negligent infliction of emotional distress is fundamentally the same as the claim of negligence, which requires the essential elements of duty, breach, causation, and damages.[78] Additionally, as was seen in the *Plotnik* decision, courts may award emotional distress damages based on any other tort claim, such as trespass to chattels, but have rarely done so.[79]

Although no state currently allows an award of emotional distress damages based on the negligent injury or death of an animal, some states have acknowledged that this possibility may in fact exist. In the 1981 case of *Campbell v. Animal Quarantine Station*, the Supreme Court of Hawaii awarded emotional distress damages when a plaintiff's pet dog was negligently killed during her transportation to a nearby hospital.[80] The court stated that "[w]here a claim for serious mental distress is made, and the mental distress is inflicted when a person endures negligently inflicted property damage, there is no requirement that plaintiffs must actually witness the tortious event in order to recover," and awarded the plaintiffs $1000 in emotional distress damages.[81] However, five years later, Hawaii's legislature enacted a statute which barred recovery for emotional distress arising from any type of property damage, effectively rendering the court's holding in *Campbell* invalid.[82] The statute was enacted as part of a tort reform effort triggered by a local hurricane, when numerous plaintiffs sought emotional distress damages arising from damage to their homes and belongings.[83] Although Hawaii no longer permits such recovery, the court's analysis in *Campbell* provides useful insight into the possibility of allowing emotional distress damages in future negligence cases

---

77 *Id.* at 829 n.10.
78 *Gu*, 33 Cal. Rptr. 3d at 623.
79 *See supra* Section II.A.
80 Campbell v. Animal Quarantine Station, 632 P.2d 1066, 1067 (Haw. 1981).
81 *Id.* at 1066.
82 HAW. REV. STAT § 663-8.9 (West 2016).
83 WAGMAN ET AL., *supra* note 23, at 201.

involving damage to personal property. In reaching its holding, the court relied on its previous ruling in *Rodrigues v. State*, in which it permitted recovery for mental distress due to the negligent destruction of the plaintiff's home.[84] By drawing this comparison between a pet and a home, the court suggests that these distinct types of personal property should be treated the same. Of course, such an analysis would necessitate the concession that animals are in fact property, but the benefits of allowing an award of emotional distress damages based on this logic would likely outweigh any negative implications attached to an animal's already established property classification.

Hawaii is not the only state that has acknowledged the possibility of awarding emotional distress damages in negligence cases involving injury to an animal. In *McAdams v. Faulk*, the Arkansas Court of Appeals held that "[d]amages on a negligence claim are not limited to economic loss damages, and include compensation for mental anguish" and reversed the dismissal of a case involving veterinary malpractice where the plaintiff's dog suffered a neck injury after the veterinarian's office inappropriately used a choke holder to quiet him.[85] Additionally, in *Knowles Animal Hospital, Inc. v. Willis*, the Florida Third District Court of Appeal held that "the [lower] court did not commit err by including for consideration of the jury the element of the mental pain and suffering of the plaintiff-owners of the dog" when a dog was negligently left on a heating pad following its operation at a hospital, resulting in a severe burn and disfigurement, and ultimately, his death.[86] Moreover, in determining whether the bystander theory of negligent infliction of emotional distress applied in a case where the plaintiff's dog was shot and killed by a police officer, the Supreme Court of Wisconsin recognized that "humans form important emotional connections that fall outside the class of spouse, parent, child, grandparent, grandchild or sibling. . . . The emotional harm occurring from witnessing the death or injury of an individual who falls into one of these relationships is serious, compelling, and warrants special recognition."[87] Nevertheless, the court refused to award emotional distress damages in such a case because allowing recovery would "enter a field that has no sensible or just stopping point."[88] Courts have repeatedly acknowledged

---

84 *Campbell*, 632 P.2d at 1068.

85 McAdams v. Faulk, No. CA 01-1350, 2002 WL 700956, at *5 (Ark. Ct. App. Apr. 24, 2002).

86 Knowles Animal Hosp., Inc. v. Willis, 360 So. 2d 37, 38 (Fla. Dist. Ct. App. 1978).

87 Rabideau v. City of Racine, 627 N.W.2d 795, 801 (Wis. 2001).

88 *Id.* at 802.

the existence of an emotional connection between companion animals and their owners and have conceded that special recognition should be afforded to such relationships, yet the law has failed to provide for this recognition in cases involving the negligent injury to or death of a pet. Due to the courts' acknowledgement of such a bond, the next logical step towards the expansion of civil recovery is the allowance of non-economic damages in cases involving the negligent conduct of an individual.

III. ALLOWING NON-ECONOMIC DAMAGES IN CLAIMS INVOLVING NEGLIGENT CONDUCT

There are many situations where an individual's pet may be negligently injured or killed, such as cases involving veterinary malpractice[89] and negligence in driving a vehicle[90] or allowing a potentially dangerous dog to roam freely and harm other animals.[91] In each of these scenarios, the plaintiff loses a pet due to the negligent actions of another, and is forced to suffer the loss without just compensation. Although some states, including California, have allowed the recovery of emotional distress damages based on the intentional injuring or killing of a companion animal, this recovery should similarly apply in cases involving negligent conduct. The bystander and direct victim theories that have been uniformly applied in analyzing claims for negligent infliction of emotional distress should apply to cases involving animals with equal force as with any other type of negligent injury claim. Furthermore, the purpose of awarding compensatory damages is to make the plaintiff whole, and emotional distress damages should therefore be awarded in any case where compensatory damages are required in order to accomplish this purpose, regardless of whether the defendant's conduct was intentional or negligent.

A. Bystander and Direct Victim Theory as Applied to Cases Involving Companion Animals

The bystander theory of liability and direct victim theory of liability can both be applied to cases involving the negligent injury to or death of a companion animal. Due to the close familial relationship that many people develop with their pets, plaintiffs should be entitled to emotional distress damages when

89 *See* McMahon v. Craig, 97 Cal. Rptr. 3d 555, 564 (Ct. App. 2009).
90 *See* Carbasho v. Musulin, 618 S.E.2d 368, 369 (W. Va. 2005).
91 *See* Marshall v. Ranne, 511 S.W.2d 255, 256 (Tex. 1974).

they witness the death of or injury to their pet. Additionally, there are countless situations where persons have a legal duty to behave in a certain way and have breached that duty in causing injury to an animal, subjecting them to liability for emotional distress. Such duties include the duty to control an animal and prevent it from harming another, the duty to act reasonably, and the legal duty of veterinarians to their patients.

1. Bystander Theory

In order to recover for negligent infliction of emotional distress based on the bystander theory, California has consistently held that a plaintiff must establish a direct relationship with the victim, and that "no justification exists for permitting recovery for [negligent infliction of emotional distress] by persons who are only distantly related to the injury victim."[92] More and more frequently, courts are beginning to acknowledge the significant relationship that develops between people and their pets.[93] As such, situations that provide for a remedy when a plaintiff witnesses the negligent injury or death of a family member should likewise apply to the witnessing of the negligent injury or death of a companion animal. In *Rabideau v. City of Racine*, which involved a police officer's shooting of the plaintiff's pet dogs, the Supreme Court of Wisconsin refused to recognize recovery for negligent infliction of emotional distress because of its inapplicability in the context of a "best friend who is human."[94] The court held that "[f]or purposes of recovery for negligent infliction of emotional distress, this court treats the death of a dog the same as it treats injury to or death of a best friend, a roommate, or a nonmarital partner: It allows no recovery."[95] This rationale is without merit because a person's best friend or roommate has a separate family that could recover for witnessing their death or injury. The animal's only "family" in such a situation would be the owner, and disallowing the owner to recover for emotional distress would essentially render the entire doctrine of bystander liability moot in such a situation. If the pet's owner is not permitted to recover damages after witnessing a traumatic accident, the owner's rights will not be vindicated.

---

92 Thing v. La Chusa, 771 P.2d 814, 829 n.10 (Cal. 1989).

93 *See, e.g.*, Ammon v. Welty, 113 S.W.3d 185, 187 (Ky. Ct. App. 2002) ("The affection an owner has for, and receives from, a beloved dog is undeniable.").

94 Rabideau v. City of Racine, 627 N.W.2d 795, 801 (Wis. 2001).

95 *Id.* at 807.

When people adopt a companion animal and welcome the pet into their home, they are manifesting a concrete addition to their family and establishing a relationship that is vastly different than a simple human-to-human friendship. In fact, many believe that a dog's relationship not only rises to the level of human connection, it greatly surpasses that of a human. As Justice Andell of the Texas Court of Appeals for the First District so eloquently stated in his concurring opinion in *Bueckner v. Hamel*, which involved the intentional shooting and killing of the plaintiff's pet Dalmatian and Australian Shepherd, dogs "represent some of the best of human traits, including loyalty, trust, courage, playfulness, and love. This cannot be said of inanimate property. At the same time, dogs typically lack the worst human traits, including avarice, apathy, pettiness, and hatred."[96] Why else are they so often referred to as "man's best friend"?

In determining the availability of civil damages, family members have been afforded similar remedies in the context of other legal claims, such as actions involving wrongful death of a child or spouse. In these cases, like cases involving the death of a pet, a plaintiff may not recover emotional distress damages involving sentimental values such as grief or sorrow.[97] However, in these types of wrongful death actions, courts may award pecuniary damages for the loss of love, companionship, comfort, care assistance, protection, and affection.[98] Due to the fact that California has recognized that dogs have comparable pecuniary value that may be ascertained by reference to the dog's usefulness or other qualities,[99] these pecuniary damages should likewise be available in cases involving the death of an animal. This comparison between the death of a family member and that of a companion animal reflects California's understanding that these beings share many similar qualities and their loss is often accompanied by analogous emotional devastation, thereby indicating that an individual who suffers the loss of a pet should

---

96 Bueckner v. Hamel, 886 S.W.2d 368, 377 (Tex. Ct. App. 1994) (Andell, J., concurring).

97 *See* Quiroz v. Seventh Ave. Ctr., 45 Cal. Rptr. 3d 222, 226–27 (Cal. Ct. App. 2006) ("A plaintiff in a wrongful death action . . . may *not* recover for such things as grief or sorrow attendant upon the death of a loved one, or for his sad emotions, or for the sentimental value of the loss.").

98 JUDICIAL COUNCIL OF CAL., CIVIL JURY INSTRUCTIONS, CACI No. 3921 (2016); *see also* Parsons v. Easton, 195 P. 419, 422 (Cal. 1921) (stating that there may be a pecuniary loss to a parent from the death of a child arising from the deprivation of the comfort and protection of the child).

99 Roos v. Loeser, 183 P. 204, 205 (Cal. Ct. App. 1919).

be afforded similar remedies as a person who suffers the loss of a family member.

In *Bueckner*, the Texas Court of Appeals for the First District specifically acknowledged this unique relationship by noting some of the special characteristics possessed by companion animals.[100] In his concurring opinion, Justice Andell stated: "Because of the characteristics of animals in general and of domestic pets in particular, I consider them to belong to a unique category of 'property' that neither statutory law nor case law has yet recognized."[101] He goes on to suggest:

> The law should reflect society's recognition that animals are sentient and emotive beings . . . . In doing so, courts should not hesitate to acknowledge that a great number of people in this country today treat their pets as family members. Indeed, for many people pets are the *only* family members they have.[102]

He concludes his opinion with the proposition that "testimony that an animal is a beloved companion should generally be considered sufficient to justify a finding of damages well beyond the market value of the animal . . . ."[103]

On a similar note, in his dissenting opinion in *Carbasho*, a 2005 West Virginia Supreme Court decision involving a plaintiff who witnessed the death of her pet dog when he was struck by a negligently driven vehicle, Justice Starcher suggested that the law should be altered to conform with present ideals and values, stating that "[w]hen the common law of the past is no longer in harmony with the institutions or societal conditions of the present, this Court is constitutionally empowered to adjust the common law to current needs."[104] He critiqued the majority's decision by stating that they continue "to maintain the primitive limits of the common law, and refuse[] to adjust to the realities of the modern world, and permit recovery of damages for sentimental value, mental suffering, or emotional distress."[105] It is imperative that courts recognize their obligation to adjust the law to adapt to modern perspectives and societal outlooks. Such conformity requires a change in the way that courts approach issues regarding companion animals, particularly in situations where a plaintiff is forced to witness the injury to or death of a beloved pet.

---

100 *Bueckner*, 886 S.W.2d at 377 (Andell, J., concurring).
101 *Id.*
102 *Id.* at 378.
103 *Id.*
104 Carbasho v. Musulin, 618 S.E.2d 368, 372 (W. Va. 2005) (Starcher, J., dissenting).
105 *Id.*

2. Direct Victim Theory

In terms of the direct victim theory of liability, although the California Supreme Court has implied that a plaintiff may not be able to recover emotional distress damages for the negligent injury of an animal simply because there is no duty that exists in such a scenario,[106] there are numerous cases where such a duty does exist and is breached when the animal has been injured. For example, in *Marshall v. Ranne*, a case involving a boar owned by the defendant who attacked and injured the plaintiff, the Texas Supreme Court stated that "a possessor of a non-vicious animal may be subjected to liability for his negligent handling of such an animal," suggesting that a person has a duty to prevent a pet from injuring another person, pet, or property.[107] Moreover, the California Supreme Court has repeatedly held that it is a general rule of negligence that "every person has a duty to refrain from acting in a manner that causes foreseeable injury to another."[108] Therefore, any situation in which a person is not acting as a reasonably prudent person otherwise would act, such as negligently operating a vehicle and striking a dog in the road, would subject that person to liability for negligence. In these cases, emotional distress damages would be required in order to fully compensate plaintiffs for their losses.

Additionally, there exists a duty in veterinary malpractice cases that could subject a veterinarian to liability for emotional distress damages resulting from negligent conduct. In fact, the vast majority of cases involving negligent injury to a companion animal involve claims of veterinary malpractice.[109] In medical malpractice lawsuits, the duty of care that a physician owes patients has traditionally been defined as the standard of "learning, skill and ability which others similarly situated ordinarily possess."[110] Courts have further elaborated on this standard by defining "similarly situated" as "a standard of professional competence and care customary in the field of practice among practitioners in similar communities."[111] While some states are in conflict regarding whether the same standard

106 Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 807 (Cal. 1993) ("[T]here is no duty to avoid negligently causing emotional distress to another, and . . . damages for emotional distress are recoverable only if the defendant has breached some other duty . . . .").

107 Marshall v. Ranne, 511 S.W.2d 255, 259 (Tex. 1974).

108 Parsons v. Crown Disposal Co., 936 P.2d 70, 95 (Cal. 1997).

109 WAGMAN ET AL., *supra* note 23, at 215.

110 *Id.* at 219.

111 Williams v. Reynolds, 263 S.E.2d 853, 855 (N.C. Ct. App. 1980).

should be applied to veterinarians,[112] California courts have unanimously found that the medical malpractice standard applies to veterinary malpractice cases.[113] In doing so, courts have looked to California statutes such as the California Business & Professions Code, which categorizes both medical doctors and veterinarians as licensed health care providers, and the California Code of Civil Procedure, which treats both types of cases the same for statute of limitations purposes.[114] Thus, it is clear that a duty exists in veterinary malpractice cases, and when a veterinarian breaches this duty through negligent conduct, he or she should be liable for emotional distress damages to the aggrieved plaintiff under the direct victim theory of liability.

B. Emotional Distress Damages Serve to Make a Plaintiff Whole

As a form of compensatory damages, emotional distress damages are awarded to compensate plaintiffs for any injury that has wrongfully been inflicted upon them. In determining the amount of damages to be awarded, the court must look at the extent of the injury to the plaintiff as a result of the defendant's conduct. This is distinguishable from punitive damages, where the court must look at the defendant's conduct and determine whether the conduct is so reprehensible as to warrant additional damages for the purpose of punishing or deterring the defendant. Accordingly, in cases where the court has considered emotional distress damages based on the intentional injury to a pet, the court focuses on the effect that the injury or death has had on the plaintiff and the hardship that often accompanies such a loss.[115] Due to the fact that courts place such a strong emphasis on the effect of the action on plaintiffs, there should be no distinction

---

112 *Compare* Gillette v. Tucker, 65 N.E. 865, 869 (Ohio 1902) (adopting a similar malpractice analysis for all doctors, regardless of species), *with* Pruitt v. Box, 984 S.W.2d 709, 711 (Tex. Ct. App. 1998) (holding that the standard applicable to medical malpractice should not be applied to veterinary malpractice cases).

113 *See* Williamson v. Prida, 89 Cal. Rptr. 2d 868, 872 (Ct. App. 1999) (holding that the medical malpractice standard applies to veterinary malpractice cases).

114 CAL. BUS. & PROF. CODE § 4800 (West 2016); CAL. CIV. PROC. CODE § 340.5 (West 2016); CIV. PROC. § 597.5; *see also Williamson*, 89 Cal. Rptr. 2d at 872 (relying on the California Business and Professional Code and Civil Procedure Code in holding that veterinarians and physicians are treated the same).

115 *See* Richardson v. Fairbanks N. Star Borough, 705 P.2d 454, 456 (Alaska 1985) ("[T]he loss of a beloved pet can be especially distressing in egregious situations."); La Porte v. Associated Indeps., Inc., 163 So. 2d 267, 269 (Fla. 1964) ("[T]he affection of a master for his dog is a very real thing and . . . the malicious destruction of the pet provides an element of damage for which the owner should recover."); Womack v. Von Rardon, 135 P.3d 542, 546 (Wash. Ct. App. 2006) ("[H]arm may be caused to a person's emotional well-being by malicious injury to that person's pet as personal property.").

between intentional or negligent conduct by the defendant. In either situation, the plaintiff is forced to endure the loss or injury to a pet, and the way in which this injury has occurred should be irrelevant. Of course, it would make no logical sense to award punitive damages for negligent conduct, but emotional distress damages serve a different purpose. Without emotional distress damages in situations where a plaintiff's pet has been negligently harmed, the plaintiff is not provided an adequate remedy. The focus in these cases must be on the plaintiff's recovery, not the defendant's conduct.

It is generally thought that courts are reluctant to extend compensatory damages to include those for emotional distress for two primary reasons. First, emotional distress damages are inherently difficult to prove or measure, and second, opening the door to these types of emotional distress claims would invite a floodgate of trivial or fictitious litigation.[116] Some scholars have further argued that emotional distress damages are so unique to each individual that such damages are unforeseeable, and as such, the defendant should not be held liable for injuries of this sort.[117] While it is certainly true that measuring emotional distress damages is not a simple task involving a predetermined formula, courts have uniformly permitted plaintiffs to recover emotional distress damages in other contexts.[118] In fact, though limited in its application, the separate cause of action for intentional infliction of emotional distress has been consistently recognized throughout the country. If courts are willing to permit such recovery in these various situations, there should be no reason to prevent recovery in the context involving the negligent treatment of animals. The measure of pain and suffering experienced by the plaintiff is still going to be a subjective test based upon the plaintiff's reaction to the defendant's unlawful conduct, and the underlying context therefore has no relevance. Moreover, advances in medicine and science now allow for a better attempt at measuring emotional distress damages to determine with higher certainty the severity of such damages. For example, expert testimony may be used to prove emotional distress damages, such as long-term emotional trauma related to

---

116 Wise, *supra* note 7, at 50.

117 *Id.*

118 *See, e.g.*, Johnson v. Thigpen, 788 So. 2d 410, 412 (Fla. Dist. Ct. App. 2001) (allowing emotional distress damages in case involving workplace harassment); Carey v. Lovett, 622 A.2d 1279, 1294 (N.J. 1993) (awarding emotional distress damages to parents in medical malpractice claim involving birth of daughter); Kennedy v. McKesson Co., 448 N.E.2d 1332, 1344 (N.Y. 1983) (recognizing availability of emotional distress damages in case involving dental malpractice).

the defendant's conduct.[119] The issue of foreseeability is also moot because medical science now recognizes that "in many situations, a plethora of mental damages, including fright, shock, grief, and anxiety, are foreseeable."[120]

Furthermore, the simple fear that allowing plaintiffs to recover emotional distress damages will result in a "Pandora's box" of litigation is not sufficient to prevent the award of non-economic damages altogether. The current state of the law disallowing emotional distress damages in situations involving intentional or negligent injury to or death of an animal is severely underinclusive and must be better adapted to provide sufficient remedies for plaintiffs in these situations. It is underinclusive in that countless claims involving obvious and severe emotional distress have gone uncompensated and are barred from recovery under this general rule, despite the clear need for an additional remedy in order to make the plaintiff whole.[121] It is one of the general duties of the judiciary to distinguish meritorious claims from frivolous ones, and a law preventing the meritorious claims from being heard is significantly more detrimental than the minimal burden of weeding out those that lack merit.

CONCLUSION

The relationship between humans and companion animals has been undergoing tremendous development in recent history. Although animals continue to be characterized as the personal property of humans, the judicial and legislative branches have become increasingly aware of the unique bond that is commonly formed in such a relationship, and as a result, have altered the way they have approached such situations to a limited extent. California in particular has taken significant steps in recognizing the importance of adjusting the way the law treats nonhuman animals and their human counterparts, such as allowing an owner to recover emotional distress damages when a pet has been intentionally injured or killed. This significant decision was a major breakthrough in the California legal system, which has historically limited the available damages in such cases to

---

119 JON R. ABELE, EMOTIONAL DISTRESS: PROVING DAMAGES 110 (2003).

120 Wise, *supra* note 7, at 51.

121 *Id.*; *see, e.g.*, Burgess v. Taylor, 44 S.W.3d 806, 812 (Ky. Ct. App. 2001) (finding that plaintiff suffered severe emotional distress but refusing to award emotional distress damages); Daughen v. Fox, 539 A.2d 858, 862 (Pa. Super. Ct. 1988) (denying emotional distress damages award despite plaintiffs' severe emotional distress resulting in the death of one of the plaintiffs).

economic damages. Nevertheless, the judiciary has failed to keep pace with this evolving trend, and it is insufficient to end the transition here, as this remedy does not take into account those plaintiffs who have suffered the loss of a pet as a result of the negligent actions of another. Regardless of whether the pet has been harmed by another's intentional or negligent actions, the owner nonetheless must bear the loss, and as such, should be afforded similar treatment when seeking a remedy.

Without sufficient compensation for the death or injury to a companion animal in cases involving negligent conduct, plaintiffs are being denied proper compensation and are never truly made whole. It is an unfortunate tragedy that when a plaintiff suffers the loss of a pet, that individual "has no remedy for . . . grief and emotional distress in our common law."[122] By allowing plaintiffs to recover emotional distress damages in situations where their pet has been negligently killed or injured, California will be one step closer to conforming the law to modern societal values. Whether the allowance of emotional distress damages should be permitted in claims involving damage to personal property, incorporated into the concepts of direct victim liability or bystander liability, or based upon an entirely separate cause of action, this is a change that must take place in order to provide pet owners with sufficient compensation under the law. To illustrate the strong emotional bond that exists between a man and his dog, Justice Starcher concluded his dissenting opinion in *Carbasho* by quoting an old country song entitled "Old Shep."

When I was a lad
And old Shep was a pup
Over hills and meadows we'd stray
Just a boy and his dog
We were both full of fun
We grew up together that way.
I remember the time at the old swimmin' hole
When I would have drowned beyond doubt
But old Shep was right there
To the rescue he came
He jumped in and then pulled me out.
As the years fast did roll
Old Shep he grew old
His eyes were fast growing dim
And one day the doctor looked at me and said
I can do no more for him Jim.
With hands that were trembling
I picked up my gun
And aimed it at Shep's faithful head
I just couldn't do it
I wanted to run
I wish they would shoot me instead.
He came to my side
And looked up at me
And laid his old head on my knee
I had struck the best friend that man [ever had
I cried so I scarcely could see.
Old Shep he has gone
Where the good doggies go
And no more with old Shep will I roam
But if dogs have a heaven
There's one thing I know
Old Shep has a wonderful home.[123]

122 Carbasho v. Musulin, 618 S.E.2d 368, 373 (W. Va. 2005) (Starcher, J., dissenting).
123 *Id.* at 372–73.

The *Chapman Law Review* is published by its student members at Chapman University Dale E. Fowler School of Law The *Chapman Law Review* can be reached by phone at (714) 628-2582, online at www chapmanlawreview com, or by e-mail at chapmanlawreviewonline@gmail.com. The office of the *Chapman Law Review* is located in Donald P Kennedy Hall on the campus of Chapman University, One University Drive, Orange, CA 92866.

Subscriptions to the *Chapman Law Review* are $24.00 per year. The price is subject to change without notice. Please mail payment to the above address. Telephone orders are also accepted with a valid Visa or MasterCard. Institutional subscriptions are renewed automatically, unless otherwise notified. Address changes or other requests should be directed to the Production Editor.