Chapman Law Review

CHAPMAN UNIVERSITY ADMINISTRATION

MATTHEW PARLOW
President

JESSICA BERGER
Executive Vice President and Chief Advancement Officer

MICHAEL IBBA, PH.D.
Executive Vice President, Provost, and Chief Academic Officer

AMY ROGAN-MEHTA, ESQ.
Executive Vice President and Chief of Staff

BRIAN THOMPSON
Interim Executive Vice President and Chief Operating Officer

JANNA BERSI, ED.D.
Chief Investment Officer

RICK BISCHOFF
Senior Vice President of Enrollment Management

GABRIELA CASTAÑEDA, ED.D.
Vice President of First-Generation and Promising Futures Program

COLLETTE CREPPELL
Vice President of Campus Planning and Design

PHILLIP LYLE
Interim Vice President and Chief Information Officer

MARTINA NIESWANDT, PH.D.
Vice President of Research

JERRY PRICE, PH.D.
Senior Vice President for Student Affairs and Dean of Students

VALERIE REIF
Interim Chief Human Resources Officer

HIMA VATTI
General Counsel

NIDHI VOGT
Vice President and Deputy Chief of Staff

MARIE WILLIAMS
Senior Vice President of Marketing and Public Affairs

BOARD OF TRUSTEES

JAMES P. BURRA, *Chair*
JAMES V. MAZZO, *Vice Chair*
SCOTT CHAPMAN, *Secretary*
MARILYN ALEXANDER
LISA ARGYROS ‘07
GAYE BIRTCHER
KEN BUNT ‘93
ROBERT CASE
AKIN CEYLAN ‘90
IRVING M. CHASE
JEROME W. CWIERTNIA
ZEINAB DABBAH (JD ‘12)
DALE E. FOWLER ‘58
GAVIN S. HERBERT, JR.
MARK HILBERT
ANDY HOROWITZ
ANDRÉS IRLANDO
MARK CHAPIN JOHNSON ‘05
JASON KROTTS ‘00
DANIELLE LIMP
RICK LOWE
MELINDA MASSON
MARONYA MOULTRIE
MARYBELLE MUSCO
RICHARD MUTH (MBA ‘81)
NELLA WEBSTER O’GRADY ‘71
JAMES B. ROSZAK
THE HONORABLE LORETTA SANCHEZ ‘82
KEVIN SCHEETZ
RONALD M. SIMON
MAX VALDES
TIM VANDERHOOK
THE HONORABLE GADDI H. VASQUEZ ‘09
ANNETTE WALKER
GEORGE WALL
KAREN R. WILKINSON ‘69
JANE FUJISHIGE YADA
CHARLIE ZHANG

EMERITUS CHAIRS

WYLIE A. AITKEN
THE HONORABLE GEORGE L. ARGYROS ‘59
DOY B. HENLEY
PARKER S. KENNEDY
DONALD E. SODARO

EMERITUS TRUSTEES

DONNA FORD ATTALLAH ‘61
ARLENE R. CRAIG
DAVID C. HENLEY
ROGER C. HOBBS
WILLIAM K. HOOD
JOANN LEATHERBY
TOM MALLOY
RICHARD R. SCHMID
R. DAVID THRESHIE

EX-OFFICIO TRUSTEES

ADRIENNE BRANDES (M.A. ’84)
REVEREND LATAUNYA BYNUM ’76
REVEREND JAY HARTLEY
REVEREND DAYNA KINKADE
MICHAEL PENN (JD ’04)
MICHELE PHILO ‘03
REVEREND RACHAEL PRYOR
REVEREND RICHIE SANCHEZ
SUSIE WILLITS ‘71

BOARD OF ADVISORS

KENNETH A. STAHL
THOMAS D. PHELPS, *Chair*
WYLIE A. AITKEN
ROBERT ALVARADO
JOHN R. EVANS
WOLFGANG FRISCH ‘97 (JD ‘00)
THE HONORABLE ANDREW J. GUILFORD
JANET E. HUMPHREY
PARKER S. KENNEDY
THE HONORABLE LAYNE H. MELZER
DAVID MURPHY

SCHOOL OF LAW ADMINISTRATION

KENNETH STAHL
Interim Dean

RICHARD E. REDDING
Associate Dean for Academic Affairs

DEEPA BADRINARAYANA
Associate Dean for Research and Faculty Development

MARIO MAINERO
Associate Dean for Governance and Strategic Initiatives & Bar Preparation and Academic Standards

JUSTIN CRUZ
Associate Dean of Admission and Diversity Initiatives

SARIRA A. SADEGHI
Sam & Ash Assistant Dean for Academic Achievement

MARYAM ISLES
Assistant Dean for Academic Services and Registration

CAMILLE HEENAN
Assistant Dean for Career Services

JESSICA JOHN, ESQ.
Assistant Dean for Student Affairs

KELLY OTO, MA'11
Assistant Dean for Administration

LAW SCHOOL FACULTY

DR. DEEPA BADRINARAYANA
Professor of Law
Associate Dean for Research and Faculty Development

MICHAEL BAZYLER
Professor of Law
1939 Society Law Scholar in Holocaust and Human Rights Studies

SEAN BIGLEY
Visiting Associate Professor of Law

TOM W. BELL
Professor Emeritus

DR. DENIS BINDER
Professor of Law

JOHN BISHOP
Associate Professor of Legal Practice

DANIEL BOGART
Professor of Law
Bolinger Chair in Real Estate, Land Use and Environmental Law

DR. TOM CAMPBELL
Professor of Law
Doy and Dee Henley Distinguished Professor of Jurisprudence
Former Dean (2011–2016)

LAN CAO
Professor of Law
Betty Hutton Williams Professor of International Economic Law

JENNY CAREY
Professor of Legal Research and Writing

TINA CHING
Director of Hugh & Hazel Darling Law Library

MARISA S. CIANCIARULO
Professor of Law

BOBBY DEXTER
Professor of Law

KURT EGGERT
Professor of Law
Director of the Alona Cortese Elder Law Center

GEORGE "JUDD" FUNK
Professor of the Practice of Entertainment Law

DR. JOHN HALL
Professor of Law

ERNESTO HERNÁNDEZ-LÓPEZ
Professor of Law

HUGH HEWITT
Professor of Law

SCOTT HOWE
Professor of Law
Frank L. Williams Professor of Criminal Law
Former Interim Dean (2010–2011, 2016)

NAHAL KAZEMI
Assistant Professor of Law

JANINE KIM
Wylie A. Aitken Professor of Law, Race, and Social Justice

CAROLYN YOUNG LARMORE
Professor of the Practice of Law
Director of the Externship Program

STEPHANIE LASCELLES
Associate Professor of Legal Research and Writing

MARIO MAINERO
Professor of Academic Achievement and Bar Services
The Gray Family Professor of Law
Associate Dean for Bar Preparation and Academic Achievement

CELESTINE MCCONVILLE
Professor of Law
Henry Salvatori Professor of Law and Community Service

HENRY NOYES
Professor of Law

MATTHEW PARLOW
Professor of Law
President
Donald Bren Presidential Chair in Law

DR. PAUL PATON
Donald P. Kennedy Chair in Law
Professor of Law and Ethics

ABIGAIL PATTHOFF
Professor of Legal Research and Writing

DR. RICHARD REDDING
Professor of Psychology and Education
Ronald D. Rotunda Distinguished Professor of Jurisprudence
Associate Dean for Academic Affairs

SUSANNA RIPKEN
Professor of Law
William P. Foley II Chair in Corporate Law and Taxation

LAWRENCE ROSENTHAL
Professor of Law

MARY-LEE RYAN
Professor of the Practice of Entertainment Law and Entertainment Law Clinic

DR. VERNON SMITH
George L. Argyros Endowed Chair in Finance and Economics
Professor of Economics and Law

KENNETH STAHL
Interim Dean
Professor of Law
Director of the Environmental Land Use and Real Estate Law Program

DR. WILLIAM STALLWORTH
Professor Emeritus of Law

DR. RIAZ TEJANI
Visiting Professor of Law

KIM TYLER
Visiting Professor of the Practice of Entertainment Law

MATTHEW TYMANN
Assistant Professor of the Practice of Legal Research and Writing

PARHAM WILLIAMS
Dean Emeritus of Law
Former Dean (1997–2007)

GEORGE WILLIS
Professor of Law
Clinical Faculty Director of the Tax Law Clinic

BART WILSON
Professor of Law
Donald P. Kennedy Chair in Economics and Law Director, Smith Institute for Political Economy and Philosophy

Chapman Law Review

Volume 29 Symposium Issue Number 3

KEYNOTE ADDRESS

ARTICLES

Editor's Note

Chapman Law Review closes out Volume 29 with the Symposium Issue. This is the third and final issue published by Volume 29, following General Issue One and General Issue Two. This issue features scholarship on data privacy and supplements the *Chapman Law Review* symposium, Data Flow Frontiers: Privacy, Policy & Practice, which took place on Friday, February 6, 2026, in a sold-out Kennedy Hall in Orange, CA. The symposium was an engaging discussion on modern data privacy.

Panel One, titled "The Social Contract: Terms, Conditions & Privacy," explored social media companies and how their terms of service and data practices affect users. The panel focused on how much privacy users give up for free platforms, along with issues like AI, children's data, and the TikTok ban, highlighting the balance between user choice, transparency, and how companies use personal information. The panelists were Professor Jon M. Garon of Nova Southeastern University Shepard Broad College of Law, Lily Li of Metaverse Law, and Nancy Libin of Davis Wright Tremaine, moderated by Nahal Kazemi of Chapman University Dale E. Fowler School of Law.

Panel Two, titled "Privacy in Flux: The International Digital Divide," explored how the United States and the European Union take different approaches to data privacy and how those differences shape the way personal information is regulated. The panel focused on the trade-offs between innovation and stronger privacy protections, as well as broader issues like AI, cross-border data flows, and the global influence of digital platforms, highlighting the challenges of balancing privacy, accountability, and technological growth in an interconnected world. The panelists were Professor Gregory S. McNeal of Pepperdine University Caruso School of Law, Gretchen Ramos of Greenberg Traurig, LLP, and Professor John M. Yun of George Mason University Antonin Scalia School of Law, moderated by Professor Mason R. Clark of St. Mary's University School of Law.

The keynote address was delivered by the distinguished Professor Paul M. Schwartz of UC Berkeley School of Law to immense praise. Professor Schwartz transformed his address into the article published in this Issue, both titled *Data Privacy Federalism 3.0*. Professor Schwartz explains that states are taking the lead by passing new privacy laws while Congress has largely failed to act, raising new questions about how federal and state laws should work together. He also highlights growing conflicts over the federal government accessing state-held personal data and argues

that constitutional limits should protect that information. Schwartz concludes that the future of federalism depends on how federal and state governments share data.

Next, Professor Mason R. Clark argues that current privacy laws do not do enough to protect children online and place too much responsibility on parents to manage complex data practices. In *It Takes a Village (To Raise Children's Privacy)*, Clark explains that content-based systems often fail because parents lack the time, knowledge, and tools to make informed decisions, while companies continue to collect and use large amounts of children's data. Clark proposes a reworked pay-for-privacy model that would give parents clear, regular reports about their child's data and simple tools to control it, combined with strong oversight to ensure fairness and accountability.

Dean Jon M. Garon argues that new technology—especially social media and AI—has changed how information is created and shared, making it harder for traditional ideas about free speech and the "marketplace of ideas" to work as intended. In *Promoting and Protecting the Marketplace of Ideas in the AI Information Age*, Garon explains that the shift away from traditional media has weakened gatekeepers and made it more difficult to sort truth from noise. He concludes that while free speech remains important, the law may need to adjust to better balance innovation, public protection, and today's digital reality.

Finally, Professor Gregory S. McNeal explains that the GDPR and the CCPA are often treated as similar, but they take very different approaches to data privacy. In *The Compliance Stack*, McNeal shows that the GDPR treats privacy as a fundamental right and requires companies to justify data use upfront, while the CCPA focuses on consumer protection by requiring transparency and giving users control after the fact. He also highlights major differences in areas like cross-border data transfers and enforcement. McNeal ultimately concludes that these frameworks serve different goals and cannot be treated as interchangeable in practice.

The 2026 *Chapman Law Review* Symposium was a tremendous success thanks to the people behind the scenes who worked so hard to create an important and memorable event. Executive Program Editor Riya Beri worked tirelessly to invite speakers, coordinate the logistics, and develop the marketing that led to a sold-out event. The administration, namely interim Dean Kenneth Stahl, Deane Sutic, Aaron Rodriguez, Jonathan Smith, Assistant Dean Kelly Oto, and Assistant Dean Jessica John provided crucial support and guidance throughout the process. The faculty,

especially Professors Celestine McConville, Lan Cao, Mario Mainero, and Lawrence Rosenthal, and law librarian Phillip der Mugrdechian contributed vital support and advice.

When we kicked off Volume 29, our goal was simple: we wanted to leave the Journal better than we found it. Previous iterations of *Chapman Law Review* paved the way for us and allowed us to build on the strong foundation they had built. Our article submissions team implemented processes to increase our reach and profile. Our editing team improved our procedures and demonstrated meticulous attention to detail. Our production team emphasized communication and prioritized our authors. Our symposium amplified a cutting-edge topic and introduced creative marketing initiatives. In all, I believe we left the Journal better than we found it.

To the members of *Chapman Law Review*, thank you for your hard work, dedication, and positivity throughout the year. Without each member's crucial contributions, the three issues and the symposium would not have been possible. Volume 29 published crucial pieces that will only become more important as the years go by. Volume 30 is in excellent hands, and I cannot wait to see the continued growth of *Chapman Law Review*. It has been the honor of a lifetime to serve as Editor-in-Chief and I am forever indebted to the individuals who made the experience so special. Thank you.

Jack Mays
Editor-in-Chief

Data Privacy Federalism 3.0

Paul M. Schwartz

CONTENTS

Data Privacy Federalism 3.0

*Paul M. Schwartz**

Federalism is a bedrock concept in the political organization of the United States. It is also a topic of intensive scholarly attention. Yet, compared to other areas of federalism, questions concerning personal data have received little notice. This Article's analysis of data privacy federalism is organized around two topics: preemption (Data Privacy Federalism 1.0) and anti-commandeering (Data Privacy Federalism 2.0). It argues that recent developments have dramatically changed the landscape for preemption and federal-state data sharing, resulting in Data Federalism 3.0.

In Data Federalism 3.0, a number of developments have dramatically altered the past landscape for preemption. First, there has been an explosion of omnibus state privacy statutes. Second, there is a continuing lack of a federal omnibus privacy law and an almost complete absence of congressional privacy lawmaking at the sectoral level. This Article advocates for continuing state lawmaking on privacy matters and does so on federalism grounds. State lawmaking about data privacy is supported by the classic Brandeisian notion of the states as laboratories for innovative policymaking. In addition, there is the potential of states to serve as catalysts for bipartisan policy cooperation.

There have also been important recent developments concerning the sharing of personal data among different levels of government. These changes significantly implicate the anti-commandeering doctrine. Data-driven unilateral actions by the Trump administration toward the states represent "agonistic federalism," to use a term recently coined by Professors Aziz Huq and Zachary Clopton. The executive branch has engaged in a hostile attack on the states by weaponizing personal data collected through federal-state programs. In response, this Article proposes that anti-commandeering provisions should extend to personal information. The states should develop this constitutional doctrine as part of their opposition to the Trump administration's seizures of personal data. This Article's main lesson is that the future of federalism depends on the rules for personal data sharing among the federal and state governments.

---

* Jefferson E. Peyser Professor of Law. This Article was presented on February 6, 2026, as the Keynote Address at the *Chapman Law Review*'s symposium, Data Flow Frontiers. My thanks to Brianna Gerth and Jack Mays of the *Chapman Law Review* for their expert assistance and to symposium participants for their helpful remarks. Many thanks as well to my research assistants Nadia Orchid Ghaffari, Aaniyah Hicks, and Allen Park. Thanks as well to Doug Avilla and I-Wei Wang of the Berkeley Law Library. Finally, I am grateful to Professor Aziz Huq and Dean Erwin Chemerinsky for their helpful comments.

I. INTRODUCTION

Federalism is a bedrock concept in the political organization of the United States. As the Supreme Court has held, "[i]t is incontest[able] that the Constitution established a system of 'dual sovereignty.'"[1] While the states surrendered many of their powers to the federal government at the founding, they retained explicit and implicit sovereignty under the Constitution. Federalism is also a topic of intensive scholarly attention. Yet, compared to other areas of federalism, questions concerning personal data have received little notice.

An analysis of data privacy federalism can be structured around two topics. First, there is the issue of preemption. Data Privacy Federalism 1.0 considers the extent to which federal law should preempt state law in regulating the use of personal data by private companies. Should data privacy issues involving the private sector be regulated by the federal government, or by state governments? Should this power be shared and, if so, how? These questions have been present from the enactment of the first federal data privacy law in 1970.[2]

Second, there is the matter of the terms and conditions under which federal and state governments share personal data with each other. A central issue in Data Privacy Federalism 2.0 is the extent to which the Constitution limits the authority of the federal government to access state data. Under the anti-commandeering principle, neither Congress nor the executive branch can "command" state and local officials in certain ways.[3] Yet, the Supreme Court has never decided whether the core federalism principle of anti-commandeering applies to personal data. The question remains open as to whether there is an "information sharing exception" to federalism.[4]

Recent political developments have dramatically changed the landscape for preemption and federal-state data sharing. The result is Data Federalism 3.0. This Article explores the altered outlook for these aspects of federalism. It advocates for continuing

---

1 Printz v. United States, 521 U.S. 898, 918 (1997) (quoting Gregory v. Ashcroft, 501 U.S. 452, 457 (1991)).

2 For an introduction to preemption issues present in data privacy law, see generally Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).

3 For an introduction, see *Amdt10.4.2 Anti-Commandeering Doctrine*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt10-4-2/ALDE_00013627/ [https://perma.cc/59BC-ZNYS] (last visited Mar. 25, 2026).

4 Bridget A. Fahey, *Data Federalism*, 135 HARV. L. REV. 1007, 1026 (2022).

state enactment of data privacy legislation and calls for development of anti-commandeering principles to guard against the ongoing data grabs of the executive branch. These actions by the federal government have changed the past terms of data sharing for a variety of vitally important federal-state programs, including Medicaid and the Supplemental Nutrition Assistance Program (SNAP).[5]

Before this Article turns to data privacy federalism, an introduction to the basics of data privacy law and federalism would be helpful. Data privacy law defines rules for personal data processing by organizations and individuals.[6] As a normative matter, data privacy serves an essential role in promoting individual autonomy and democracy.[7] Yet, the collection, processing, and transfer of personal data are also essential. These activities can promote economic development, assist law enforcement, safeguard national security, and further other important policy goals.

As for federalism, it distributes power among a central government and subdivisional governments. Federalism considers which powers should belong to the national authority, which to the states and localities, and which are to be shared.[8] Like data privacy, which seeks to establish appropriate tradeoffs among different policy goals, federalism does not seek to maximize the authority of a single level of government but instead seeks to assign governmental authority among dual sovereigns. This Article's main lesson is that the future of federalism depends on the rules for personal data sharing among the federal and state governments.

II. DATA PRIVACY FEDERALISM 1.0: PREEMPTION

Data Privacy Federalism 1.0 is about the division of power among different levels of government when regulating private sector data use. The first federal data privacy law in the United

---

5 *See, e.g.*, Jude Joffe-Block, *At Least 27 States Turned Over Sensitive Data About Food Stamp Recipients to USDA*, NPR (Oct. 16, 2025, at 12:55 ET), https://www.npr.org/2025/10/16/nx-s1-5533045/snap-privacy-usda-lawsuit [https://perma.cc/4N6N-J6KX].

6 DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 2 (8th ed. 2024).

7 *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613–14 (1999); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709–10 (1987).

8 For an overview of federalism scholarship, see Jessica Bulman-Pozen, *From Sovereignty and Process to Administration and Politics: The Afterlife of American Federalism*, 123 YALE L.J. 1920, 1924–27 (2014).

States, the Fair Credit Reporting Act (FCRA) (1970), contains a strong preemption clause. From the start, the FCRA preempted state laws "to the extent that those laws are inconsistent with any provision of [it]."[9] Congress has also modified the contours of the FCRA preemption several times in the more than half-century since its enactment.[10] In 1996, for example, Congress expanded the FCRA's preemption of state laws inconsistent with any provision of the FCRA. The 1996 amendment to the statute explicitly references "any State regulation related to specifically enumerated subjects already regulated by the FCRA."[11] Enumerated subjects in this law include the prescreening of consumer reports, the duties of a person who takes adverse action in respect to a consumer, and the information available to victims of identity theft.[12]

As this example demonstrates, preemption has long been a moving target for data privacy federalism. It is also a vitally important doctrine because of how the United States regulates this area. Unlike the rest of the world, the United States lacks a so-called omnibus or general national data protection law.[13] Almost all other countries have enacted such a national law, and the European Union itself has taken this approach at a supranational level.[14] Its General Data Protection Regulation is one of the most influential privacy regulations in the world.[15] In the United States, in contrast, Congress has traditionally proceeded through the enactment of sectoral laws, that is, laws that regulate only a specific area of personal data use.[16]

The number of federal sectoral laws is extensive, but there are also notable gaps remaining. Federal data privacy statutes include the FCRA (1970), the Family Educational Rights and Privacy Act (1974), the Driver's Privacy Protection Act (DPPA) (1994), the Electronic Communications Privacy Act

---

9 15 U.S.C. § 1681t(a).

10 As the Consumer Financial Protection Bureau summarizes regarding the FCRA in a 2025 interpretative rule, "the scope of that preemption has changed over time." Fair Credit Reporting Act; Preemption of State Laws, 90 Fed. Reg. No. 48710, 48710–11 (Oct. 28, 2025) (to be codified at 12 C.F.R. pt. 1022).

11 For a discussion, see *id.* at 48711–12.

12 *See id.*

13 SOLOVE & SCHWARTZ, *supra* note 6, at 1056–57.

14 *See id.* at 1056.

15 *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 772 (2019).

16 STEPHEN P. MULLIGAN, WILSON C. FREEMAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., DATA PROTECTION LAW: AN OVERVIEW 7 n.60 (2019).

(1986), the Video Privacy Protection Act (VPPA) (1988), the Health Insurance Portability and Accountability Act (HIPAA) (1996), the Children's Online Privacy Protection Act (COPPA) (1998), and the Gramm-Leach-Bliley Act (1999). The jurisdictional reach of these laws rests on the congressional vision at the time of enactment, including its understanding of the critical technology of that day. To illustrate, the FCRA's reach rests on the concept of a "consumer reporting agency," a settled idea in 1970, but an area of commerce with more fluid borders today.[17] The nearly forty-year-old VPPA's meaning in the twenty-first century turns on judicial interpretations of several key statutory terms, including "video tape service provider."[18]

In addressing the extent to which federal and state data privacy laws should or should not co-exist, Congress has developed a variety of solutions. These approaches to data preemption are important because many state sectoral laws occupy the same or similar terrain as federal statutes. For example, the leading federal health care privacy regulation is HIPAA's Privacy Rule, which explicitly permits stricter state laws.[19] HIPAA sets a floor for protection of individuals. But to complicate matters, HIPAA also preempts any state law that is "contrary" to it.[20] A contrary state law is one that makes it impossible to comply with both HIPAA and state law. There is ample case law analyzing whether a state health privacy law is more protective of patients, or is, in fact, contrary to the federal regulation.[21]

Another set of issues is raised when state sectoral privacy laws are enacted *before* a federal law aimed at a similar area of personal data use. For example, there are no federal biometric statutes, but states, including Colorado, Texas, Illinois, and Ore-

---

17 *See* Fair Credit Reporting Act, 15 U.S.C. § 1681a(f). To illustrate, Spokeo, the operator of a "people search engine" and not a traditional "credit reporting agency," was engaging in activities that fell under the FCRA's scope. Spokeo, Inc. v. Robins, 578 U.S. 330, 333–36 (2016).

18 18 U.S.C. § 2710(a)(4); *see, e.g.*, Osheske v. Silver Cinemas Acquisition Co., 132 F.4th 1110, 1111 (9th Cir. 2025) (noting that "a classic in-theater movie-going experience is [not] subject to the Video Privacy Protection Act," even if its website shows trailers for films).

19 45 C.F.R. § 160.203(b) (2026).

20 *Id.* § 160.202.

21 *See, e.g.*, Ledford v. UofL Health-Louisville, Inc., 720 S.W.3d 594, 601 (Ky. Ct. App. 2025) ("State laws that are not contrary to HIPAA are not preempted. If, and only if, a state law is contrary to HIPAA must a court then consider whether the state law is more stringent."); Washington v. Alderwood Surgical Ctr., LLC, No. C22-1835-RSM, 2023 WL 6461145, at *3 (W.D. Wash. Oct. 4, 2023) (noting that "since Washington state law is more stringent than HIPAA, the [Uniform Healthcare Information Act] preempts the federal procedure").

gon, have passed such laws.[22] The Illinois Biometric Information Privacy Act (BIPA) (2008) is the most important of these statutes, at least judging from the amount of litigation and high monetary settlements that it has generated.[23] Should the federal government express interest in enacting a federal biometric statute, these states, as first-movers, will likely oppose any congressional enactment that would water down their own laws.

Fortunately, preemption under Data Privacy Federalism 1.0 has never been an all-or-nothing matter. As noted above, Congress has an impressive toolkit for setting the terms of the interplay between federal and state laws. These include subject matter preemption; the creation of ceilings and floors in federal legislation; the limitation of a ceiling or floor only to "conduct" regulated; sunset provisions (which re-open federal-state negotiations after a set period); and the sharing of enforcement authority.[24] As we have seen, the FCRA demonstrates that federal preemption choices can change over time through congressional amendment of laws. The FCRA has made use of a sunset provision, which permitted a re-opening of federal-state negotiations in 2003.[25] With the enactment that year of the Fair and Accurate Credit Transactions Act, an amendment to the FCRA, Congress removed any sunsets from the FCRA.[26]

The results of Data Federalism 1.0 have also sometimes been uncomplicated. As an example, COPPA permits enforcement of its requirements both by the Federal Trade Commission (FTC), the leading federal consumer protection agency, and by state Attorneys General. Shared prosecutorial powers have led to many successful enforcements to protect children's interests. To illustrate, the FTC and New York carried out a joint enforcement ac-

---

22 Bobby Allyn, *With No Federal Facial Recognition Law, States Rush To Fill Void*, NPR (Aug. 28, 2025, at 13:23 ET), https://www.npr.org/2025/08/28/nx-s1-5519756/biometrics-facial-recognition-laws-privacy [https://perma.cc/XMR8-ZHWC]; *Global Biometrics Regulation Chart*, BAKER DONELSON (May 2025), https://www.bakerdonelson.com/webfiles/Publications/Global-Biometrics-Laws-Chart.pdf [https://perma.cc/XL59-7MYL].

23 Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2024); *see* Ryan Kenney, *What Is BIPA and Why Does It Matter?*, EDGEWORTH ECON. (Sep. 7, 2023), https://www.edgeworthеconomics.com/insight-what-is-BIPA-why-does-matter [https://perma.cc/5ZDK-ADWQ]. For a discussion on the significance and impact of BIPA, see SOLOVE & SCHWARTZ, *supra* note 6, at 854–62.

24 Schwartz, *supra* note 2, at 919–21, 943, 945.

25 *See* Fair Credit Reporting Act; Preemption of State Laws, 90 Fed. Reg. 48710, 48714 (Oct. 28, 2025) (to be codified at 12 C.F.R. pt. 1022).

26 *See id.*

tion against Google that settled for $170 million in 2019.[27] The split saw $136 million collected by the FTC and $34 million by New York.[28]

Similarly, HIPAA permits enforcement of its provisions by both the Department of Health and Human Services (HHS) and state Attorneys General.[29] This division of authority has led to high settlements by both entities following investigations of violations of federal health care law.[30] States also sometimes pool resources and engage in multistate actions. One such action by New York, New Jersey, and Connecticut in 2024 led to a $4.5 million settlement with Enzo Biochem.[31]

III. DATA PRIVACY FEDERALISM 2.0: ANTI-COMMANDEERING

We turn now to Data Federalism 2.0, which concerns the sharing of data among different levels of government. As a distinct field of law, data privacy first emerged in the late 1960s and early 1970s.[32] A key concern of that time was the threat posed by the increasing amount of personal data in control of the government. In his account of the rise of first-generation data privacy statutes, Viktor Mayer-Schönberger summarizes, "Without computers a modern welfare state could not operate."[33] In particular, the Great Society of President Lyndon B. Johnson sought the creation of domestic programs to expand social welfare, eliminate racial injustice, and improve access to education and healthcare.

---

27 Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sep. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law [https://perma.cc/7VSU-TY4U].

28 *Id.*

29 *See State Attorneys General*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Dec. 21, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html [https://perma.cc/85PE-LGBJ] (noting that a 2009 amendment to HIPAA added this authority for state Attorneys General).

30 The largest HIPAA fine collected to date by the federal government was the 2018 penalty assessed against Anthem Inc. for a data breach. *See Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest Health Data Breach in History*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Oct. 15, 2018), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html [https://perma.cc/F3Z6-Y9DD].

31 Steve Alder, *HIPAA Enforcement by State Attorneys General*, THE HIPAA J. (Jan. 25, 2026), https://www.hipaajournal.com/hipaa-enforcement-by-state-attorneys-general/ [https://perma.cc/99ZP-56T5].

32 For a comparative study examining the rise of data privacy law, see COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 2–3 (1992).

33 Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 219, 222 (Phillip E. Agre & Marc Rotenberg eds., 1997).

This agenda also called for enhanced governmental collection of digitalized personal data.[34]

The rational provision of governmental services meant not only the computerization of personal data, but the linkage of information held by different levels of government. Many social welfare programs in the United States involve joint federal and state administration. Medicaid provides a good example of Data Federalism 2.0. Created in 1965, Medicaid is a joint federal-state program that provides free or low-cost health coverage to millions of low-income individuals.[35] It is also a data-driven partnership in which the federal government sets guidelines, oversees compliance, and approves state plans. As for the states, they operate the program and determine eligibility within federal rules.

Until recently, the sharing of data among different levels of government received scant scholarly attention. That changed in 2022 with the publication of Professor Bridget Fahey's path-breaking article, *Data Federalism*.[36] In it, Professor Fahey develops an insightful account of federal-state "data pools."[37] Her article identifies four essential elements present in the "intergovernmental data market."[38] First, personal data should be seen as a form of governmental power.[39] Second, federalism now does more than divide governing authority; it concerns the terms of access to personal data.[40] Third, rather than traditional cooperative federalism, which is established through detailed federal statutes, data federalism operates in an "interstitial space" where different levels of government collaboratively fill in gaps in statutory formal law through negotiated agreements about sharing data.[41]

As for Professor Fahey's fourth point, it links data federalism to an important constitutional limitation on the federal government, namely, the anti-commandeering principle.[42] *Printz v. United States* is the leading Supreme Court case about

---

34 *See* BENNETT, *supra* note 32, at 46, 68–70.

35 *Medicaid 101*, MEDICAID & CHIP PAYMENT & ACCESS COMM'N, https://www.macpac.gov/medicaid-101/ [http://perma.cc/AM7J-65R9] (last visited Mar. 18, 2026).

36 *See* Fahey, *supra* note 4, at 1009.

37 *Id.* at 1012.

38 *Id.* at 1016–29.

39 *Id.* at 1017.

40 *Id.* at 1029.

41 *Id.* at 1014.

42 *Id.* at 1054–55.

this doctrine.[43] In it, the Court observed that "the Federal Government . . . may not compel the States to enact or administer a federal regulatory program."[44] As Justice Antonin Scalia stated for the *Printz* Court, the Federal Government cannot issue orders requiring that the states address particular problems.[45] It also cannot command state officers "to administer or enforce a federal regulatory program."[46] In the view of the *Printz* Court, "[S]uch commands are fundamentally incompatible with our constitutional system of dual sovereignty."[47]

How does anti-commandeering relate to data privacy federalism? According to Professor Fahey, data takings by the federal government should be seen as a form of "commandeering." When the federal government engages in "snatching up and carting away" state data assets, it is engaging in "commandeering" that is contrary to the Constitution.[48] We turn now to Data Privacy Federalism 3.0. How have recent developments changed the terms of the debate around preemption and anti-commandeering?

IV. DATA PRIVACY FEDERALISM 3.0

The foundation for federalism policy considerations has shifted considerably. These developments more than justify viewing the new era as one of Data Privacy Federalism 3.0.

A. Preemption Today

Regarding preemption, two important changes have occurred in the privacy landscape. The first is the explosion of omnibus state privacy statutes. The second is the continuing lack of a federal omnibus privacy law, as well as an almost complete absence of congressional privacy lawmaking at the sectoral level.[49]

---

43 *See* 521 U.S. 898, 925 (1997).

44 *Id.* at 926 (quoting New York v. United States, 505 U.S. 144, 188 (1992)).

45 *Id.* at 935.

46 *Id.*

47 *Id.*

48 *Id.*

49 In 2025, Congress enacted the TAKE IT DOWN Act, Pub. L. No. 119-12, 139 Stat. 55. This statute criminalizes the non-consensual publication of intimate imagery and gives enforcement power to the FTC. David Leibert, *Congress's Attempt to Criminalize Nonconsensual Intimate Imagery: The Benefits and Potential Shortcomings of the TAKE IT DOWN Act*, NAT'L ASS'N OF ATT'YS GEN. (Aug. 26, 2025), https://www.naag.org/attorney-general-journal/congresss-attempt-to-criminalize-nonconsensual-intimate-imagery-the-benefits-and-potential-shortcomings-of-the-take-it-down-act/ [https://perma.cc/UUV7-FND6].

Already in 2013, a headline in the *New York Times* noted, *No U.S. Action, so States Move on Privacy Law*.[50] The article observed that over two dozen sectoral privacy laws had been enacted that year in more than ten states, and "in places as different as Oklahoma and California."[51] Some of the most important state legislation at the time concerned data breach notification and data disposal requirements. All fifty states and the District of Columbia have now enacted data breach notification statutes.[52] The only federal requirement in this area is found in an amendment to HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act (2009), which requires HIPAA-covered entities and their business associates to notify affected individuals and the Secretary of HHS within sixty days of discovery of a breach of certain kinds of personal data.[53] Like HIPAA, the HITECH Act only preempts state breach notification laws that are less protective than it or that conflict with federal requirements.[54]

The next important development at the state-level dates back to 2018 and the enactment of the California Consumer Privacy Act (CCPA).[55] This law is an EU-style general data privacy law. As Professor Graham Greenleaf observed in 2020, "[f]ifty years after the 1970 enactment of the first data privacy Act by the German state of Hesse, the US private sector finally has a broadly applicable data privacy Act."[56] In recent years, other states have followed California's example and enacted omnibus-style privacy laws. There are now twenty states with such general laws.

An area of cutting-edge sectoral state legislation concerns geolocational data. In 2025, Maryland and Oregon banned the sale of precise geolocational data.[57] At least four other states

---

50 Somini Sengupta, *No U.S. Action, so States Move on Privacy Law*, N.Y. TIMES (Oct. 30, 2013), https://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html [https://perma.cc/32LN-G6G8].

51 *Id.*

52 SOLOVE & SCHWARTZ, *supra* note 6, at 901–05.

53 45 C.F.R. §§ 164.400–.414 (2026).

54 The obligations of state laws that are stricter than HIPAA must be followed. State breach notification laws, however, generally sweep more broadly than HITECH by covering leaks of all personal data law, including non-health data. In contrast, HITECH reaches only "Protected Health Information." 45 C.F.R. § 160.102; *see also* SOLOVE & SCHWARTZ, *supra* note 6, at 453.

55 The law is codified at Title 1.81.5. CAL. CIV. CODE §§ 1798.100–.199.100 (2023).

56 Graham Greenleaf, *California's CCPA 2.0: Does the US Finally Have a Data Privacy Act?*, 168 PRIV. L. & BUS. INT'L REP., Dec. 2020, at 16–17, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3793435 [https://perma.cc/S3QT-6DHT].

57 *See* Tonya Riley, *Protecting Geolocation Data Emerges as State Privacy Priority*, BLOOMBERG L. (Feb. 13, 2026, at 02:00 PT), https://news.bloomberglaw.com/privacy-and-data-

have now introduced bills that ban the sale of geolocational data.[58] Another frontier of state sectoral regulation is surveillance pricing. New York has now enacted a law requiring disclosure to consumers when companies use algorithms to set prices.[59] In contrast to dynamic pricing, which changes prices based on overall market demand, surveillance pricing leverages an individual's personal data to set a tailored cost for a product or service.[60] Violations of the New York law can result in civil penalties of up to $1,000 per violation.[61]

Finally, state enactment of sectoral privacy laws includes a wave of laws regulating AI. While AI is not exclusively a data privacy issue, it raises significant issues about this area. In the assessment of Professor Daniel Solove, "AI remixes existing privacy problems in complex and unique ways."[62] For example, it encourages collection of more personal data to improve predictive AI's accuracy.[63] AI also raises privacy concerns around the scraping of data online without consent and the leakage from large language models that can release personal information drawn on in training models.[64] At present, four states have broadly applicable AI laws: California, Colorado, Texas, and Utah.[65] Beyond these general AI statutes, and somewhat surprisingly, almost every state has enacted regulations affecting one or another aspect of AI.[66]

In contrast to this intense state activity, Congress has been mired in gridlock around privacy legislation, including an absence of federal laws regarding geolocational data, surveillance pricing, or AI. The standstill reflects an overall lack of congres-

---

security/protecting-geolocation-data-emerges-as-state-privacy-priority [https://perma.cc/R9M4-2EUS].

58 *Id.*

59 *Consumer Alert: Attorney General James Warns New Yorkers About Algorithmic Pricing as New Law Takes Effect*, N.Y. STATE ATT'Y GEN. (Nov. 5, 2025), https://ag.ny.gov/press-release/2025/attorney-general-james-warns-new-yorkers-about-algorithmic-pricing-new-law-takes [https://perma.cc/X2GE-YKQ8].

60 Darrell M. West, *What Is Dynamic Pricing and Why Do Consumers Need Better Protections?*, BROOKINGS INST. (Mar. 18, 2026), https://www.brookings.edu/articles/what-is-dynamic-pricing-and-why-do-consumers-need-better-protections/ [https://perma.cc/ZDU6-4MWP].

61 *Consumer Alert*, *supra* note 59.

62 Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 FLA. L. REV. 1, 5 (2025).

63 *See id.* at 9–11.

64 *See id.* at 5–6, 9–11.

65 *Artificial Intelligence Update - August 2025*, QUINN EMANUEL (Aug. 18, 2025), https://www.quinnemanuel.com/the-firm/publications/artificial-intelligence-update-august-2025/ [https://perma.cc/VC4M-7F5R].

66 *See U.S. AI Law Tracker*, ORRICK (Mar. 27, 2026), https://ai-law-center.orrick.com/wp-content/uploads/Orrick-US-AI-Law-Tracker.pdf [https://perma.cc/3XFB-AHQ7].

sional activity; beyond data privacy, the current Congress has "a growing reputation as the least productive in modern history."[67] The most recent significant federal attempt to enact a national privacy law concerned the proposed 2022 American Data Privacy and Protection Act.[68] One of the most important hurdles to enactment of this bill and subsequent omnibus privacy bills has been whether the national law would override stricter state laws, such as California's CCPA.[69] Congressional enactment of new sectoral privacy laws is also at a virtual standstill.

With each new general state privacy law enacted, the task of passing a federal law has become more difficult. Yet, this result is not inevitable. Indeed, as scholars have demonstrated, state legislative efforts in a variety of areas (such as environmental law) led to a "flight to Washington" by regulated industries to seek a federal legislative solution. J.R. DeShazo and Jody Freeman have termed this phenomenon "defensive preemption."[70] As DeShazo and Freeman observe, state-level regulations can motivate regulated industries and prompt their demand for federal preemptive lawmaking.[71] In writing about preemption and privacy in 2009, I devoted much of my analysis to "life under defensive preemption" for privacy law.[72] At the time, it seemed likely to me that the future of privacy law would be, if not a federal omnibus law, a federal consolidation of state sectoral laws. Yet, even federal sectoral lawmaking has not occurred with any frequency.

It is an open question as to why Congress has been inactive in the privacy landscape. One factor may be a lack of pressure in D.C. by tech companies in favor of a federal privacy law. It is possible that the tech industry now has a general distrust of federal legislative solutions and is willing to live with the (state) devils that it knows. Something like that may explain why there are now fifty state breach notification laws and no sectoral

---

67 Barbara Sprunt, *'Congress is in a Coma.' Former Lawmakers Sound Alarm on Health of the House*, NPR (Dec. 21, 2025, at 05:00 ET), https://www.npr.org/2025/12/21/g-s1-101741/congress-is-in-a-coma-former-lawmakers-sound-alarm-on-health-of-the-house [https://perma.cc/ST89-CZ2W].

68 American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

69 Emily Catron & Gary Kibel, *Federal Data Privacy Legislation: Differences with State Laws Raise Preemption Issues*, REUTERS (Aug. 10, 2022), https://www.reuters.com/legal/legalindustry/federal-data-privacy-legislation-differences-with-state-laws-raise-preemption-2022-08-10/ [https://perma.cc/ZUP2-6XCW].

70 J.R. DeShazo & Jody Freeman, *Timing and Form of Federal Regulation: The Case of Climate Change*, 155 U. PA. L. REV. 1499, 1500 (2007).

71 *Id.* at 1530.

72 Schwartz, *supra* note 2, at 931–40.

federal data breach notification statute that would consolidate the sometimes vastly different obligations under the state statutes. Another possibility is that the many chokepoints in Congress mean that only legislation with overwhelming bipartisan support can be enacted.[73]

Beyond gridlock, another development has been the attempt of the Trump administration to prohibit or limit state regulation in emerging technological areas. To be sure, there has not yet been a federal attempt to stop states from enacting omnibus data privacy statutes. Rather, this federal effort has centered around AI, which, as already noted, is a matter that raises privacy concerns and has led to considerable state legislative activity. Revoking the Biden administration's Executive Order 14067, President Donald Trump's Executive Order 14365 has sought to federalize the issue of AI regulation. Issued on December 11, 2025, this Executive Order mandates a "minimally burdensome national policy framework for AI."[74] The order observes, "State-by-State regulation by definition creates a patchwork of 50 different regulatory regimes that makes compliance more challenging, particularly for start-ups."[75] It calls for congressional action "to ensure that there is a minimally burdensome national standard—not 50 discordant State ones."[76]

Trump's Executive Order would permit state activity concerning AI only in limited areas, including child safety and infrastructure development.[77] Pursuant to it, Congress is to block other state AI laws.[78] The Executive Order also raises specific objections to state AI regulation that is considered to be ideologically-driven or violative of the First Amendment.[79] In anticipation of the enactment of a minimally burdensome federal law, the order also creates an AI Litigation Task Force at the Department of Justice. Its task is to challenge state AI laws that are "inconsistent with the policy set forth" in the order.[80]

---

73 Abraham Newman points to the presence in the United States of extensive institutional veto points on the enactment of new legislation, "including the bicameral nature of the U.S. Congress and the presidential system," as a historic factor limiting the scope of U.S. federal privacy law. ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 59–60 (2008).

74 Exec. Order No. 14365, 90 Fed. Reg. 58499, 58499 (Dec. 16, 2025).

75 *Id.*

76 *Id.*

77 *Id.*

78 *Id.*

79 *Id.* at 58500.

80 *Id.* at 58499.

In parallel to the issuance of the Executive Order, the House of Representatives introduced a ten-year ban on states and municipalities enacting laws and regulations related to AI.[81] Ultimately, the Senate rejected this bill and did so overwhelmingly.[82] A second congressional attempt to block state AI laws involved placing the ban in the National Defense Authorization Act.[83] Ultimately, this provision was stripped from the defense bill.[84] At that time, Republican House leadership promised that AI preemption language would show up in future legislation.[85]

The latest salvo in this federal-state conflict is represented by the Trump administration's National Policy Framework for Artificial Intelligence, released on March 20, 2026.[86] The framework emphasizes the need for congressional action regulating AI.[87] Among its goals, it calls for enactment of a federal AI law to protect children, to respect intellectual property rights, to safeguard residential ratepayers from increased electricity costs due to new AI data centers, and prevent the use of AI in banning "content based on partisan or ideological agendas."[88]

Finally, this document calls for a federal AI policy framework that will preempt cumbersome state AI laws. Much is unclear, however, about the precise boundaries of this future

---

81 Danielle Ochs & Zachary V. Zagger, *U.S. Senate Strikes Proposed 10-Year Ban on State and Local AI Regulation from Spending Bill*, OGLETREE DEAKINS (July 2, 2025), https://ogletree.com/insights-resources/blog-posts/u-s-senate-strikes-proposed-10-year-ban-on-state-and-local-ai-regulation-from-spending-bill/ [https://perma.cc/7TM6-XXZM].

82 Press Release, U.S. Senate Comm. on Com., Sci., & Transp., Senate Strikes AI Moratorium from Budget Reconciliation Bill in Overwhelming 99-1 Vote (July 1, 2025), https://www.commerce.senate.gov/press/dem/release/senate-strikes-ai-moratorium-from-budget-reconciliation-bill-in-overwhelming-99-1-vote-2025-7/ [https://perma.cc/TB8Z-EED9].

83 *See* Press Release, Cong. Progressive Caucus, Congressional Progressive Caucus Announces Official Position Opposing Preemption of State AI Regulations in Annual Pentagon Policy Bill (Nov. 26, 2025), https://progressives.house.gov/2025/11/congressional-progressive-caucus-announces-official-position-opposing-preemption-of-state-ai-regulations-in-annual-pentagon-policy-bill [https://perma.cc/K7JB-KFWL].

84 *See* Joshua A. Geltzer et al., *What the NDAA Means for AI and Cybersecurity*, WILMERHALE (Dec. 19, 2025), https://www.wilmerhale.com/en/insights/client-alerts/20251219-what-the-ndaa-means-for-ai-and-cybersecurity [https://perma.cc/AWF9-K33M].

85 Press Release, Steve Scalise, House Majority Leader, Scalise, Johnson, Guthrie, Jordan, Babin: House Will Work to Implement National AI Framework (Mar. 20, 2026), https://scalise.house.gov/press-releases/Scalise-Johnson-Guthrie-Jordan-Babin-House-Will-Work-to-Implement-National-AI-Framework [https://perma.cc/PDU8-AGFW].

86 *A National Policy Framework for Artificial Intelligence*, THE WHITE HOUSE (March 20, 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf [https://perma.cc/L3RH-UJM7].

87 *Id.*

88 *Id.*

preemption. On one hand, "Preemption must ensure that State laws do not govern areas better suited to the Federal Government or act contrary to the United States' national strategy to achieve global AI dominance."[89] On the other hand, the resulting national standard is not to preempt "traditional police powers retained by the states to enforce laws of general applicability against AI developers . . . , including particular laws to protect children, prevent fraud, and protect consumers."[90] In sum, the threat remains of federal blocking legislation that stops state AI laws.

With or without federal blockage of state data lawmaking, continuing state enactment of laws in this area might also lead to significant challenges resting on the Dormant Commerce Clause.[91] The current crop of state data privacy laws are drafted well, however, to survive such challenges. In *National Pork Producers Council v. Ross*, the Supreme Court rejected an expansive view of the Dormant Commerce Clause.[92] California had acted to forbid the in-state sale of whole pork meat that came from breeding pigs that were "confined in a cruel manner."[93] The Court upheld the contested state law largely because the statute imposed the same burden on in-state and out-of-state pork producers. The California statute was not designed to protect local economic interest and penalize out-of-state competitors. Consequently, there was no violation of the "antidiscrimination principle" that rests at the "very core" of Dormant Commerce Clause jurisprudence.[94]

Along the same lines as the California statute in *National Pork Producers Council*, state omnibus privacy laws and emerging state sectoral laws are nondiscriminatory. These laws apply to local and out-of-state industries alike. For example, the CCPA extends its protection to "consumers," defined as California residents, and regulates businesses, whether in-state or out-of-state in the same fashion based on their activities as pertaining to "a

---

89 *Id.*

90 *Id.*

91 For a discussion of the scope of the Dormant Commerce Clause in the age of the Internet, see generally Jack Goldsmith & Eugene Volokh, *State Regulation of Online Behavior: The Dormant Commerce Clause and Geolocation*, 101 TEX. L. REV. 1083 (2023).

92 598 U.S. 356, 364 (2023).

93 *Id.* at 365–66 (quoting CAL. HEALTH & SAFETY CODE § 25990(b)(2) (West 2026)).

94 *Id.* at 369 (citation omitted). For an analysis of this case that finds its core concern in how the Dormant Commerce Clause prevents purposeful discrimination against out-of-state economic interests, see generally Jack Goldsmith & Eugene Volokh, *The Relevance of* Ross *to Geolocation and the Dormant Commerce Clause*, 102 TEX. L. REV. ONLINE 30 (2023).

consumer's personal information."[95] As a further example, the Colorado AI law extends its protections to a "consumer," defined as "an individual who is a Colorado resident."[96] Its obligations apply to a "developer," which means "a person doing business in this state that develops or intentionally and substantially modifies an artificial intelligence system."[97] There is no distinction made between in-state and out-of-state developers. Thus, at least under current caselaw, Dormant Commerce Clause attacks on state data regulations will represent a constitutional challenge that favors the states.

On its own merits, moreover, state lawmaking around emerging privacy issues should be welcome on federalism grounds. An important distinction is first to be made. Concerning privacy lawmaking, I already observed in 2009, "Whether one is a privacy advocate or skeptic, history teaches that the federal government and the states may switch back and forth in their concern for and level of attention to this issue."[98] Moreover, privacy advocates and skeptics alike should exercise realism about the data-driven preferences of the states. For example, regarding data about reproductive choices post-*Dobbs*, states can be expected to exercise the ideological preferences of the majority party. As a consequence, some states will oppose privacy protections for personal data that reveal reproductive decisionmaking. To illustrate, the Texas Attorney General sued the federal government in fall 2024 to stop federal medical privacy rules that would prevent state authorities "from viewing the medical records of women who travel out of state to seek abortions where the procedure is legal."[99]

Independent of one's prior normative commitments, however, a federalism perspective offers at least two insights about potentially positive state contributions to regulating data privacy. The first is the classic Brandeisian notion of the states as laboratories for innovative policymaking. The second is the potential of states as catalysts for bipartisanship policy cooperation.

---

95 CAL. CIV. CODE § 1798.100 (West 2023).

96 S.B. 24-205, 2024 Gen. Assemb., Reg. Sess. (Colo. 2024).

97 *Id.* § 6-1-1701(7).

98 Schwartz, *supra* note 2, at 938.

99 *See* Michael Wines, *Texas Sues for Access to Records of Women Seeking Out-of-State Abortions*, N.Y. TIMES (Sept. 6, 2024), https://www.nytimes.com/2024/09/06/us/texas-abortion-medical-records.html [https://perma.cc/TMX3-XSDY].

We begin with the Brandeisian argument for state lawmaking. Justice Louis Brandeis famously pointed to this benefit of state regulation and identified the ability of these "novel social and economic experiments" to take place, at least some of the time, "without risk to the rest of the country."[100] As regards data privacy law, states have often preceded the federal government in identifying areas of regulatory significance and in taking action. The states have also provided innovative approaches to regulation of privacy. Indeed, the states have created opportunities for simultaneous experiments with different policies.[101]

As for the states as a force for bipartisan policy consensus, some scholars have already explored how federalism can assist different levels of government and various political entities in the United States in negotiating differences. Professor Judith Resnick has identified among the "core challenges of federalism" the production of "shared commitments while respecting differences."[102] In a similar approach, Dean Cristina Rodríguez sees federalism as allowing the creation of a framework for "negotiation of disagreements large and small."[103] In my view, these approaches are especially appealing today because of the fractured times in which we live.[104]

Federalism has tremendous promise as a framework for negotiating national differences concerning the regulation of personal information. This Article has already mentioned joint federal-state enforcement activities under COPPA, a federal law. At the state level as well, there have been shared enforcement actions. For example, a bipartisan coalition of twenty-eight states

---

100 New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

101 See Paul M. Schwartz, *The Value of Privacy Federalism*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 334 (Beate Roessler & Dorota Mokrosinska eds. 2015) (arguing that the "social value of privacy federalism" is to ensure "diversity and competition" in the response to "new kinds of technologies and social forms").

102 Judith Resnick, *Federalism(s)' Forms and Norms: Contesting Rights, Deessentializing Jurisdictional Divides, and Temporizing Accommodations*, *in* FEDERALISM AND SUBSIDIARITY: NOMOS LV 363, 368 (James E. Fleming & Jacob T. Levy eds., 2014).

103 Christina M. Rodríguez, *Negotiating Conflict Through Federalism: Institutional and Popular Perspectives*, 123 YALE L.J. 2094, 2097 (2014).

104 For a prescient analysis of polarized disputes in constitutional adjudication and the development of an "equality principle" for polarized disputes, see generally ROBERT A. BURT, THE CONSTITUTION IN CONFLICT (1992).

has objected to the sale of personal genetic information.[105] The states involved ranged on the political spectrum from Florida, Kansas, and Oklahoma to Colorado, Minnesota, and New York.[106] In addition, both Texas and California are now investigating the personal data practices of car manufacturers, an important topic in today's age of connected cars.[107] Finally, California, joined by several other states, has created the bipartisan Consortium of Privacy Regulators. Ten states are now part of this organization, including one red state, Indiana.[108]

In the age of D.C. gridlock, it is important that the states continue to regulate digital data issues. As Professor Spiros Simitis, a European pioneer of data privacy, stated in 1987, all data privacy regulations "remain provisional measures because of the incessant advances in technology."[109] In Professor Simitis' judgment, "The regulation of personal data collection and retrieval should be regarded as a constant learning process based on continual observation of both the changes in information techniques and the conflicts generated by systematic data use."[110] In the face of the never-ending tidal wave of changes in cyberspace, policy inaction should not be an alternative. The states should continue to seize the day. Moreover, the hope should be for a consolidation of lessons learned, whether through federal law or states amending their statutes.[111]

At the same time, however, the power of the states to regulate data privacy and cybersecurity is not boundless. One possible issue for the future will be whether state privacy enforcement actions interfere with the Constitution's assignment of power

---

105 Press Release, William Tong, Att'y Gen., Connecticut Enters Multistate Legal Fight to Protect Genetic Information in 23andMe (June 11, 2025), https://portal.ct.gov/ag/press-releases/2025-press-releases/connecticut-enters-multistate-legal-fight-to-protect-genetic-information [https://perma.cc/C89P-QGGT].

106 *Id.*

107 Press Release, Cal. Priv. Prot. Agency, Ford to Change Practices, Pay Fine for Adding Unnecessary Friction to Opt-Out Process (Mar. 5, 2026), https://privacy.ca.gov/2026/03/ford-to-change-practices-pay-fine-for-adding-unnecessary-friction-to-opt-out-process/ [https://perma.cc/8KUW-45UP]; Press Release, Ken Paxton, Att'y Gen. of Tex., Attorney General Ken Paxton Opens Investigation into Car Manufacturers' Collection and Sale of Drivers' Data (June 6, 2024), http://texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-opens-investigation-car-manufacturers-collection-and-sale-drivers-data [https://perma.cc/SH5R-TSAX].

108 *Minnesota and New Hampshire Join Bipartisan Consortium as Privacy Collaboration Continues Growing Nationwide*, CAL. PRIV. PROT. AGENCY (Oct. 8, 2025), https://cppa.ca.gov/announcements/2025/20251008.html [https://perma.cc/4NTE-2EVH].

109 Simitis, *supra* note 7, at 742.

110 *Id.* at 741.

111 *See* Schwartz, *supra* note 2, at 939–41.

over foreign relations to the President and Congress. As an example of a state role that touches on foreign affairs, the Texas Attorney General is currently enforcing its general consumer protection law against "China-Aligned Companies."[112] In a series of lawsuits, Ken Paxton, Texas' Attorney General, is arguing that Chinese law requires these companies to divulge Americans' personal data to Chinese intelligence agencies.[113] Texas is also alleging that devices from these entities raise security risks with their products being used to "launch multiple cyber-attack operations against the United States."[114]

To be sure, states are traditionally permitted wide discretion to protect their citizens. A classic example of this protection with a global dimension would be civil or administrative actions against foreign manufacturers of products that cause in-state harm. At the same time, the dormant foreign affairs doctrine restricts the ability of states to intrude into the "field of foreign affairs" reserved for the federal government.[115] In 2003, the Supreme Court drew on this concept in a data privacy case. In *American Insurance Ass'n v. Garamendi*, it invalidated a California law that required insurers licensed in that state to disclose Holocaust-era insurance policies to the California Insurance Commissioner.[116] This information was to be used in a state-run registry of unclaimed Holocaust-era life insurance policies; the hope was that this step would allow descendants of the victims of the Shoah to learn about and collect on these policies.[117] The Supreme Court invalidated the California Holocaust Victim Insurance Relief Act on grounds that "the Executive's responsibility for foreign affairs" blocked this state action.[118]

---

112 *See, e.g.*, Press Release, Att'y Gen. of Tex., Attorney General Paxton Sues TP Link for Allowing the CCP to Access Americans' Devices in First of Several Lawsuits Being Filed this Week Against China-Aligned Companies (Feb. 17, 2026), https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-sues-tp-link-allowing-ccp-access-americans-devices-first-several-lawsuits [https://perma.cc/2GYA-QSB6].

113 *Id.*

114 *Id.*

115 Zschernig v. Miller, 389 U.S. 429, 432, 436 (1968). For a discussion, see ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 459–65 (7th ed. 2023).

116 539 U.S. 396, 401 (2003).

117 *See id.* at 410–11.

118 *Id.* at 420. In this case, I had provided an expert opinion regarding German data protection law in the proceedings before the lower courts. Gerling Glob. Reinsurance Corp. of Am. v. Quackenbush, No. S-00-0506WBSJFM, 2000 WL 777978, at *10 (E.D. Cal. 2000), *rev'd sub nom.*, Am. Ins. Ass'n v. Garamendi, 539 U.S. 396 (2003).

There are scant Supreme Court decisions regarding the dormant foreign affairs doctrine. Most likely, state enforcement activities pursuant to general state legislation, as currently pursued by the Texas Attorney General, are constitutionally unproblematic under this doctrine.[119] In contrast, a state statute that singled out a specific foreign nation would likely raise constitutional problems. Such a law might name one or more "countries of concern" and seek to regulate personal data transfers to these foreign adversaries.[120] Thus far, however, the states do not appear interested in enacting such legislation. In my judgment, a greater source of constitutional friction with state data privacy laws will be the First Amendment and its protections for flows of information, including personal data.[121]

B. Anti-Commandeering Today

Professor Fahey has wisely alerted us to the extent that governmental data pools raise federalism issues. And, in this context, there is another notable Trump administration executive order to consider. Trump Executive Order 14243 would radically alter the established process for sharing personal data among different levels of government.[122] In place of past negotiations at the federal and state level around the creation of data pools, the executive branch is now acting by fiat. The Executive Order states, "Immediately upon execution of this order, Agency Heads shall take all necessary steps, to the maximum extent consistent with law, to ensure the Federal Government has unfettered access to comprehensive data from all State programs that receive Federal funding . . . ."[123] The import of this sentence is clear: the Trump administration wishes to command full federal access to data collected through the countless state programs that rely on federal

---

119 As another example, under general state authority, Florida has started a CHINA Prevention Unit within the Office of the Attorney General to address "threats posed by the Chinese Communist Party (CCP) and other foreign adversaries to Florida consumers, data privacy, and economic security." Press Release, Off. of Att'y Gen. State of Fla., Attorney General James Uthmeier Launches China Prevention Unit to Counter Foreign Adversaries and Protect Floridians' Data (Feb. 5, 2026), https://www.myfloridalegal.com/newsrelease/attorney-general-james-uthmeier-launches-china-prevention-unit-counter-foreign [https://perma.cc/WK88-ELUS].

120 *See* Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363, 366 (2000) (invalidating a Massachusetts statute that "bars state entities from buying goods or services" from any company doing business with Burma in a unanimous decision).

121 *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011) (invalidating a Vermont prescription privacy law because it singled out pharmaceutical marketers and data miners).

122 Exec. Order No. 14243, 90 Fed. Reg. 13681, 13681–82 (Mar. 20, 2025).

123 *Id.* at 13681.

money. The Executive Order also reaches private-sector data to the extent that a private entity is acting as a vendor managing state information.

Prior to this Executive Order, the Trump administration's new approach to federal-state data relations began through actions by the Department of Government Efficiency (DOGE).[124] One of the aims of this short-lived federal entity was to collect and consolidate personal information from as many federal governmental sources as possible. According to one tally, DOGE tried to gain access to more than eighty data systems across at least ten federal agencies.[125] Its goal was total information sharing and the destruction of any "information silos" within the government regarding personal data.[126] DOGE engaged in an unprecedented data grab to begin construction of a totalizing federal database. As part of its activities, it also seized state-supplied data that was in the control of federal agencies for limited use in administering federal-state programs.

DOGE has now been disbanded, but many of its employees have gone to other federal agencies.[127] While DOGE has vanished as a formal entity, it forged a path that is being followed by other federal agencies, including the Department of Homeland Security (DHS) and the Department of Agriculture (USDA). Twenty states are now suing HHS for sharing state health data with DHS.[128] The

---

124 Exec. Order No. 14158, 90 Fed. Reg. 8441, 8441 (Jan. 29, 2025); *see* Sarah Cahalan et al., *The People Carrying Out Musk's Plan at DOGE*, N.Y. TIMES (June 16, 2025), https://www.nytimes.com/interactive/2025/02/27/us/politics/doge-staff-list.html [https://perma.cc/6CAB-VCTP].

125 Jonathan Swan et al., *A Subdued Musk Backs Away from Washington, but His Project Remains*, N.Y. TIMES (Apr. 24, 2025), https://www.nytimes.com/2025/04/23/us/politics/elon-musk-doge-trump.html [https://perma.cc/GM43-YFLQ].

126 *See* Stephanie K. Pell, Josie Stewart & Brooke Tanner, *Privacy Under Siege: DOGE's One Big, Beautiful Database*, BROOKINGS INST. (June 25, 2025), https://www.brookings.edu/articles/privacy-under-siege-doges-one-big-beautiful-database/ [https://perma.cc/V9CG-NJ3B].

127 Press Release, Elizabeth Warren, Senator, Warren, Blumenthal, Garcia Launch Investigation into DOGE Employees Embedding into Top Government Roles (Aug. 7, 2025), https://www.warren.senate.gov/newsroom/press-releases/warren-blumenthal-garcia-launch-investigation-into-doge-employees-embedding-into-top-government-roles [https://perma.cc/EQN2-WKZP]. For a post-mortem examination of DOGE, see Makena Kelly & Vittoria Elliott, *DOGE Isn't Dead. Here's What Its Operatives Are Doing Now*, WIRED (Dec. 2, 2025, at 06:00 PT), https://www.wired.com/story/what-is-doge-doing-now/ [https://perma.cc/KWT9-C549].

128 Amanda Seitz & Kimberly Kindy, *20 States Sue After the Trump Administration Releases Private Medicaid Data to Deportation Officials*, AP NEWS (July 1, 2025, at 20:07 PT), https://apnews.com/article/trump-medicaid-immigrant-california-161f7e1b9087512d674258f32f822878 [https://perma.cc/456M-Z5J3].

states gave this personal information to HHS for administration of the Medicaid program.[129] Early in the second Trump administration, HHS turned this information over to DHS for immigration enforcement.[130] This action affected millions of individuals.

As for the USDA, it is the federal entity responsible for SNAP, which helps approximately forty-two million Americans, or about one in eight, purchase groceries.[131] The USDA and the states jointly administer this program. In late 2025, the USDA announced that it would stop paying SNAP funds to states that did not turn over extensive personal information about program recipients, including home addresses, Social Security Numbers, recent locations, and immigration status.[132] The federal goal was to use this data for immigration enforcement. Twenty-two states have sued to prevent the Trump administration from demanding that they turn over this data.[133]

In early stages of the ensuing litigation in both matters, state litigants have largely been successful. In December 2025, Judge Vince Chhabria issued a preliminary injunction against the data sharing between HHS and DHS.[134] His injunction does allow basic biographical contact and locational information to be shared by the HHS with the DHS.[135] But Judge Chhabria found that the federal government had offered no justification for its sharing of additional personal data, such as "sensitive medical information about Medicaid patients."[136] In issuing an earlier preliminary injunction, Judge Chhabria pointed to the long-standing HHS policy of not sharing certain personal data of Med-

129 *Id.*

130 *Id.*

131 *See Supplemental Nutrition Assistance Program Participation and Costs*, USDA FOOD & NUTRITION SERV. (Feb. 13, 2026), https://fns-prod.azureedge.us/sites/default/files/resource-files/snap-annualsummary-4.pdf [https://perma.cc/5JNY-Y2U9].

132 Linda Qiu, *Agriculture Dept. Threatens to Withhold Food Stamps from Democratic States*, N.Y. TIMES (Dec. 2, 2025), https://www.nytimes.com/2025/12/02/us/politics/food-stamps-democratic-states.html [https://perma.cc/K7HA-M372].

133 Nate Raymond, *Trump Administration Cannot Force States to Supply Food Stamp Data, US Judge Rules*, REUTERS (Feb. 26, 2026, at 13:48 PT), https://www.reuters.com/legal/government/trump-administration-cannot-force-states-supply-food-stamp-data-us-judge-rules-2026-02-26/ [https://perma.cc/7Z73-ZA2X].

134 Order Granting in Part and Denying in Part Motion for Preliminary Injunction at *1, California v. U.S. Dep't of Health & Hum. Servs., No. 25-cv-05536-VC, 2025 WL 3751931 (N.D. Cal. Dec. 29, 2025).

135 *Id.* at *2–3.

136 *Id.* at *3.

icaid patients and added that various federal and state actors in the Medicaid system had relied on this approach.[137]

In the SNAP litigation, state litigants have also enjoyed victories in federal courts. In September 2025, a district court in the Northern District of California issued a temporary restraining order that prevented the contested data collection and blocked the USDA from withholding administrative funding from states.[138] More recently, on February 26, 2026, this court issued a preliminary injunction that continued the block on the federal withholding of SNAP funding from the states that had refused to share recipient data.[139]

How do these recent data-driven actions by the federal government fit into a federalism framework? The actions of the Trump administration toward the states go far beyond the range of behavior that scholars have termed "uncooperative federalism." To illustrate, we can consider the argument in favor of "uncooperative federalism" by Jessica Bulman-Pozen and Heather Gerken in 2009.[140] As part of their approach, and perhaps unexpectedly, these scholars took a stance in favor of commandeering. In their view, uncooperative federalism can play a positive role in "a well-functioning federal system."[141] Bulman-Pozen and Gerken argue, "[t]he state's leverage over the federal government only increases after the federal government has devolved regulatory powers to the state."[142] Involvement of state officials through commandeering would lead to a range of positive results, including "greater federal-state integration," states with "greater agenda-setting power," and the enabling of state bureaucrats to serve "as 'connected critics' within the federal system."[143] This analysis does not fit the current moment.

When it comes to data privacy federalism at present, there is an absence of federal-state integration, state agenda setting, or

---

137 *See id.*

138 Order Granting Temporary Restraining Order as to All Plaintiff States Other than State of Nevada at 25, California v. U.S. Dep't of Agric., 800 F. Supp. 3d 1015 (N.D. Cal. 2025) (No. 25-cv-06310-MMC).

139 Order Granting in Part Plaintiff States' Motion to Enforce or Expand Preliminary Injunction at *13, California v. U.S. Dep't of Agric., No. 25-cv-06310-MMC, 2026 WL 534417 (N.D. Cal. Feb. 26, 2026).

140 Jessica Bulman-Pozen & Heather K. Gerken, *Uncooperative Federalism*, 118 YALE L.J. 1256, 1258–60 (2009).

141 *Id.* at 1260.

142 *Id.* at 1268.

143 *Id.* at 1297.

connected state critics within the federal system. While we still live in an era of federalism, it is one marked by extreme hostility on the part of the federal government to state policies contrary to the administration's goals. Professors Aziz Huq and Zachary Clopton term this new approach, "agonistic federalism."[144] Federalism under the Trump administration is not an extension of uncooperative federalism. It represents not continuity, but "a rupture of integrated federalism instigated by the federal government."[145] As one of its primary elements, the current administration is engaged in "the weaponization of states' entanglement in cooperative federalism programs."[146] Huq and Clopton argue that "something new is afoot" and point to the volume and scope of the federal actions to terminate state funding upon noncooperation.[147] With considerable understatement, they also note the Trump administration's "disinterest for statutory requirements and settled conventions."[148]

The Huq-Clopton model is extremely helpful in mapping the contours of the second Trump administration's approach to data privacy federalism. The Trump administration is now seizing and consolidating data from within federal-state data pools (as in the Medicaid example) and threatening to defund federal-state social programs if states do not share personal information (as in the SNAP example). As a result of the breakdown of integrated federalism, the anti-commandeering concept is more important than ever. There is also an urgent need to develop it for the information age in which we live.

In particular, the Supreme Court has never ruled that its anti-commandeering jurisprudence applies to personal data. In *Printz*, Justice Scalia for the majority explicitly declined to answer this question. *Printz* conceded the existence of "a number of federal statutes enacted within the past few decades that require the participation of state or local officials in implementing federal regulatory schemes."[149] The majority opinion added that some of these regulatory programs "require only the provision of infor-

144 Aziz Z. Huq & Zachary D. Clopton, *Agonistic Federalism*, 104 TEX. L. REV. (forthcoming 2026) (manuscript at 14) (available at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2420&context=public_law_and_legal_theory) [https://perma.cc/JP28-3LDS].

145 *Id.* at 15.

146 *Id.* at 21.

147 *Id.* at 22–24.

148 *Id.* at 24.

149 Printz v. United States, 521 U.S. 898, 917 (1997).

mation to the Federal Government."[150] These programs also did not "involve the precise issue before" the *Printz* Court, which was "the forced participation of the States' executive in the actual administration of a federal program."[151] Thus, *Printz* explicitly reserved for another day the question of whether anti-commandeering protections extended to personal information.[152]

Subsequent to *Printz,* the Supreme Court rejected a state challenge to a federal data privacy statute. In *Reno v. Condon*, the unanimous Court upheld the DPPA as a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause.[153] The *Reno* Court noted the DPPA's wide reach. It declared, "[t]he DPPA regulates the universe of entities that participate as suppliers to the market for motor vehicle information—the States as initial suppliers of the information in interstate commerce and private resellers or redisclosers of that information in commerce."[154] In an opinion by Chief Justice William Rehnquist, the *Reno* Court concluded, "Because drivers' information is, in this context, an article of commerce, its sale or release into the interstate stream of business is sufficient to support congressional regulation."[155]

As for the idea of anti-commandeering, the *Reno* Court dismissed any similarities with *Printz* or its earlier federalism decision in *New York v. United States*. In these opinions, the Court was concerned with Congress taking over the state legislative process, or "conscripting the States' officers directly."[156] The *Reno* Court conceded that "the DPPA's provisions will require time and effort on the part of state employees."[157] But this federal law did not require "the States in their sovereign capacity to regulate their own citizens."[158] It also did not require the enactment of any

150 *Id.* at 918.

151 *Id.*

152 Two other Justices in *Printz* addressed the relationship between personal data and federalism. In her concurrence, Justice Sandra Day O'Connor approved of the Court's choice to refrain from deciding whether "purely ministerial reporting requirements imposed by Congress on state and local authorities" were invalid. *Id.* at 936 (O'Connor, J., concurring). In contrast, Justice John Paul Stevens in dissent argued that the anti-commandeering principle did not apply to personal data. He stated, "The enactment of statutes that merely involve the gathering of information . . . do not raise even arguable separation-of-powers concerns." *Id.* at 960 n.22 (Stevens, J., dissenting).

153 528 U.S. 141, 143 (2000); U.S. CONST., art. I, § 8, cl. 3.

154 *Reno*, 528 U.S. at 151.

155 *Id.* at 148.

156 *Id.* at 149 (quoting *Printz*, 521 U.S. at 935).

157 *Id.* at 150.

158 *Id.* at 151.

state laws or draw on "state officials to assist in the enforcement of federal statutes regulating private individuals."[159]

Data Privacy Federalism 3.0 is concerned with a different policy issue than *Reno*. The policy issue in *Reno* concerned a federal legislative approach where the states maintained the personal information in question. Records from the Department of Motor Vehicles were and are the province of state agencies that license motor vehicles.[160] The policy controversy in Data Federalism 3.0 involves federal use of state data for new purposes and without legislative authority or state agreement. In German, the pithy term for this general kind of action is "*Zweckentfremdung*," or "purpose alienation," and it is the source of much scholarly analysis in that country's data protection treatises.[161]

In the United States, a new debate has just started on this concept in the context of actions taken by the Trump administration over federal-state data resources. This federal behavior is not, however, without precedent. The Center for Democracy & Technology identifies federal efforts to access sensitive data as beginning "[u]nder the George W. Bush administration and continuing through much of the Obama administration."[162] This think tank notes that such behavior has "accelerated over the last decade" and faced "significant legal pushback from a bipartisan group of states and fierce opposition from the civil rights and pro-democracy communities."[163]

Considering the renewed attempts during the second Trump administration to pressure states to surrender personal data to it, we are fortunate that Professor Fahey has begun the process of analyzing how anti-commandeering should apply to personal data. Already in 2022, she provided a ringing endorsement for its application to data privacy federalism. She writes, "As data moves

---

159 *Id.*

160 Like HIPAA, moreover, the DPPA permits state laws that are more protective and do not conflict with it. The DPPA only sets out "permissible uses," 18 U.S.C. § 2721(b), but does not prohibit states from enacting stronger disclosure requirements.

161 *See* Alexander Roßnagel, DATENSCHUTZRECHT: DSGVO MIT BDSG [DATA PROTECTION LAW: GDPR WITH BDSG] art. 6, ¶ 4 (1st ed. 2019) (Ger.); Tobias Herbst, *Zweckbindung* [*Purpose Limitation*], *in* DATENSCHUTZ-GRUNDVERORDNUNG/BDSG KOMMENTAR [GENERAL DATA PROTECTION REGULATION/BDSG COMMENTARY] 274–86 (Jürgen Kühling & Benedikt Buchner eds. 2024) (Ger.).

162 CTR. FOR DEMOCRACY & TECH., FEDERAL EFFORTS TO EXPAND ACCESS TO DATA FROM STATE-RUN PROGRAMS AND INDIVIDUAL PRIVACY 3 (July 23, 2025), https://cdt.org/wp-content/uploads/2025/07/Federal-Efforts-to-Expand-Access-to-Data-from-State-Run-Programs-and-Individual-Privacy-FINAL.pdf [https://perma.cc/8EAQ-V7ZQ].

163 *Id.*

across governmental boundaries, it remains connected to the individual who originated it and the government that collected it."[164] Fahey argues that governments "retain an interest in safeguarding their data as it is put to use by their sister governments."[165]

Like Fahey, I believe that anti-commandeering principles apply to personal data. As Huq and Clopton warn, "the national government is engaging in a form of asymmetrical assault on the states through a no-holds-bar reneging on what had seemed an enduring and enabling intergovernmental bargain."[166] Federalism offers a vitally important constitutional bulwark for resistance to these actions. Professor Jennifer Urban, my colleague at Berkeley Law and Chairperson of the California Privacy Protection Agency, has pointed in this regard to two important tasks for the states.[167] Their first role is to "buttress their privacy laws to protect their people's data and vigorously enforce those laws."[168] In addition, Professor Urban calls for the states to "vigorously oppose any attempts by Congress to preempt their protections."[169] The result will be to create a "privacy immune system" for the United States.[170] At this juncture, Federalism 2.0 (anti-commandeering) meets Federalism 1.0 (preemption).

There is also a complication here. As noted above, privacy advocates should not view ever-increasing deference to state privacy regulation as invariably serving their policy preferences. Professor Bulman-Pozen wisely reminds us that the meaning of federalism has long been a historically contingent matter.[171] Independent of prior normative commitments, one should be skeptical of any theory of federalism as a "one-way ratchet" that will always favor the states. In their approaches to data privacy issues, the states will not invariably reflect a narrow Democratic or Republican perspective. Hence, there is also potential here for bipartisan cooperation among blue and red states. At the same time, however, some state activity simply will "flesh out nationwide controversies" at the state level.[172]

---

164 Fahey, *supra* note 4, at 1073.

165 *Id.*

166 Huq & Clopton, *supra* note 144, at 27.

167 Jennifer M. Urban, *Governing Data: The Role of State Privacy Law*, 28 YALE J.L. & TECH. 1, 35–36 (2026).

168 *Id.* at 36.

169 *Id.*

170 *Id.* (emphasis removed).

171 *See* Jessica Bulman-Pozen, *Partisan Federalism*, 127 HARV. L. REV. 1077, 1098–1100 (2014).

172 Bulman-Pozen, *supra* note 8, at 1946.

Where does anti-commandeering fit in as part of this evolving landscape? As *Printz* emphasizes, the states are independent, sovereign entities in the US.[173] Professor Fahey has demonstrated how much federal-state data sharing occurs through "intergovernmental agreements" rather than formal legislation.[174] These agreements exist in a "kind of interstitial space between and across governments."[175] Current behavior by the Trump administration unilaterally changes the terms of past bargaining and eviscerates their democratic legitimacy. Instead of honoring the terms of past intergovernmental agreements, the Trump administration has been adopting a policy of "grab-and-go" concerning personal data.

This conduct represents a problematic commandeering of resources in which the states retain an interest. As *Printz* also stresses, federalism serves an important role in protecting citizens from arbitrary or excessive government action.[176] Indeed, Judge Chhabria in his initial injunction in the Medicaid data litigation objected to the HHS action as "arbitrary and capricious" under the Administrative Procedure Act.[177] In *New York v. United States*, an anti-commandeering case that preceded *Printz*, the Court stated, "the Constitution divides authority between federal and state governments for the protection of individuals."[178] Anti-commandeering principles should be used as part of the opposition by the states to the Trump administration's seizures of personal data.

Finally, there are actions that the states can take regarding the federal data grab. Consider the executive order that Governor Jay Pritzker of Illinois issued in May 2025, to protect the privacy of Illinois residents with autism.[179] The order prohibits state agencies from disclosing autism-related data to the federal government unless there is individual consent or it is legally re-

173 *See* Printz v. United States, 521 U.S. 898, 919–20 (1997).

174 Fahey, *supra* note 4, at 1014.

175 *Id.*

176 *Printz*, 521 U.S. at 921.

177 Order Granting in Part and Denying in Part Motion for Preliminary Injunction at *3, California v. U.S. Dep't of Health & Hum. Servs., No. 25-cv-05536-VC, 2025 WL 3751931 (N.D. Cal. Dec. 29, 2025).

178 505 U.S. 144, 181 (1992).

179 GOVERNOR OF ILL., EXECUTIVE ORDER 2025-02: EXECUTIVE ORDER TO PROTECT THE CIVIL RIGHTS, HUMAN RIGHTS, AND PRIVACY OF AUTISTIC PEOPLE IN ILLINOIS (2025), https://www.illinois.gov/government/executive-orders/executive-order.executive-order-number-02.2025.html [https://perma.cc/CQH2-H8TJ].

quired.[180] Moreover, disclosures are to be limited to the minimum amount of information and anonymized where allowed and practicable. This action was taken in response to the stated plan of HHS Secretary Robert F. Kennedy, Jr. to create a national autism database. As this example indicates, the states are not without tools to protect their residents within the intergovernmental data market.

V. CONCLUSION

A new federalism era for information has begun, that of Data Privacy Federalism 3.0. This epoch is marked by a combination of federal legislative inactivity and an avalanche of state privacy legislation. These developments make the topic of preemption more important than ever. In response, this Article has advocated for continuing state lawmaking.

From a federalism perspective, the first benefit of this activity will be the states having an opportunity to act as laboratories for policy innovation. Beyond this classic argument for federalism, a second advantage will be to create opportunities for bipartisan policymaking at the state level. Due to today's polarized environment, these avenues for cooperation are especially important. At the same time, there are limits to the state role for data privacy. On the horizon may be the question of whether potential state attempts to regulate the data activities of international companies interfere with a more appropriate exclusively federal role in this area.

A further aspect of the new federalism age for information is the importance of the anti-commandeering doctrine for data privacy. It is long established that neither Congress nor the executive branch can command the states in certain ways. Whether this anti-commandeering applies to personal information is an open question. An aspect of data federalism making headlines today concerns federal agencies making unilateral decisions about personal information collected as part of joint federal-state programs. An anti-commandeering principle should apply to these actions and form an essential part of data privacy federalism today.

---

180 *Id.*; *see* Press Release, JB Pritzker, Off. of Governor, Gov. Pritzker Issues Executive Order to Safeguard Rights of Autistic Illinoisans (May 7, 2025), https://gov-pritzker-newsroom.prezly.com/gov-pritzker-issues-executive-order-to-safeguard-rights-of-autistic-illinoisans [https://perma.cc/3N6K-6FPZ].

It Takes a Village (To Raise Children's Privacy)

Mason R. Clark

CONTENTS

It Takes a Village (To Raise Children's Privacy)

Mason R. Clark∗

Raising children is an expensive and (mostly) rewarding commitment. Many parents, guardians, and caregivers are willing to invest in indestructible car seats, private schools, and organic, farm-fresh, whole-grain, low-sugar, dye-free, naturally flavored foods. Is it reasonable to ask them to invest in children's privacy? Surely companies can't expect parents to stand guard at the edge of a digital playground they never built and never (knowingly) agreed to let their children enter.

The digital age has profoundly reshaped children's privacy. It is hard to imagine listening to a podcast or scrolling on a social media platform without being bombarded by reports, rants, and reels about the unprecedented privacy risks children face online. Most federal and state privacy laws have failed to provide a comprehensive framework for safeguarding children's digital privacy. Scholars in this area have proposed legislative and regulatory reform and critiqued corporate malfeasance. This Article suggests it is time to reimagine the pay-for-privacy (PFP) model—an often-discredited model in which users pay for enhanced privacy protections—as a potential solution to minimize children's privacy risks.

This Article makes three arguments. Part II suggests parents are the primary gatekeepers of children's online privacy, and can responsibly manage their child's digital footprints (with some help). It also acknowledges deceptive corporate privacy practices and explores the pitfalls of PFP models. Part III argues companies are well-positioned to provide detailed reports to parents about their child's data and design child-centric privacy protections using revenue from a PFP model. Part IV then claims that the Federal Trade Commission (FTC) may have the expertise and the momentum to moderate between parents and companies in a PFP model.

Like the adage "it takes a village to raise a child," it takes a village to ensure children's privacy. As caregivers consider essential costs to raising children, this Article argues privacy may be one of those costs. PFP models, with appropriate oversight and equity, can enhance parental engagement and incentivize corporate accountability to foster a more private digital environment for children.

∗ Assistant Professor of Law at St. Mary's University School of Law. Former Bruce R. Jacob Visiting Assistant Professor at Stetson University College of Law (2023–2025).

I. INTRODUCTION

For readers who, like me, started using the internet as children in the early 2000s, they may remember their parents or caregivers watching Dateline NBC's *To Catch a Predator* television series[1] and constantly lecturing them about the internet's inherent danger. But no matter how many controls, filters, and blockers parents deployed to stop children from using chatrooms and websites, children were nonetheless able to create social media accounts (the most popular at the time being Myspace) and enter online chatrooms like AOL Instant Messenger to have months-long conversations with complete strangers. The rise of social media use among children and the ensuing moral panic about children's online activities resulted in controversial pieces of legislation like the Deleting Online Predators Act,[2] aimed at preventing children from using social networking sites and chatrooms. This and other pieces of legislation ultimately failed and, as discussed later in this Article, so too have many recent attempts to legislate children's online privacy.

Congress's repeated failure to pass comprehensive protections for children online is perhaps more distressing in today's modern digital age. Although concerns about children's digital privacy still include the "stranger danger" and/or cyberbullying fears from almost thirty years ago, parents are now also concerned about the massive amounts of data—personal, usage, or otherwise—collected from children by online platforms. From nightly news segments to viral TikToks, Americans are reckoning with a growing sense that today's children are also being surveilled and manipulated by the countless devices and platforms they use at home and even in the classroom. Pediatricians, psychologists, and even social media influencers have warned that children are living through a massive, uncontrolled experiment with childhood itself. Jonathan Haidt, one of the most visible critics of children's relationships with technology, calls this period of children's increased use of technology "The Great Rewiring," and he argues that technology has altered not just how children so-

1 For an interesting post hoc review of the controversial television series, see Adrian Horton, *To Catch a Predator: Exploring the Uneasy Legacy of the Controversial TV Series*, THE GUARDIAN (Jan. 27, 2025, at 07:56 ET), https://www.theguardian.com/film/2025/jan/27/to-catch-a-predator-sundance [https://perma.cc/H2JL-VMSS].

2 H.R. 5319, 109th Cong. (2006); *see* Wade Roush, *The Moral Panic over Social-Networking Sites*, MIT TECH. REV. (Aug. 7, 2006), https://www.technologyreview.com/2006/08/07/228481/the-moral-panic-over-social-networking-sites/ [https://perma.cc/8UN5-Q4F9].

cialize and learn, but how they are profiled, categorized, and monetized by the devices and platforms they use.[3]

And yet, the legal tools available to respond to these harms remain limited and outdated. At the federal level, the Children's Online Privacy Protection Act (COPPA), enacted in 1998, remains the central statute regulating the collection of data from children under thirteen.[4] COPPA was groundbreaking at the time of its passage, but it is now widely seen as insufficient. Legal scholars have criticized its reliance on parental consent,[5] its exclusion of certain apps which have teen users and exclusion of teens aged thirteen to seventeen altogether,[6] and its inability to adapt to mobile platforms, biometric data, and algorithmic profiling.[7] COPPA "can be better understood in light of the privacy protection climate in 1998," and may have been "enacted at a time when the major concern was protecting kids from revealing personal information rather than companies collecting kids' user data."[8] And although the Federal Trade Commission (FTC), the agency responsible for enforcing COPPA, has taken notable enforcement actions under the statute—such as two settlements totaling $520 million with Epic Games, Inc. in 2022 and a $170

---

3 JONATHAN HAIDT, THE ANXIOUS GENERATION: HOW THE GREAT REWIRING OF CHILDHOOD IS CAUSING AN EPIDEMIC OF MENTAL ILLNESS 3–7 (2024); *see also* FED. TRADE COMM'N, A LOOK BEHIND THE SCREENS: EXAMINING THE DATA PRACTICES OF SOCIAL MEDIA AND VIDEO STREAMING SERVICES, at i (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf [https://perma.cc/4AX8-7MPV] (reporting on social media companies' use of personal data that "pose unique risks to children and teens").

4 15 U.S.C. §§ 6501–6506. COPPA applies to "operators" of commercial websites, including mobile apps, that are directed at children under thirteen or have actual knowledge that they are collecting personal information from children under thirteen. *See* Abdullah Ahmed, Hashim Hayat & Daheem Hayat, *A Comprehensive Guide to COPPA*, WALTURN (May 23, 2024), https://www.walturn.com/insights/a-comprehensive-guide-to-coppa [https://perma.cc/3F8W-E7S7]. Some of the requirements include notice to parents of data collection, use, and disclosure practices (through privacy policies); obtaining verifiable parental consent before collecting, using, or disclosing children's personal data; and restrictions on behavioral advertising toward children. *Id.*

5 *E.g.*, Zahra Takhshid, *Children's Digital Privacy and the Case Against Parental Consent*, 101 TEX. L. REV. 1417, 1417–22 (2023) (arguing that reliance on parental consent to protect children's privacy is a "fundamental problem" of COPPA).

6 *Id.* at 1454 ("Nevertheless, although not required by COPPA, companies may ask for parental waivers to insulate themselves from potential liability for kids between the ages of thirteen to eighteen."); *see also* Stacey Steinberg, *The Myth of Children's Online Privacy Protection*, 77 SMU L. REV. 441, 449 (2024) (describing how TikTok and Instagram, two social media apps which are not governed by COPPA, are legally accessed by children over thirteen).

7 Steinberg, *supra* note 6, at 457–58 ("When COPPA was initially enacted in 1998, few could imagine a world connected in the ways in which we are now. . . . While policymakers seem aware that such risks exist, federal lawmakers have been unable to agree on legislation to address these growing concerns.").

8 Takhshid, *supra* note 5, at 1426.

million settlement with Google and its subsidiary, YouTube, in 2019[9]—these large settlements are relatively rare. Steinberg described the Google and YouTube settlement as "a drop in the bucket" compared to the revenue made while the companies were being accused of COPPA violations.[10]

Repeated attempts to modernize COPPA have failed. In 2023, bipartisan coalitions in Congress introduced both the Kids Online Safety Act (KOSA) and the Children and Teens' Online Privacy Protection Act (COPPA 2.0), which sought to expand the statute's reach to older minors, limit behavioral advertising, and enhance transparency requirements.[11] Despite support from children's advocacy groups and FTC commissioners, the bills failed to pass, and Senator Ed Markey (D-Mass.)—one of COPPA's original sponsors—said "House Republican leaders abandoned their responsibility and prevented this Congress from enacting life-saving measures for our families."[12]

Recently, Senator Markey and Senator Bill Cassidy (R-La.) reintroduced COPPA 2.0 and were able to obtain unanimous passage of the legislation through the U.S. Senate Commerce Committee in June 2025.[13] The FTC also finalized changes to the

---

9 Press Release, Fed. Trade Comm'n, FTC Finalizes Order Requiring Fortnite Maker Epic Games to Pay $245 Million for Tricking Users into Making Unwanted Charges (Mar. 14, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making [https://perma.cc/5XLD-Q3TS]; Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sep. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law [https://perma.cc/CLR6-XNXW].

10 Steinberg, *supra* note 6, at 455.

11 Kids Online Safety Act, S. 1409, 118th Cong. (2023); Children and Teens' Online Privacy Protection Act, S. 1628, 117th Cong. (2021); *see* Kevin Collier, *Why a Landmark Kids Online Safety Bill That Just Passed the Senate Is Still Deeply Divisive*, NBC NEWS: TECH (July 31, 2024, at 11:03 PT), https://www.nbcnews.com/tech/tech-news/will-kosa-coppa-20-controversial-bills-explained-rcna163243 [https://perma.cc/92CR-BWS9].

12 See Press Release, Sen. Ed Markey, Sen. Markey Statement on Failure to Pass COPPA 2.0 Children and Teen Privacy Legislation by End of Congress (Dec. 18, 2024), https://www.markey.senate.gov/news/press-releases/sen-markey-statement-on-failure-to-pass-coppa-20-children-and-teen-privacy-legislation-by-end-of-congress [https://perma.cc/LD6X-WKEF].

13 Press Release, Sen. Ed Markey, Senators Markey and Cassidy Celebrate Committee Passage of Children and Teens' Online Privacy Protection Legislation (June 25, 2025), https://www.markey.senate.gov/news/press-releases/senators-markey-and-cassidy-celebrate-committee-passage-of-children-and-teens-online-privacy-protection-legislation [https://perma.cc/H5PQ-ZFS6]. COPPA 2.0 would improve upon COPPA's protections in five key areas by: (1) banning targeted advertising to children and teens, including those up to age sixteen; (2) requiring companies to permit users to delete personal information collected from a child or teen; (3) establishing data minimization rules to prohibit the excessive collection of children and teens' data; (4) revising COPPA's "actual knowledge" standard (discussed above) to close the loophole that allows platforms to ignore kids and teens on their sites; and (5) prohibiting internet companies from collecting

COPPA Final Rule,[14] requiring "parents to opt in to third-party advertising" and "address[ing] the emerging ways that consumers' data is collected and used by companies, and particularly how children's data is being shared and monetized."[15] Yet even with this recent momentum by both Congress and the FTC—and COPPA 2.0's support from groups like the Center for Digital Democracy and Google[16]—it remains to be seen if COPPA 2.0 will survive another round of bargaining in the House and ultimately be enacted as a federal law. With regard to the changes to the Final Rule, specifically, privacy experts note "the timing of the [F]inal [R]ule is uncertain following the Trump administration's stay of new regulations," and believe "the [F]inal [R]ule's future may hinge on the new administration's priorities — namely, whether [FTC] Chair [Andrew] Ferguson will revisit amendments he took issue with now that the administration paused the rule's publication."[17]

Moreover, in the absence of any legislative revisions to COPPA or a comprehensive federal privacy law[18]—or an omnibus privacy law which is industry agnostic and protects both children

---

personal information from users who are thirteen to sixteen years old without their consent. *Id.*

14 The Children's Online Privacy Protection Rule, referred to as the "COPPA Final Rule" or simply the "Rule," is the FTC's implementing regulation for enforcing COPPA, and it was last amended in January 2013. *See* 16 C.F.R. pt. 312 (2025).

15 Press Release, Fed. Trade Comm'n, FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data (Jan. 16, 2025) [hereinafter FTC Finalizes Changes], https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data [https://perma.cc/XKE4-J7YW]. The amendments to the Final Rule would include: (1) "[r]equiring opt-in consent for targeted advertising and other disclosures to third parties"; (2) requiring "operators to only retain personal information for as long as reasonably necessary to fulfill a specific purpose for which it was collected"; and (3) improving COPPA's Safe Harbor programs (self-regulatory programs that implement protections of the Rule) transparency. *Id.*

16 Am. Acad. of Pediatrics et al., *CDD Joins Coalition of Child Advocates Urging Senate E&C Committee Members to Advance COPPA 2.0*, CTR. FOR DIGIT. DEMOCRACY: DIGIT. YOUTH (June 23, 2025), https://democraticmedia.org/publishings/letter-cdd-joins-coalition-of-child-advocates-urging-senate-e-c-committee-members-to-advance-coppa-2-0 [https://perma.cc/R8UP-UNPV]; Trinity Velazquez, *Google Supports Louisiana Senator's Bill to Strengthen Online Privacy for Children, Teens*, YAHOO NEWS (June 25, 2025, at 07:08 PT), https://www.yahoo.com/news/google-supports-louisiana-senator-bill-140852940.html [https://perma.cc/E9CV-32GX].

17 Stacy Feuer, Maria Nava & Courtney Cox, *Top 5 Impacts of the New COPPA Rule*, IAPP (Feb. 14, 2025), https://iapp.org/news/a/top-5-impacts-of-the-new-coppa-rule [https://perma.cc/GC7W-JWCG].

18 *See* Lina M. Khan, Samuel A.A. Levine & Stephanie T. Nguyen, *After Notice and Choice: Reinvigorating "Unfairness" to Rein in Data Abuses*, 77 STAN. L. REV. 1375, 1378 (2025) ("The United States is the only advanced economy in the world with no comprehensive law protecting people's online privacy.").

and adults as consumers online—several states have in recent years passed their own children's privacy and/or consumer privacy laws. California, Virginia, Colorado, and Connecticut now provide statutory privacy rights, including access, deletion, and opt-out mechanisms, to residents including teens as young as thirteen.[19] In 2022, California also passed its Age-Appropriate Design Code (AADC), which imposes additional obligations on platforms likely to be accessed by children, including data minimization, high-default privacy settings, and impact assessments for new features.[20] Other states like Arkansas, Delaware, and Utah have also passed laws that target specific purported harms to children online, such as marketing restrictions, social media use, and age verification.[21] These are promising steps, but these state law efforts are "relatively new, infrequently enforced, and challenging for many families, lawyers, and even judges to understand."[22]

More critically, these state laws still rely heavily on "notice and choice" or "notice and consent"—a legal model that has been increasingly disavowed by scholars.[23] Under this model, privacy protection is presumed to occur when a user (or parent) is presented with a disclosure and affirmatively agrees. But as Daniel Solove argues, this approach turns privacy into a procedural formality, not a substantive right.[24] Takhshid further casts doubt on the use of consent-based models for children's privacy, particularly when using services associated with educational technology

19 For a more detailed discussion on the rise of state consumer privacy laws in the absence of a federal privacy law, see Mason R. Clark, *Consumer Privacy and the* Dobbs *Disruption*, 58 U. MICH. J.L. REFORM 1, 12–16 (2024).

20 *See* CAL. CIV. CODE § 1798.99.31 (West 2023).

21 *See* Steinberg, *supra* note 6, at 458–61 (describing the state legislative efforts—some successful and some failed—at protecting children's online privacy through a variety of mechanisms).

22 *Id.* at 461.

23 Several recent publications discuss the failures of notice and choice in U.S. privacy law. *See* Khan, Levine & Nguyen, *supra* note 18, at 1375 (arguing that "for much of its history, the [FTC] relied on self-regulation through a 'notice and choice' framework that left the public vulnerable in an era of rampant data collection and digital surveillance"); *see also* Takhshid, *supra* note 5, at 1455 (suggesting that privacy law should "move away from frameworks that seek to protect children's digital privacy by relying on notice and parental consent forms and instead advocate[] for the adoption of positive law to protect children's digital privacy"); Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 593 (2024) (claiming that "[t]he evidence of actual consent is nonexistent under the notice-and-choice approach").

24 Solove, *supra* note 23, at 599–601 (describing how the "choice" in notice-and-choice is "take-it-or-leave-it—either do business . . . or do not," privacy policies are often unreadable, and plaintiffs have few remedies for breach of privacy notices without FTC intervention).

(EdTech), artificial-intelligence-enabled tools, and voice- and facial-recognition tools.[25]

Parents are cast as the primary protectors of their children's digital privacy under existing state and federal privacy laws. Parents are the ones who download the apps, configure the devices, enter the birthdates, and, at least on paper, consent to data collection. Under COPPA, they are required to provide "verifiable parental consent" before websites or online services may lawfully collect data from children under thirteen.[26] Under state laws like the California Consumer Privacy Act (CCPA) and Virginia Consumer Data Privacy Act, they can exercise data subject rights (such as the right to opt-out of sale or sharing of personal information) on their child's behalf.[27] In theory, this structure places control in the hands of families. In practice, it places the burden there instead—one that most parents are ill-equipped to shoulder.[28]

This burden creates what this Article refers to as a "parent's privacy paradox."[29] Like the broader privacy paradox that describes users who say they value privacy but do not act to protect it, parents often express deep concern about their children's digital safety but are either unprepared to take meaningful action(s) to prevent privacy harms—such as consenting even though they don't understand the technology—or willing to accept privacy harms and provide their child's personal information in spite of

---

25 Takhshid, *supra* note 5, at 1420 ("In the era of EdTech and artificial-intelligence-enabled tools such as ChatGPT, and voice-and facial-recognition tools, parental consent can no longer meaningfully serve its traditional purpose of protecting the best interests of the child, particularly given the complexity of innovation and potential for breaches of privacy . . . ." (footnote omitted)).

26 15 U.S.C. §§ 6501–6506; 16 C.F.R. § 312.5 (2025).

27 CAL. CIV. CODE § 1798.120(c) (West 2023); VA. CODE ANN. § 59.1-577(A)(5) (2023).

28 *See* Steinberg, *supra* note 6, at 464–65. Here, Steinberg critiques the notion that parents are the gatekeepers of children's privacy, highlighting the possibility of conflicting interests between parent and child:

> It is important to note that there may be times where a child's interest and a parent's interest do not align regarding children's privacy and protection. While parents may want to protect children, young people have interests in autonomy and independence. Our legal system is ill equipped to give young people a meaningful voice when their interests do not match those of their parents.

Id. (citation omitted).

29 For an introduction to "the privacy paradox," see Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFFS. 100, 100–01 (2007); *cf.* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 1 (2021) (arguing that the privacy paradox is a "myth created by faulty logic" and is a reductive concept that does not account for the "vast, complex, and never-ending project" that is managing one's privacy).

understanding the technology.[30] A "parent's privacy paradox" is an extension of the privacy paradox which describes the disconnect between parental concern and parental capacity.

The reasons parents intentionally or unintentionally act against their children's privacy interests are manifold. Parents are busy. They are not privacy professionals. Many of them lack the time, training, or technical fluency to parse privacy policies.[31] And even if they want to opt out, they might not know how. Platforms bury privacy settings across multiple menus, use dark patterns to obscure opt-out options, and frame default tracking as necessary to the user experience.[32] Empirical studies confirm this disconnect.[33]

The discrepancy is not necessarily a reflection of parental apathy. It reflects a system that outsources legal compliance to the least empowered stakeholder in the data ecosystem. And when platforms default to parental opt-outs (rather than opt-ins), most families may end up accepting the status quo.[34] Behavioral economists have long shown that default settings carry outsized influence, particularly when users are fatigued or uncertain.[35] As children's data is silently collected through location tracking, browsing habits, and voice recordings, very little of these practices are disclosed, and almost none of them are explained to parents in plain language.[36]

---

30 *See* Takhshid, *supra* note 5, at 1421 (writing that even though parents may grant consent, they "are not sufficiently aware of the potential harms of online activities and their technological complexities to be able to meaningfully consent to them on behalf of their children"); *see also* Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839, 843–44 (2017) (describing how parents may intentionally or unintentionally violate their own children's privacy by choosing to share their children's personal information online).

31 Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1436–37 (2017) (noting that in the context of COPPA notice and parental consent requirements, "[c]onsumers frequently do not read or understand privacy policies").

32 WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 23–25 (2018) (discussing how design shapes user decision-making).

33 Elvy, *supra* note 31, at 1441 (noting that "[c]onsumers may want more privacy and control over their data . . . , but they may not know how to achieve this result," and citing empirical studies conducted by the Pew Research Center and the FTC that explore how consumers understand privacy policies and how companies overpromise privacy protections).

34 *See* Solove, *supra* note 23, at 601–02 (describing how "a remarkably low percentage of people opt out," even though opt-out mechanisms remain fundamental to emerging privacy laws in the U.S.).

35 Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. ON REG. 413, 416–17 (2015).

36 *See* FED. TRADE COMM'N, *supra* note 3, at i, 42; Michael Atleson et al., *AI and the Risk of Consumer Harm*, FED. TRADE COMM'N (Jan. 3, 2025),

Even well-meaning attempts to help parents can backfire. App store labels may disclose whether a product collects personal data, but rarely clarify what kind, how it is used, or who it is shared with. "Parental control" tools often block or restrict access without providing transparency about underlying data flows. As a result, parents conflate control with protection, assuming that if they've toggled the right content filters, then they've addressed privacy. But privacy isn't just about what children see. It's about who sees them and what can be done with the digital record of their behavior.

This is the heart of the parent's privacy paradox: The law expects parents to make meaningful, informed privacy decisions but gives them neither the visibility nor the infrastructure to do so. What looks like empowerment is often abdication disguised as agency.

This is not a call to exclude parents from the conversation. Some scholars have suggested that parents should be *less* involved in gatekeeping their children's privacy in order to give children a voice in their own decision-making.[37] But neither children nor their parents can bear the burden alone. This Article argues that a restructured pay-for-privacy (PFP) model—one that requires companies to provide parents with accessible and actionable privacy insights in the palm of their hands—could be a better solution than continued failed attempts under consent models.

This restructured model must be tailored specifically for children's digital privacy. The model is simple in concept: parents would pay a modest monthly fee—say, three to five dollars—for a regularly issued, mobile-accessible report that tells them what data has been collected from their child, by whom, and for what purposes. This report would also include interactive tools (like a toggle button) to opt out of behavioral targeting, restrict the sale of data, and delete specific categories of personal information. Think of it as a privacy control center for parents delivered on a smartphone and not buried in an app's website or privacy policy. Importantly, the PFP model does not replace legal obligations. It supplements them. Platforms would still be required to comply with COPPA, the AADC, and other applicable state consumer privacy laws like the CCPA, all of which require companies to

https://data.aclum.org/storage/2025/01/FTC_www_ftc_gov_policy_advocacy-research_tech-at-ftc_2025_01_ai-risk-consumer-harm.pdf [https://perma.cc/8KBN-TQ3J].

37 Steinberg, *supra* note 6, at 473 (writing that, among other reforms, the law should honor a child's right to privacy for various reasons, not least among them to protect children from parents' "[s]harenting," meaning the parents' posting of their child's personal information online).

have this kind of data on hand anyway.[38] The PFP layer simply packages existing compliance obligations (like data subject rights centers, opt-out toggle buttons, and transparency requirements) into a format that parents can read and use.

The PFP model draws inspiration from tools or requirements that already exist but are underutilized or inaccessible. Many companies now must respond to data subject requests under privacy laws like the European Union's General Data Protection Regulation (GDPR), the CCPA, and other emerging state privacy laws, that let their users view, correct, limit, or delete their data.[39] The PFP proposal envisions a streamlined, mobile-friendly tool that tells parents: *Here's what we've collected. Here's what we're doing with it. Here's what you can do next.*

To prevent abuse or inequity, the PFP model must be paired with regulatory guardrails. Companies would be prohibited from inflating prices, coercing families into paid plans, or punishing users who don't subscribe. Pricing caps and sliding-scale subsidies could ensure that the tool is accessible to low-income families.[40] The FTC would serve as the supervisory and enforcement agency, empowered to enforce penalties under its section 5 authority to prevent unfair or deceptive practices,[41] a power it may be more willing to wield given its recent interest in revising the COPPA Final Rule.[42]

---

38 COPPA requires operators of websites to provide, upon request by a child's parent, "a description of the specific types of personal information collected from the child by that operator" and to provide notice on the website of "what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information." 15 U.S.C. § 6502(b)(1)(A)(i), (b)(1)(B)(i). The AADC requires businesses that provide online products or services to conduct a Data Protection Impact Assessment which, among other things, includes documentation of the business's collection of children's personal information and the impacts and risks of such collection and subsequent data management practices. CAL. CIV. CODE § 1798.99.31(a)(1)(B)(i)–(viii) (West 2025). Finally, the CCPA requires businesses to provide both a right to know and a right to access the personal information being collected, used, sold, or disclosed by the business, as well as the purposes for which it is collected, sold, or shared. CAL. CIV. CODE § 1798.110.

39 Richard English, *Data Subject Access Requests (DSARs) for GDPR and CCPA Compliance*, DISCO: BLOG (Mar. 19, 2025), https://csdisco.com/blog/dsars-gdpr-ccpa-guide [https://perma.cc/BH58-67FU]; *see supra* note 19 and accompanying text.

40 *See* Elvy, *supra* note 31, at 1400. The price caps and sliding-scale subsidies could serve to prevent a PFP model that creates what Elvy describes as a "divide between those that can afford privacy and those that cannot." *Id.*

41 15 U.S.C. § 45; *see A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (July 2025) [hereinafter *A Brief Overview*], https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/EX2N-KPY5].

42 *See* FTC Finalizes Changes, *supra* note 15.

This is not a radical departure. Americans already pay for subscription-based digital services that offer enhanced control, fewer ads, or higher privacy, such as YouTube Premium, Apple's Private Relay, or Meta Verified.[43] The difference here is that the model would be child-centered and equity-aware. It would recognize that while the ideal solution is a substantial revision to federal privacy laws like COPPA that limits or outright bans the collection, use, and disclosure of children's data, the reality is that (1) this type of legislation is unlikely; (2) most parents are navigating a fragmented, underregulated digital landscape; and (3) companies are well-positioned—due to the data subject rights they must grant under emerging state privacy laws—to provide a report that helps parents understand their children's online activities.

Monetizing privacy raises innumerable ethical concerns, some of which this Article addresses in detail in the next section. Many scholars have warned that monetizing privacy risks creating a two-tiered system, one in which wealthier families can afford enhanced protections while low-income families cannot.[44] This concern is particularly urgent when applied to children. If privacy becomes a subscription-based service, the protections children receive will depend not on their needs or vulnerabilities, but on their parents' income and digital literacy.

This Article does not dismiss these critiques. A functional PFP model must be accompanied by strong regulatory guardrails to prevent coercion, ensure equity, and limit abuse. These guardrails include: (1) design restrictions; (2) proactive FTC enforcement; and (3) baseline protections for all. PFP services should be priced low enough (three to five dollars per month) that most families can reasonably afford them. Higher fees would disincentivize adoption and exacerbate inequality. Low-income families should receive access to PFP tools at reduced or no cost. This could be facilitated through school partnerships, Medicaid eligibility, or federal grants to nonprofit intermediaries. Companies offering PFP must be prohibited from manipulating users into

---

43 *See, e.g.*, *iCloud Private Relay & Privacy*, APPLE: LEGAL (Dec. 12, 2025), https://www.apple.com/legal/privacy/data/en/icloud-relay/ [https://perma.cc/3QQK-B7ZF]; *Stand Out with Meta Verified*, META, https://about.meta.com/technologies/meta-verified/ [https://perma.cc/W7JF-EFWH] (last visited Nov. 15, 2025).

44 Elvy, *supra* note 31, at 1402 ("Even when [low-income and minority] consumers obtain access to the Internet, they may be subjected to increased data collection and a lack of privacy and control with respect to their data unless they are able to pay for the products and services offered by PFP companies to minimize these concerns.").

upgrading via dark patterns,[45] misleading interfaces, or degraded default experiences. Companies may not withhold core privacy rights from users who decline to pay, a form of non-discrimination protection already seen in emerging state privacy laws like the CCPA.[46] PFP services must offer additive transparency and control and not just replace the rights that should be universal. By embedding these protections into the framework, the PFP model becomes a transitional tool that helps families navigate a complex digital world without waiting for additional legislation or resorting to a total privatization of data.

Moreover, the existence of a voluntary, regulated PFP system may exert pressure on companies to improve their free-tier offerings. Proactive FTC investigation and enforcement could expose disparities in treatment between paid and unpaid users, motivating platforms to converge toward higher standards of care. It can also further restrict behavioral advertising and mandate clearer data disclosures.

Under this proposal, companies offering PFP services would be required to register their tools with the FTC and submit periodic compliance reviews. These reviews would assess whether the PFP tool (1) satisfies design restrictions and requirements; (2) follows FTC guidance and enforcement; and (3) establishes baseline protections for all. The FTC would also establish complaint portals—both for parents and public-interest watchdogs—to report abuse.

This regulatory structure is not without precedent. The FTC has already demonstrated its capacity to supervise complex digital ecosystems. In 2019, the Agency imposed a $5 billion fine on Facebook (now Meta), and required detailed privacy program audits after a series of misleading practices were uncovered and a complete overhaul of Facebook's own internal privacy department structure.[47] The 2019 YouTube settlement likewise forced Google to change how it collects data from children, restrict per-

---

45 S. 1409, 118th Cong. (2023) (describing a dark pattern as a design practice that has "the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice in order to weaken or disable safeguards or parental controls").

46 Alysa Z. Hutnik, Aaron J. Burstein & Alexander I. Schneider, *The CCPA Non-Discrimination Right, Explained*, KELLEY DRYE (Apr. 29, 2020), https://www.kelleydrye.com/viewpoints/blogs/ad-law-access/the-ccpa-non-discrimination-right-explained [https://perma.cc/P5ZQ-29Q9].

47 Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook [https://perma.cc/JZQ3-6ES9].

sonalized ads on kids' content, and create a pathway for channel-level COPPA compliance.[48]

More importantly, the FTC has shown its willingness to evolve as the technology children use (and the privacy threats it creates) changes. In 2024, the FTC released a 6(b)[49] study of social media platforms, highlighting aggressive data harvesting from youth.[50] That same year, it updated the COPPA Rule to clarify that companies may not use age-gating to avoid liability and must provide clearer data disclosures and default settings for child-directed services.[51] The goal is not to offload privacy responsibilities onto the market, but to create infrastructure that works now while larger reforms remain politically stalled.

This vision of enforcement does not rely solely on federal intervention. State Attorneys General would retain their powers under state consumer protection laws and consumer privacy laws, and they could bring actions for deceptive or discriminatory PFP offerings. Nonprofit watchdogs, legal clinics, and privacy researchers would be encouraged to test and challenge offerings. Together, this would allow PFP to function not as a Band-Aid, but as a bridge with a regulated, transparent tool for families that connects a broken present to a more secure future.

The stakes could not be higher. The digital economy is not waiting for Congress to act. While lawmakers debate, companies are refining machine-learning models on behavioral data collected from children.[52] They are building advertising profiles, mapping social graphs, and recording location histories, all before a child has learned how to write in cursive (if that is even still required!).[53] Privacy harms are live and ongoing erosions of children's autonomy and psychological safety. Parents know this, but knowing is not the same as acting, especially in an ecosystem designed to resist action.

---

48 Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sep. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law [https://perma.cc/TGB5-FEGD].

49 *A Brief Overview*, *supra* note 41 ("Section 6 of the FTC Act provides another investigative tool. Section 6(b) empowers the Commission to require an entity to file 'annual or special . . . reports or answers in writing to specific questions' to provide information about the entity's 'organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals.'" (citing 15 U.S.C. § 46(b))).

50 FED. TRADE COMM'N, *supra* note 3, at i.

51 FTC Finalizes Changes, *supra* note 15.

52 *See* FED. TRADE COMM'N, *supra* note 3, at 72–73.

53 *Id.*

The PFP model proposed in this Article is, at best, a pragmatic solution in a broken system. It offers parents a chance to reclaim some control, not by decoding terms of service or clicking through endless menus, but by receiving a regular, visual report that tells them: *This is what we collected, this is how it was used, and this is what you can do about it.* Crucially, PFP only works if it is regulated and equitable. It must include a firm legal floor (no one should be penalized for not paying); sliding-scale subsidies for low-income families; a mobile-friendly design to meet users where they are; and active FTC and state-level enforcement to deter deception and abuse. If designed this way, PFP can function as a tool of empowerment. It can pressure companies to compete on transparency and usability. It can nudge families toward more active engagement. And it can fill the gap between what the law should require and what it currently allows.

This Article proceeds in three Parts. Part II explores the "parent's privacy paradox" and, while it critiques the failure of consent-based regimes in children's privacy law, it suggests that parents can still make choices about their children's digital privacy if they are better informed with easily accessible information. Part III analyzes how some companies, particularly those which exist outside of COPPA's purview, are technically and financially well-positioned to implement a regulated PFP model and how the model aligns with existing legal obligations and emerging consumer trends. And Part IV proposes a regulatory framework for PFP, focusing on equity, usability, and enforceability under FTC supervision and existing state privacy law. Together, these sections advance a single proposition: Children's privacy is a collective responsibility.

II. CAN (OR SHOULD) PARENTS MAKE PRIVACY CHOICES?

Parents are often the gatekeepers and the first line of defense for their children's digital privacy. They buy the devices, download the apps, set the passwords, and, under laws like COPPA, are expected to give "verifiable parental consent" before personal data is collected.[54] In theory, parents decide what data is collected, when, and by whom. In practice, however, parents only have the illusion of control. Parents are routinely overburdened (or intentionally misled) by consent forms and privacy policies. They are told they are in control, but the control is often

[54] 16 C.F.R. § 312.5(a)(1) (2025) ("An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children . . . .").

symbolic. As such, scholars have critiqued parental consent as the basis for protecting children's privacy.[55] This section agrees that parental consent cannot be the bedrock of children's privacy online for the very same reasons articulated by Takhshid, Steinberg, Solove, and many others. However, even if parental consent no longer serves as the foundation of children's privacy, it does not mean that parents cannot—or should not—still retain some decision-making authority. If parents are given frequent, easily accessible information about their children's online activity in the palm of their hands, and they can make decisions about that activity (such as by requesting the collector to delete the data) with one click on their mobile device, they can help mitigate against downstream privacy harms.

A. The Illusion of Consent

Most privacy interfaces are not designed for usability. They are designed for legal compliance and user attrition.[56] Platform interfaces routinely hide key privacy settings across multiple menus and use algorithms, data analytics, and/or artificial intelligence in their data processing to further obfuscate data collection practices.[57] Even though many platforms and devices offer parental controls, these tools often overwhelm parents and present a host of other problems for both parent and child.[58]

Scholars have recognized this problem for years. Hartzog and Solove have each critiqued the legal system's reliance on consent mechanisms and "notice-and-choice" regimes that are structurally designed to fail.[59] Not to mention, most companies are strongly incentivized to obtain consent, so they may make

---

55 *See* Takhshid, *supra* note 5, at 1417 (arguing that "under the common law tradition of protecting the best interests of the child, when it comes to protecting children's digital privacy, relying solely on parental consent is insufficient and ill-suited" and suggesting that common law privacy torts may "motivate companies to be more vigilant towards handling minors' data to avoid potential lawsuits"); *see also* Steinberg, *supra* note 6, at 464–65 (writing that parental consent sometimes intentionally or unintentionally harms children and robs them of their autonomy and independence).

56 HARTZOG, *supra* note 32, at 27–32.

57 FED. TRADE COMM'N, *supra* note 3, at 61–62.

58 Sara M. Grimes & Riley McNair, *Parental Controls on Children's Tech Devices Are Out of Touch with Child's Play*, THE CONVERSATION (July 6, 2025, at 08:51 ET), https://theconversation.com/parental-controls-on-childrens-tech-devices-are-out-of-touch-with-childs-play-257874 [https://perma.cc/LLF6-MKTF] (explaining that a study by the Family Online Safety Institute revealed parents don't use parental controls because they feel overwhelmed, and suggesting that parental controls present other problems such as a lack of risk awareness by children and poor communication between parent and child).

59 HARTZOG, *supra* note 32, at 60–61; Solove, *supra* note 23, at 601 (stating that "[t]he notice-and-choice approach has been savaged in academic literature").

special effort to manipulate or coerce their customers—children and adults—into providing it.[60]

Parental consent in the modern privacy landscape operates more like a waiver than an informed choice. And because many privacy policies are vague or incomplete, parents are often only minimally aware that data is even being collected, sold to brokers, or shared with unknown third parties.[61] The parent's privacy paradox, then, becomes more profound when one considers the scope and opacity of modern data collection. Children's devices track browsing history, app usage, geolocation, search queries, biometric signals, and even facial expressions—often without any ongoing disclosure and with the assistance of emerging artificial intelligence capabilities.[62] Many of these activities are justified by platforms under broad headings like "functional data" or "performance analytics," which are rarely explained in concrete terms.[63] This makes meaningful oversight nearly impossible. The average parent, even one with a college education, cannot reasonably be expected to navigate a privacy regime that assumes such a high level of privacy literacy. Yet that is exactly what the current system demands.

But altering the parental consent model is no small task. The concept of consent has long served as the backbone of American privacy law.[64] If a company tells you what it is doing with your data and you agree, that agreement legitimizes the practice. This logic extends to COPPA, which prohibits the collection of personal data from children under thirteen without "verifiable parental consent."[65] It also underlies the broader consumer privacy laws passed in California, Virginia, and other states, which permit data collection and sharing so long as users are given notice and an opportunity to opt out.[66]

But as countless privacy scholars have shown, consent in this context is largely legal fiction.[67] In the children's privacy

60 Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1489 (2019).

61 Solove, *supra* note 23, at 622 (asserting that "[w]hat people are told in privacy notices are vague meaningless statements" which do not describe internal governance programs or "how well privacy is integrated into the design of products and services, among many other things").

62 FED. TRADE COMM'N, *supra* note 3, at v–vi.

63 *Id.* at 27.

64 Solove, *supra* note 23, at 596.

65 16 C.F.R. § 312.5 (2025).

66 *See* CAL. CIV. CODE § 1798.120 (West 2023); VA. CODE ANN. § 59.1-577(A) (2023).

67 Solove, *supra* note 23, at 598–600.

context, this fiction becomes even more absurd. Children cannot consent, and parents are asked to consent on their behalf, often without understanding the full scope of what they are authorizing.[68] Although there have been recently enacted state consumer privacy laws and changes to the COPPA Final Rule, as discussed above, these laws have so far failed to require companies to provide intelligible summaries of exactly what a parent is consenting to on behalf of their child. And once consent is given, it is rarely revisited. Unlike data processing under the GDPR, which often requires renewed or contextual consent,[69] COPPA consent is typically a one-time event. Data collection continues indefinitely unless the parent actively intervenes, which, as noted earlier, most do not. This creates a regulatory sleight of hand in which companies claim legal compliance by offering notice and obtaining consent, but in practice, the parent neither notices nor consents in any meaningful way. Daniel Solove refers to this as "murky consent"—a model in which the existence of a checkbox or policy is treated as proof of agreement, regardless of actual comprehension or voluntariness.[70] He argues that the law must shift away from consent as a universal solution and toward substantive privacy protections that apply regardless of whether a user clicks "I agree."[71]

Children's data deserves nothing less. If it is acknowledged that parents are overwhelmed, interfaces are deceptive, and privacy policies are unreadable, then it must also be acknowledged that consent alone cannot carry the regulatory burden. Any privacy regime that depends on informed parental decision-making must first give parents the tools, time, and support to make decisions that matter. Because even some who criticize consent-based regimes acknowledge that individual choices will (and should) nevertheless be made:

> Respect for people's autonomy gives them space to make informed choices based on their determination of what is in their own self-interest. The problem is that for privacy, people's decisions are often highly manipulated and ill-informed. . . . Even accepting that these problems can never be surmounted, respect for autonomy involves

---

68 Takhshid, *supra* note 5, at 1421 ("Today, across the internet from online gaming to other entertainment apps, companies rely on parental consent . . . . [P]arents themselves are not sufficiently aware of the potential harms of online activities and their technological complexities to be able to meaningfully consent to them on behalf of their children.").

69 Commission Regulation 2016/679, art. 7, 2016 O.J. (L 119) 37 (EU). Under article 7 of the GDPR, consent must be freely given, specific, informed, and unambiguous. *Id.* It also must be given each time a company creates a new use or purpose for the data. *Id.*

70 *See* Solove, *supra* note 23, at 593–94.

71 *See id.* at 632–33.

> preserving space for individual choice, as unsound and compromised as it often is.[72]

B. Solutions Without Consent

What are scholars, lawmakers, and regulators proposing now to address the insufficiency of consent-based privacy? There is a plethora of proposals, some of which are industry specific (e.g., EdTech v. social media) but almost all of which are in favor of abandoning parental consent as the bedrock for children's privacy. For example, Takhshid argues that, in the EdTech sphere, COPPA's "verifiable parental consent" mechanism invites oversimplified (and overabused) parental consent forms that do not address other uses of children's data; creates a heavy burden for parents to access and understand school records; and violates public policy by allowing companies to use the "parental-consent apparatus" to put the "child's privacy rights at the mercy of a tech company."[73] Takhshid expressly rejects the argument that parental consent for EdTech data collection is equivalent to their right to make decisions concerning the care and control of children under the Fourteenth Amendments' Due Process Clause, instead claiming that parents are not exercising their right to shape their child's education when they make uninformed choices about such data collection.[74] Her solutions included both "tough regulation," which could have companies "competing . . . by promoting . . . top-notch privacy-protection tools rather distracting apps and colorful games,"[75] and exploration of common law privacy tort lawsuits.[76]

Steinberg, on the other hand, supports comprehensive federal legislation,[77] arguing that "[c]hildren's online privacy law is in disarray."[78] She suggests that lawmakers should use the California AADC[79] as a model for children's privacy legislation in the U. S. for a variety of reasons, noting that it incorporates many in-

---

72 *Id.* at 628.

73 Takhshid, *supra* note 5, at 1442–46.

74 *See id.* at 1446–47.

75 *Id.* at 1448–49.

76 *See id.* at 1449.

77 *See* Steinberg, *supra* note 6, at 467.

78 *Id.* at 443.

79 CAL. CIV. CODE § 1798.99.31 (West 2025); *see also* Rory Sweeney, *The California Age-Appropriate Design Code Act*, CAL. LAWS. ASS'N (Oct. 16, 2023), https://calawyers.org/privacy-law/the-california-age-appropriate-design-code-act/ [https://perma.cc/RJ72-AWMC] (detailing that this law is designed to "promote a 'high-level' of privacy by default," prohibit profiling, precise geolocation collection, and harmful design tricks like dark patterns, and "reinforc[e] data minimization and purpose limitation principles").

ternational principles[80] and sufficiently narrows the scope to larger corporations to preempt corporate interest pushback.[81] Perhaps more novel, however, is Steinberg's argument against recent state children's privacy laws in Arkansas, California, Delaware, Texas, and Utah[82] that rely on the parental consent mechanism, citing concerns about children's autonomy and their civil rights.[83]

Legal scholars and commentators have long observed that privacy harms are disproportionately concentrated among low-income and marginalized communities.[84] The consent-based privacy regimes (particularly consent mechanisms present in old models of PFP, such as the privacy-discount plans)[85] fall hardest on families with the fewest resources because privacy-discount plans "may force consumers to make difficult choices between privacy and other necessities."[86] Even if we assume that all parents want to protect their children's digital privacy—and the data suggests they do—the ability to do so varies dramatically. Not all families have equal access to information, time, tools, or financial flexibility. As a result, a parent may intentionally or unintentionally sacrifice their children's data privacy in ways that could prove harmful down the road. Elvy writes,

---

80 *See* Comm. on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, at 3–6, 8–11, 14–16, 19, U.N. Doc. CRC/C/G/25 (Mar. 2, 2021); *see also* Steinberg, *supra* note 6, at 469–74 (highlighting key provisions of this convention).

81 Steinberg, *supra* note 6, at 468–69.

82 *See id.* at 443, 458–61.

83 *See id.* at 464–65 ("While parents may want to protect children, young people have interests in autonomy and independence."); *see also* Natasha Singer, *Silicon Valley Battles States over New Online Safety Laws for Children*, N.Y. TIMES (Feb. 1, 2024), https://www.nytimes.com/2024/01/31/technology/social-media-free-speech-netchoice.html [https://perma.cc/64AU-5LVW] (suggesting parental consent could keep young people from reproductive health and/or gender identity resources).

84 *See* Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1142 (2018) ("Nowhere is that power disparity [between government and corporate power over those they surveil] more evident than the State's surveillance of society's most vulnerable members."); *see also* Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1393–94 (2012) (describing how low-income Americans experience privacy differently than middle- and upper- class Americans); Nathan Newman, *How Big Data Enables Economic Harm to Low-Income Consumers*, HUFFPOST (Nov. 15, 2014), https://www.huffpost.com/entry/how-big-data-enables-econ_b_5820202 [https://perma.cc/9QL2-YSCB] (explaining how big data platforms use low-income consumer data to target vulnerable consumers with "economically exploitative services").

85 Elvy, *supra* note 31, at 1391–92 (describing privacy-discount programs as those in which "consumers also pay for privacy controls by incurring higher fees. However, unlike in the privacy-as-a-luxury model, consumers are encouraged to relinquish their privacy and data through the use of discounts.").

86 *See id.* at 1405.

> Eventually information about a child's behavioral status, preferences, experiences and other sorts of child-related data could be used to determine the types of opportunities that children receive during childhood as well as negatively impact their adulthood lives and prospects. Thus, rising data quality and quantity and increases in the digital footprints of children combined with new platforms for collecting and sharing household (and child) data may exacerbate privacy concerns for children.[87]

These disparities may be replicated when children's data is at stake. Families with fewer resources may be more likely to allow companies to monetize children's data so the families can afford necessities.[88] By contrast, wealthier families are more likely to pay for subscriptions that promise privacy, offer enhanced settings, or restrict third-party tracking.[89] This creates a stratified digital environment where privacy is a premium feature and surveillance is the default for everyone else.

It is clear from scholarship and recent legislative and regulatory activity that consent and/or notice-and-choice regimes are falling out of favor among privacy advocates because user consent is rarely well-informed and is often manipulative (at best) or coercive (at worst), particularly for those in underrepresented communities. The risk, of course, is that any privacy model—especially a PFP model, as this Article considers—could also entrench inequities. If enhanced transparency and data control are only available to those who can afford them, the children most vulnerable to exploitation will be the least protected. The PFP market "not only confirms privacy's value to users of a company's products and services but also implies the existence of lower-tier options for those unable to afford these premium privacy protections."[90]

Any serious effort to address children's privacy must confront these structural inequities. And even under the PFP model this Article proposes, parents—even parents who are able and willing to pay for privacy reports on their children's data—cannot be solely responsible for protecting children's privacy. A reimagined PFP model must be paired with a regulatory regime specifically designed for the realities of all families, not just those who can afford privacy. For this reason, any PFP model must be paired with the following regulatory guardrails: (1) design restrictions; (2) proactive FTC enforcement; and (3) baseline protections for all,

---

87 *Id.* at 1408.

88 *See id.* at 1407.

89 *See id.* at 1402.

90 Jeffrey L. Vagle, *Privacy's Commodification and the Limits of Antitrust*, 77 ARK. L. REV. 51, 72 (2024).

regardless of payment. Without these safeguards, PFP becomes a vehicle for exclusion instead of a tool for empowerment.

C. PFP as a Practical Solution

The PFP model proposed in this Article is not a cure-all. It is not a substitute for comprehensive federal privacy legislation, any sort of structural reform of coercive data collection practices, or the total abandonment of consent or notice-and-choice privacy frameworks. This Article agrees with scholars who see "privacy self-management" and rights to notice, access, and consent as "laudable goals" that nonetheless "hid[e] bad practices behind a veil of user consent based on little or no understanding of what is being consented to."[91] However, given that federal legislation seems unlikely, structural reform is, by its nature, a long process, and the most recent privacy laws at the state and federal level continue to uphold consent-based regimes, a *reimagined* PFP model—one in which (1) consent is irrelevant, and (2) parents are paying for one-click accessibility and control made possible by their contributions—could ignite a market-based solution.

In the best-case scenario, the PFP model this Article proposes would serve as a bridge away from the ruins of consent-based regimes and toward the control over information envisioned by privacy advocates. It could address two scoping problems with COPPA—that it only applies to children under thirteen and to online apps and services "directed to children"—by encouraging companies who have both under- and over-thirteen users to generate revenue from parents of both demographics.[92] The PFP model would also build on some of the more recent rights afforded to consumers, generally, under state privacy laws—such as the right to access and delete data and the right to opt-out of data sharing—and present meaningful options to parents in the palm of their hands.

Under the proposed PFP framework, parents would pay a fee to receive a monthly privacy report delivered via mobile app or email that outlines: what data was collected from their child;

---

91 *Id*. at 78.

92 15 U.S.C. §§ 6501–6502; *see* Zoë MacDonald, Note, *Defending Children's Data Privacy: Strategies for the 21st Century*, 76 U.C. L.J. 589, 594 n.22 (2025) (citing Eva Rothenberg, *Meta Collected Children's Data from Instagram Accounts, Unsealed Court Document Alleges*, CNN (Nov. 26, 2023, at 15:12 ET), https://edition.cnn.com/2023/11/26/business/meta-collecting-data-children-facebook/index.html [https://perma.cc/WGZ8-YKGD]) ("Instagram explicitly prohibits children under thirteen from creating accounts, meaning COPPA would not apply; but in reality, there are many users under age thirteen on the social media app and one lawsuit alleges that Instagram is aware of that fact and still collects user data without complying with COPPA.").

which companies collected it; whether it was shared or sold; what privacy choices are available (e.g., deletion, opt-out, restriction); and a one-click option to exercise those controls. All of this would be regulated by the FTC, which would establish minimum usability standards, audit compliance, and enforce penalties under its section 5 unfairness and deception authority.[93] Companies would be required to offer a no-cost baseline tier of privacy protection, and pricing for enhanced PFP services would be capped at a low, family-friendly level (e.g., three to five dollars per month), with subsidies for low-income households.

The goal of the PFP model and the monthly privacy report is not to turn privacy into a product. The goal is to make some of the rights mentioned above and afforded to consumers in various states[94] clearly presented to and easily exercised by any parent who pays for it. This begs the question: If those rights already exist in some states, why should parents have to pay for it? There are several reasons.

First, even though all the state privacy laws have opt-in consent requirements for collecting personal information from minors, the majority of them only require this consent for "sensitive data" collected from users thirteen or younger.[95] Second, none of those state privacy laws provide a private right of action for violating these rights—parent, child, or otherwise.[96] And third, recent enforcement reports across the states show that many states have not filed any complaints enforcing their laws, and "many consumers don't yet understand the finer points of submitting a violation complaint."[97]

The state consumer privacy laws thus create similar scoping problems and have yet to have any meaningful enforcement. Regarding the consumers' ability to understand how to submit a rights request, this problem echoes the problem with notice-and-

---

93 *See* 15 U.S.C. § 45(a)(1).

94 *See* INT'L ASS'N OF PRIV. PRO., US STATE PRIVACY LEGISLATION TRACKER 2025: COMPREHENSIVE CONSUMER PRIVACY BILLS (2025), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/3CXY-PBD9]. There are currently nineteen state consumer privacy laws in the U.S. *Id.* All nineteen states provide their residents the right to access what information has been collected about them and delete that information. *Id.* All but two states also provide the right to correct the information collected and opt out of the processing of personal data for profiling and/or targeted advertising purposes. *Id.*

95 *Id.*

96 *See id.*

97 Caroline Kibby, *Emerging Trends, Insights from Public Enforcement of US State Privacy Laws*, IAPP (June 30, 2025), https://iapp.org/news/a/emerging-trends-insights-from-public-enforcement-of-us-state-privacy-laws [https://perma.cc/3QTL-D2DJ].

choice as articulated above. Most parents interact with digital services through their smartphones while managing competing obligations. They need privacy tools that are designed for real-world parenting rather than web-based dashboards that assume hours of free time and technical fluency.[98]

By offering a recurring, digestible report and a centralized control interface, PFP can reduce the friction that discourages privacy-protective behavior. This matters in a parental context because rather than expecting a parent to scour each app's privacy policy or locate obscure settings, the PFP tool can surface key risks and offer one-click solutions regardless of any (uninformed) consent granted. The PFP model also introduces competitive pressure. If companies are required to disclose their data collection practices in plain terms each month, and parents begin comparing reports across platforms, the most privacy-invasive services may face market pushback. Parents may choose apps or devices with stronger protections, incentivizing companies to improve their default designs. In this way, PFP could promote privacy as a product differentiator. Of course, the PFP model will require buy-in from large tech companies, something that has proven to be difficult to obtain in many other attempts to regulate children's privacy.[99]

Still, no one should confuse a market tool with a rights-based framework. PFP is valuable precisely because the rights-based framework is currently weak. Until Congress enacts a federal children's privacy law with substantial improvements to COPPA or regulators clamp down hard on Big Tech and social media companies (or both), parents will remain the gatekeepers of their children's privacy. And as this Part has shown, they are currently defending the gates without much armor.

The failure of current privacy law is as much conceptual as it is technical or procedural. By currently placing the burden of privacy protection on parental consent mechanisms, parents are expected to serve as digital gatekeepers in an environment designed to overwhelm them, while companies and lawmakers escape accountability by insisting that the tools to exercise any

---

98 *See id.* In the article, Kibby describes how Texas consumers were confused about how to exercise their rights because "the method varies from [company to company]." *Id.* Kibby further notes that "consumers and businesses alike aren't quite sure yet how to adapt to the rights and responsibilities created by privacy laws." *Id.*

99 *See Big Tech's Scramble to Stop Child Safety Laws*, TECH TRANSPARENCY PROJECT (May 3, 2023), https://www.techtransparencyproject.org/articles/big-techs-scramble-to-stop-child-safety-laws [https://perma.cc/KC82-Y49K].

sort of control or choice exist, even if they are impossible to use. A better approach begins by recognizing that children's privacy is a collective public interest, not a private task.[100] Just as society regulates toy safety, food labeling, and school curricula to protect child development, it must also regulate data collection practices that shape how children are profiled and marketed to. A child's digital life should not be determined by their parents' tech savvy or disposable income. It should be supported by infrastructure that makes active participation possible.

The broader ambition of the PFP model is not just to give parents rights they should (or do) already have, but to redesign the structure of responsibility. It suggests that children's privacy should be shared between parents, companies, and regulators and sustained by systems that are accessible and responsive. By reframing privacy as a collective responsibility, PFP challenges the notion that protecting children's privacy is dualistic, where you can either strip parents and children of autonomy and place all responsibility on the companies to engage in ethical data collection practices, or you can place the burden solely on parents to exercise what little rights they do have based on information that is inaccessible and through mechanisms they do not have time or understanding to navigate. It acknowledges that structural problems require structural solutions, and that meaningful child privacy requires participation from all stakeholders. The next Part of this Article turns to the other stakeholders—the companies and the FTC—and outlines how to implement PFP with fairness, transparency, and enforceability.

III. A PFP MAKEOVER: CORPORATE ACCOUNTABILITY

A. Platforms are Positioned to Act

If parental consent is no longer a reliable foundation for children's data protection—and Part II argued it is not—then responsibility must shift upstream. The natural candidates are the platforms and service providers that design, deploy, and profit from the data collection infrastructure. These companies are best positioned to implement real-time privacy protections because they control the data pipelines, the user interfaces, and the economic incentives that shape behavior.

---

100 *See* Takhshid, *supra* note 5, at 1445 (proposing reforms to parental consent in the EdTech space by arguing that children's privacy is a collective public interest, not a private task).

Platforms already collect and process vast volumes of data on children, often with remarkable precision. In the average household, a single tablet or smartphone app may track usage metrics, device identifiers, browsing history, purchase patterns, location data, behavioral engagement, and biometric inputs like voice or facial recognition.[101] These data flows are rarely disclosed in meaningful detail to parents, yet platforms manage them in real time for internal purposes, and they even use certain data to produce targeted advertising and algorithmic optimization designed to keep them engaged.[102] If they can deploy infrastructure to monetize children's attention, they can certainly deploy infrastructure to help parents monitor it.

From a technical standpoint, most large platforms already possess the architecture needed to implement a PFP system where revenue from parents helps fund the generation of a monthly privacy report. They have user authentication systems, mobile push notifications, granular tracking dashboards, customer segmentation tools, and API endpoints that allow for data reporting and user-specific customizations. Companies like Google and Apple already offer parents partial visibility through tools such as Google Family Link and Apple Screen Time, which include device-level summaries of usage and controls over app permissions.[103] These tools, however, are siloed, underadvertised, and focused more on screen time than data collection. A PFP tool could draw on these existing capabilities but shift the emphasis toward ongoing data transparency and control.

Financially, platforms are also incentivized to offer differentiated privacy services. Scholars have shown that privacy has already become a product differentiator in some consumer products, such as the difference in pricing for an Apple iPhone versus an Android smartphone.[104] Apple promotes its devices as privacy-forward by default and has adopted App Tracking Transparency (ATT) policies that signal a growing market awareness of privacy

---

101 *See* FED. TRADE COMM'N, *supra* note 3, at 25–26.

102 *See* Michal Lavi, *Targeting Children: Liability for Algorithmic Recommendations*, 73 AM. U. L. REV. 1367, 1376–77 (2024) (describing how Facebook used inferences about minors' moods and insecurities to target advertisements to them "when [Facebook's] algorithm believed they were most vulnerable").

103 *See Use Screen Time on Your iPhone and iPad*, APPLE (Sep. 15, 2025), https://support.apple.com/en-us/HT208982 [https://perma.cc/NEA4-CTZG]; *Help Keep Your Family Safer Online*, GOOGLE: FAMILY LINK, https://families.google.com/familylink/ [https://perma.cc/Q7FS-CE8F] (last visited Dec. 23, 2025).

104 *See* Elvy, *supra* note 31, at 1400–01.

preferences.[105] This commercial reality suggests that platforms are not only capable of monetizing privacy, but that they are already doing so.

Many platforms are also well-positioned to provide monthly privacy reports because they must have the necessary data anyway under the emerging state privacy laws mentioned above. While these laws currently require these disclosures only upon request and not on a regular schedule (again, as a reflection of notice-and-choice), they nonetheless require companies to maintain detailed logs of how user data, including children's data, is processed. These laws could form the basis for a reporting infrastructure that could be repurposed or extended automatically to parents of children who choose to pay for the report in any jurisdiction, not just one in which the state legislature has passed a privacy law. Put simply, many companies—or perhaps, the most problematic companies, like social media conglomerates and streaming service providers—have the infrastructure to generate the monthly privacy report quickly and accurately, and they will have additional revenue to provide it automatically to any parent who pays for the report.

But just because these companies are well-positioned to provide these monthly privacy reports through the PFP model, the model cannot be left to self-regulation without effective regulatory oversight. In fact, privacy "self-regulation," generally, has been noted by the FTC to be a failure.[106] The PFP model would still require a regulatory framework that ensures these services are oriented toward children's privacy and equitable for all parents and children. The FTC's role in regulating the PFP model is discussed more in Part IV.

Critics may argue that giving companies more control over privacy delivery will only exacerbate the power discrepancy between consumer and company and entrench what Vagle and others have described as "information asymmetries."[107] Vagle suggests:

---

105 *See Privacy. That's Apple.*, APPLE: PRIVACY, https://www.apple.com/privacy/ [https://perma.cc/96PF-Q2D8] (last visited Dec. 23, 2025).

106 *See* Khan, Levine & Nguyen, *supra* note 18, at 1406.

107 Vagle, *supra* note 90, at 78 (describing the "click to agree" on terms of service as an example of "[p]rivacy-related information asymmetr[y]," wherein the user has little to no understanding of what they just consented to while the company ostensibly knows exactly what it allows them to do with the data collected); *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1683 (1999) (describing an early iteration of information asymmetry as the "knowledge gap" between data processors and individuals trying to exercise a privacy choice, and how "[t]he result of this asymmetrical knowledge will be one-sided bargains that benefit data processors").

> The growing spectrum of individual privacy harms continues to be documented as new circumstances arise, new technologies are developed and deployed, and as our understanding of all of the above evolves, a thread that runs throughout the sources of these injuries is the relationship between privacy and power. The power dynamic between the collectors of information and those from which it is collected is quite one-sided, where individuals are disempowered by information asymmetries, technology black boxes, and the lack of any real choices when it comes to privacy protections.[108]

But PFP does not necessarily grant platforms more control. This Article's model demands more accountability: The platforms must provide accessible data automatically, and they can't evade that obligation like they often do under state consumer privacy laws. It asks them to use their existing infrastructure to serve a public goal and help protect children from downstream privacy harms. If companies can use engagement dashboards to optimize ad revenue, they can also use them to generate monthly privacy reports for parents. The platforms are already collecting the data. They already have the infrastructure. They already differentiate based on privacy. What they lack is a legal, ethical, and enforceable obligation to put these tools to work for families. The PFP model—designed with the parent in mind but implemented by the platforms—offers a viable path forward.

The monthly privacy report would have to be accessible. In privacy terms, accessibility may translate to "transparency." But transparency in privacy law is tricky. Too much information (like a long privacy policy or the terms of use as described by Vagle above) can overwhelm a user, but a "very simple notice can't accurately describe many of the intricate ways that personal data is processed."[109] Various privacy laws in the U.S. and abroad typically require privacy policies or other notices be written in "clear and plain language" or be "reasonably accessible."[110]

Unlike privacy policies, terms of use, or even concisely written consents, the monthly privacy report would deliver a recurring snapshot of how a child's data was processed over the past month. It would summarize, in natural language and visual form, what types of data were collected (such as location, biometric, browsing history, or interactions), which entities collected it (specific app names or third-party services), and for what purposes (like advertising, analytics, content recommendation, or

108 *Id.* at 85.
109 Solove, *supra* note 23, at 617.
110 *Id.* at 616.

feature customization). It would also flag any high-risk behaviors—such as passive listening, behavioral profiling, or sale of data to brokers—and provide the parent with one-click options to delete, restrict, or opt out.

Crucially, this report must be delivered through channels parents already use, such as push notifications on mobile apps, monthly text or email alerts, or integration with other platforms like Google Family Link or Apple Screen Time. Expecting parents to log into a web portal and navigate nested menus is a recipe for disengagement. Design must meet the parent where they are (and, in my experience, parents are usually tired, busy, and multitasking until they have hit peak sensory overload).

In privacy terms, the monthly privacy report should not be "frictionless"[111] but rather should be a recurring report that says: *This is what we have done with your child's data. Click here to change that.* The monthly privacy report adapts to a child's evolving digital life. It captures new app installations, changes in data-sharing practices or data sharing partners, and/or shifts in behavioral patterns over time. For example, if a child begins spending more time on a platform that intensifies ad targeting, the report can flag that change and alert the parent. This proactive alerting creates a feedback loop that enhances both awareness and control, something virtually absent from the current consent-based regime, particularly on social media platforms and streaming services, which rely on frictionless consent to continuously collect and share a child's data.

Technically, such reports are not hard to generate. Platforms already track every relevant metric for internal use.[112] They know which apps are opened, how long they're used, what information is shared, and which third parties are involved.[113] These data pipelines already feed advertising analytics, product development, and machine learning models.[114] A report tool would

---

111 William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 15 (2013). William McGeveran defined "friction" as "the forces that impede individuals from disclosing personal information when they use online services." *Id.* For example, friction could be the number of boxes one must check or webpages one must navigate through before providing consent to share certain information. *Id.* at 15–17. Frictionless sharing, on the other hand, could be Netflix sharing all videos someone has watched with third parties after they consented just one time for one particular video. *See id.*

112 *See* BUREAU OF CONSUMER PROT., FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT 12–14 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800+Dark+Patterns+Report+9.14.2022+-+FINAL.pdf [https://perma.cc/M35A-KCCX].

113 *See id.* at 16–17.

114 *See id.* at 35.

simply repurpose that infrastructure to surface those insights for parents, not just advertisers.

A key challenge is standardization. As discussed above, the current state consumer privacy laws are struggling with standards for identity verification, processes for submitting rights requests, and other requirements under those laws.[115] If each platform creates its own version of the monthly privacy report, inconsistency will undermine usability. Policymakers or regulators like the FTC could develop reporting standards akin to the FDA's Nutrition Facts label or financial credit disclosures so that data categories and rights icons or toggle buttons are uniform across platforms and avoid the historical problems with various consent requirements and language.[116] For example, a red-yellow-green visual scale might signal privacy risk levels, while boldface toggle buttons[117] could highlight the rights associated with that data. Standardization would ensure comparability and reduce cognitive load.

Parents should be able to contextualize what matters in the monthly report, even if they don't fully grasp what exact data was collected or how that may impact their child. For instance, instead of reporting that "third parties may receive anonymous identifiers," the report might state: *Your child's location data was shared with four companies for advertising purposes. You can restrict this here*. Or: *This app collected facial recognition data to personalize filters. This is uncommon and may carry additional privacy risks*. Parents should be told not only what happened, but why it matters and what they can do. This model would benefit platforms as well. Companies that adopt a clear, usable privacy report could build trust, reduce customer service burdens, and position themselves as family-friendly brands. They would also reduce legal exposure. The FTC and state Attorneys General increasingly view vague or deceptive privacy disclosures as unfair or deceptive under section 5 of the FTC Act.[118] A month-

115 *See* Kibby, *supra* note 97.

116 *See* Solove, *supra* note 23, at 638.

117 *See id.* at 615 (noting that the California Consumer Privacy Act requires a conspicuous toggle button that users may click to opt out of a company's selling or sharing of personal information, but arguing this "fail[s] to guarantee that the privacy notices are read").

118 *See* 15 U.S.C. § 45(a)(1). See Mobilewalla, Inc., File No. 202-3196 (F.T.C. Jan. 14, 2025), and Gravy Analytics, Inc., File No. 212-3035 (F.T.C. Jan. 14, 2025), for how the FTC approved consent orders prohibiting Defendants from collecting, using, or selling location data without clear and conspicuous notice to, and affirmative express consent from, consumers after determining Defendants had misleading privacy disclosures.

ly privacy report that is uniform and consistent could serve as affirmative evidence of compliance.

Moreover, this approach complements legal notice requirements. Just as nutrition labels do not replace ingredient lists but distill the key ingredients in a standard American's diet, a monthly privacy report would distill privacy disclosures into an intelligible, consistent format. It can also serve as a tool for enforcement and parental redress when paired with backend access logs and audit trails. Misrepresented data practices in a report could become a potential basis for regulatory action.

Ultimately, the monthly privacy report transforms privacy from a one-time interaction into an ongoing conversation. It brings visibility to invisible processes. It equips parents with actionable intelligence. And it reshapes the role of the platform from passive collector to active participant in data stewardship. This ensures privacy is a shared responsibility.

B. Equity in the PFP Ecosystem

A PFP system must be more than a technical feature or market offering. It must be designed from the outset to serve families equitably, or else it risks deepening the digital divide it claims to bridge. As Part II explained, the most vulnerable children are often those whose parents have the least access to privacy-enhancing tools due to cost, language, education, time, or trust. Any viable PFP framework must confront this reality and not reinforce it.

The first and most obvious concern is cost. If PFP services require a monthly payment—no matter how small—some families will be excluded. These families may already be facing economic pressures around rent, food, and health care. Although privacy is important, its cost should not force consumers to choose privacy over essentials.[119] But the concern about privacy as a luxury good, at least as described by Elvy, is related to privacy discount plans or services.[120] The monthly privacy report would not be offered as a sort of privacy discount but as an additional transparency and choice mechanism for parents.

To address this, PFP systems must offer a free baseline level of protection. No family should be required to pay in order to access basic tools for monitoring and controlling their child's data. The paid tier, if adopted, would offer enhanced features like the

119 *See* Elvy, *supra* note 31, at 1405.

120 *See id.*

monthly privacy report. This mirrors the approach taken in other regulated contexts. For instance, federal law mandates that all Americans are entitled to one free annual credit report from each major bureau; premium services like credit monitoring or identity theft protection can be purchased separately.[121] Similarly, broadband providers offering government-subsidized internet under the Affordable Connectivity Program are not permitted to gate essential access behind premium paywalls.[122] The same logic should apply to children's data.

But financial barriers are only part of the problem. Educational and cultural barriers are equally problematic. A 2018 study demonstrated that privacy policies for more than sixty youth-oriented apps in the Apple and Google Play Stores were written at a reading grade level well above the average reading level of U.S. adults.[123] Interfaces are dense and buried within app settings that require digital literacy to navigate.[124] For families with lower digital literacy, privacy policies do little to warn them of privacy- and security-related harms.[125] Those from lower-income communities may also be vulnerable because of cultural privacy practices.[126] The design of the monthly privacy report must therefore prioritize linguistic and cultural inclusivity, plain language communication, and visual aids (such as icons, alerts, and risk indicators) that support understanding across literacy levels.

Usability is another critical factor. Time-strapped parents need tools that work without extensive setup, tech support, or ongoing calibration. The PFP system must be plug-and-play, meaning it integrates with existing devices and requires minimal

---

121 Fair Credit Reporting Act, 15 U.S.C. § 1681j.

122 *Affordable Connectivity Program*, FED. COMMC'NS COMM'N, https://www.fcc.gov/affordable-connectivity-program [https://perma.cc/M297-CD9M] (last visited Dec. 22, 2025).

123 Gitanjali Das et al., *Privacy Policies for Apps Targeted Toward Youth: Descriptive Analysis of Readability*, 6 JMIR MHEALTH & UHEALTH 1, 1 (2018) ("Analysis of privacy policies for these 64 apps revealed an average [reading grade level] of 12.78, which is well above the average reading level (8.0) of adults in the United States.").

124 Taylor Maguire, *The Hidden Risks of Complicated Privacy Settings in Popular Apps*, EMPYRION TECHS. (Aug. 27, 2024), https://www.empyrion.net/resource/the-hidden-risks-of-complicated-privacy-settings-in-popular-apps [https://perma.cc/8WR6-HZE9].

125 *See* Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 62 (2017).

126 *Id.* at 56 ("In addition to the harms created by targeting or exclusion from opportunity, the poor may face magnified privacy vulnerabilities as a result of community-specific patterns around technology use and knowledge gaps about privacy- and security-protective tools. Legal scholars have identified a broad group of consumers as 'privacy vulnerable' when they 'misunderstand the scope of data collection and falsely believe that relevant privacy rights are enshrined in privacy policies and guaranteed by law.'" (citation omitted)).

configuration for a broad spectrum of mobile devices.[127] It should also offer flexible access options—such as mobile-first design, SMS-based alerts, or even voice-response systems for those who prefer audio interfaces.

Critically, equity in PFP models must be strongly regulated. Regulation is essential to prevent platforms from ignoring the hardest-to-reach users. The FTC and state Attorneys General should incorporate equity audits into their oversight of children's privacy practices and evaluate whether they work for families across income levels, languages, geographies, and device types. Civil rights groups and consumer protection organizations should also be empowered to test PFP systems for disparate impact and file complaints when inequities arise. In short, privacy can't be pay-to-play. It must be pay-to-enhance. And enhancement must never come at the expense of fairness.

C. FTC Enforcement and Market Incentivization

1. The FTC's Legacy of Privacy Regulation

No matter how well-designed a PFP model may be in theory, its real-world impact depends on effective regulation and enforcement. Without robust oversight, PFP tools could devolve into glossy dashboards with no legal teeth. The model must be embedded in a regulatory architecture that defines minimum standards, mandates transparency, and deters abuse in order to succeed. That task will fall primarily to the FTC, which remains the de facto national regulator of privacy in the U.S.[128]

The FTC's authority under section 5 of the Federal Trade Commission Act to prohibit "unfair or deceptive acts or practices" provides a strong foundation.[129] Historically, the FTC has used this authority to challenge companies that misrepresent their data practices, enforce privacy statutes, and regulate data transfers between the U.S. and the European Union.[130] It has also enforced COPPA, which requires verifiable parental consent before collecting personal information from children under thirteen.[131] Howev-

127 Elvy, *supra* note 31, at 1400–01 ("Research on the historical digital divide and the demographics of smartphone users indicates that iPhone users tend to have significantly higher incomes than Android users, and low-income individuals frequently rely on smartphones for internet access since 'they do not have broadband.'" (citation omitted)).

128 *See* Khan, Levine & Nguyen, *supra* note 18, at 1380.

129 15 U.S.C. § 45(a)(1).

130 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

131 15 U.S.C. §§ 6501–6502.

er, the Agency's COPPA enforcement has been somewhat limited by the failure of federal lawmakers to pass updates to the law as the battle over privacy for children alone versus privacy for all Americans continues.[132]

That may be changing. In January 2025, the FTC finalized long-awaited updates to the COPPA Rule, adding restrictions on targeted advertising, limiting data retention, and enhancing parental access rights.[133] These amendments open the door to a more proactive approach that could support the deployment of PFP tools as part of a comprehensive privacy compliance strategy. Under the new rule, parents have "new tools and protections to help them control what data is provided to third parties," including a parental opt-in for third party advertising and other changes that address "how children's data is being shared and monetized."[134] Moreover, the proposed changes would require the FTC-approved COPPA Safe Harbor programs to publicly disclose membership lists and report additional information to the FTC,[135] and—at least for companies who wish to comply with the Safe Harbor programs—these requirements could support additional regulatory mandates like monthly privacy reports with streamlined control panels and minimum usability standards for parental tools.

Beyond COPPA, the FTC has also signaled growing interest in platform accountability. In recent reports and public statements, the Agency has criticized "dark patterns," which are manipulative user interfaces and other practices that exploit users' cognitive biases to suppress privacy choices.[136] Many current children-targeting applications suffer from these defects and impact parental decision-making.[137] A PFP system could prioritize simplicity and accessibility and serve as a model of compliance, while platforms that refuse to adopt such systems may face increasing scrutiny for unfair practices. Perhaps more importantly, the FTC recently used its rulemaking authority under the Magnuson-Moss Act to crack down on dark patterns.[138] Although the Magnuson-Moss rulemaking process is lengthy and politically

132 *See* Steinberg, *supra* note 6, at 454.

133 *See* FTC Finalizes Changes, *supra* note 15.

134 *Id.*

135 *Id.*

136 *See* BUREAU OF CONSUMER PROT., *supra* note 112, at 1–2.

137 *See id.* at 10.

138 Khan, Levine & Nguyen, *supra* note 18, at 1428 (noting that "[d]eploying its [Magnuson-Moss] rulemaking authority [to address dark patterns] . . . represented a significant shift" and a new strategy for the FTC).

fraught,[139] it allows for the creation of binding rules that define acceptable business practices. For example, the FTC could adopt rules specifying what a monthly privacy report must contain, what language it must use, how often it must be delivered, and what technical standards apply.[140] The Agency could also mandate disclosures about whether a platform offers paid privacy enhancements and require that those enhancements meet specific efficacy benchmarks to ensure that parents are not simply paying for the illusion of control. Enforcement, however, remains a sticking point for several reasons.

First, the FTC lacks direct fining authority for first-time violations of section 5, and its enforcement powers are limited to consent decrees and settlement orders.[141] The FTC relies on consent decrees and settlement orders strategically because it has limited resources.[142] These constraints mean that the FTC must be selective and strategic in its cases. To maximize impact, the Agency could partner with state Attorneys General, who could bring actions under parallel state laws. In addition, Congress has repeatedly failed to expand the FTC's enforcement powers through new legislation, including recent unenacted bills KOSA and COPPA 2.0.[143]

Second, any FTC rulemaking will now be impacted by the landmark 2024 U.S. Supreme Court decision in *Loper Bright Enterprises v. Raimondo*.[144] *Loper Bright* overruled the four-decade-old *Chevron* doctrine, holding that under the Administrative Procedure Act, courts must exercise independent judgment in interpreting ambiguous statutes rather than deferring to federal agency interpretations.[145] Although "FTC representatives have stated that this change will have little effect on key issues relat-

---

139 *See* Jon Leibowitz, Chairman, Fed. Trade Comm'n, Remarks at the Association of National Advertisers Advertising Law and Public Policy Conference (Mar. 18, 2010) (transcript available at https://www.ftc.gov/sites/default/files/documents/public_statements/association-national-advertisers-advertising-law-and-public-policy-conference-prepared-delivery/100318nationaladvertisers.pdf [https://perma.cc/HL9W-KLXX]) ("The requirements to promulgate a rule under these procedures are so onerous that the agency has not proposed a new Mag-Moss rule in 32 years."); Solove & Hartzog, *supra* note 130, at 620 (claiming "the FTC has only Magnuson-Moss rulemaking authority, which is so procedurally burdensome that it is largely ineffective").

140 *See* 15 U.S.C. § 57a(b)(1)–(2)(A) (outlining FTC unfair or deceptive acts or practices rulemaking proceedings under Magnuson-Moss).

141 *See* Solove & Hartzog, *supra* note 130, at 605.

142 *Id.* at 624.

143 Kids Online Safety Act, S. 1409, 118th Cong. (2023); Children and Teens' Online Privacy Protection Act, S. 1628, 117th Cong. (2021).

144 *See* 603 U.S. 369, 412–13 (2024).

145 *Id.*

ed to data privacy,"[146] this shift suggests that any legislative action which grants FTC rulemaking authority could be impacted.

Nevertheless, the FTC can support the deployment of PFP models like the monthly privacy report envisioned in this Article. For example, the Agency could issue guidance documents or staff reports that define what a "reasonable" monthly privacy report looks like under section 5. It could launch industry workshops to solicit input from child development experts, designers, educators, and parents. It could also publish compliance checklists or technical templates to help smaller platforms implement PFP tools without prohibitive costs. The FTC has the authority, the expertise, and (increasingly) the political support to make PFP a reality. But it must act deliberately. A good tool in the wrong hands—or one implemented without guardrails—can cause more harm than good. But the success of any PFP model will depend on whether platforms see a business case for adoption. Lasting changes in the tech sector, particularly for privacy changes, often include a balance of stringent regulation and market innovation.[147]

2. The Market and Privacy Innovation

Consumer demand for privacy is rising, especially among parents, and Americans generally agree that the responsibility for protecting children's privacy should be shared between parents, tech companies, and the government.[148] A recent Pew Research Center study of over 5,000 U.S. adults found:

> Americans worry about kids' online privacy – but largely expect parents to take responsibility. Some 89% are very or somewhat concerned about social media platforms knowing personal information about kids. Large shares also worry about advertisers and online games or gaming apps using kids' data. And while most Americans (85%) say parents hold a great deal of responsibility for protecting kids' online privacy, 59% also say this about tech companies and 46% about the government.[149]

---

146 Jeffrey M. Stefan & Marisa K. McConnell, *Impact of Chevron Decision on Compliance Risk Under Data Protection Regimes*, VARNUM (July 22, 2024), https://www.varnumlaw.com/insights/post-chevron-impact-data-privacy/ [https://perma.cc/W686-LP5T].

147 *See* Anu Bradford, *The False Choice Between Digital Regulation and Innovation*, 119 NW. U. L. REV. 377, 410–11 (2024) (describing how data privacy regulation does not have "a one-directional effect on innovation," but instead spurs new innovations, including social and market innovations).

148 *See* COLLEEN MCCLAIN ET AL., PEW RSCH. CTR., HOW AMERICANS VIEW DATA PRIVACY 6 (2023), https://www.pewresearch.org/wp-content/uploads/sites/20/2023/10/PI_2023.10.18_Data-Privacy_FINAL.pdf [https://perma.cc/4UZY-NKSC].

149 *Id.*

Companies are beginning to respond. Apple, for example, has heavily marketed its ATT framework as a selling point for privacy-conscious users.[150] While ATT is not specific to children, it demonstrates how privacy features can serve as brand differentiators. Similarly, Meta's rollout of a paid, ad-free experience in Europe signals a willingness to monetize privacy as a premium offering.[151] These developments suggest that platforms recognize privacy as a value proposition, not just a compliance cost, especially in light of both regulation and market innovations. A PFP model fits well within this trend. It allows platforms to offer differentiated service tiers, including a free version with default privacy protections, and a premium version with enhanced tools such as monthly privacy reports, predictive alerts, and granular parental controls. Just as platforms now sell cloud storage upgrades or priority customer support, they can sell a model that reflects what the above study demonstrated: Parents are still seen as the primary gatekeepers of children's online privacy, but tech companies and regulators are still key stakeholders.[152]

Beyond direct consumer revenue, PFP also opens the door to advertiser relationships that prioritize trust. Brands want to avoid being associated with unethical data practices, especially those involving children. A platform that adopts a certified PFP program could attract advertisers seeking to align with "safe" digital environments. Just as law firms pursue ranking in Chambers and Partners,[153] platforms could pursue privacy certifications that signal their ethical handling of user data. These reputational signals matter in an era of viral backlash.

PFP adoption could also streamline compliance costs. Right now, companies have to comply with some sectoral federal privacy laws, at least nineteen state-specific consumer privacy laws, and even some international privacy regulations like the European Union's GDPR.[154] As regulators in the U.S. and around the

---

150 *See We're Committed to Protecting Your Data*, APPLE: PRIVACY, https://www.apple.com/privacy/features/ [https://perma.cc/3258-7GRC] (last visited Nov. 16, 2025).

151 *See Facebook and Instagram to Offer Subscription for No Ads in Europe*, META (Nov. 12, 2024), https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/ [https://perma.cc/K5E2-M6HN].

152 McClain et al., *supra* note 148.

153 Chambers and Partners is an analytics company that ranks law firms and associated lawyers based on practice areas across the globe. *See* CHAMBERS & PARTNERS, https://chambers.com/ [https://perma.cc/CP77-SBF9] (last visited Nov. 16, 2025).

154 *See U.S. Privacy Laws*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/privacy-laws/united-states/ [https://perma.cc/UC6M-KV9J] (last visited Nov. 16, 2025) (providing a nearly comprehensive list of federal privacy laws); INT'L ASS'N OF PRIV. PRO., *supra* note

world tighten enforcement, platforms face increasing costs for privacy failures.[155] Implementing PFP features proactively—before they are required—can mitigate these risks and help companies streamline their compliance efforts by providing the very data that is already required of them by piecemeal legislation across the country and around the globe.

Investors may also exert pressure. Privacy and data governance increasingly appear as key indicators in environmental, social, and governance (ESG) compliance.[156] A platform that can demonstrate robust protections for children's data may become more attractive to institutional investors and mission-driven capital. These pressures are especially relevant for publicly traded tech companies, which face scrutiny not only from regulators but also from shareholder advocacy groups concerned about long-term reputational risk.[157]

Finally, there's the matter of international harmonization. Even if the U.S. is slow to adopt national privacy legislation—for children or for all Americans—global companies must comply with stricter frameworks elsewhere. The European Union's Digital Services Act and AADC impose far-reaching obligations on platforms that serve minors, including requirements for privacy-by-default, data minimization, and age verification.[158] Adopting PFP features across markets may simplify compliance and help companies build a coherent global privacy strategy. To be clear, platforms likely won't altruistically adopt PFP. But they may adopt it for customer retention, brand positioning, regulatory relief, investor confidence, and competitive edge. Privacy advocates

94; Bradford, *supra* note 147, at 405 (stating that U.S. Fortune 500 companies collectively spent over $7 billion on GDPR compliance leading up to its effective date in 2018).

155 Bradford, *supra* note 147, at 405.

156 *A New Frontier: Data Protection and Privacy in ESG*, PRICEWATERHOUSECOOPERS (Oct. 9, 2023), https://www.pwc.com/ke/en/blog/data-protection-privacy-in-esg.html [https://perma.cc/52LV-KFPQ].

157 Zack Mukewa, *Shareholder Activism and Good Governance Hygiene for Publicly Traded Companies*, LAMBERT (Dec. 19, 2024), https://lambert.com/shareholder-activism-and-good-governance-hygiene-for-publicly-traded-companies/ [https://perma.cc/FX58-CXMM].

158 *See* Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC, 2022 O.J. (L 277) 1, 19, 65 (EU); Elizabeth Denham, *Age Appropriate Design: A Code of Practice for Online Services*, INFO. COMM'R'S. OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ [https://perma.cc/K9AB-SQ66] (last visited Nov. 16, 2025).

have argued that it is better to build in privacy rather than "bolt it on . . . after the fact."[159]

A well-designed PFP system integrates privacy into the product, the process, and the pitch. But if designed poorly or deployed without safeguards, PFP systems can amplify the very harms they aim to mitigate. They may enable predatory pricing structures or obscure deeper data collection practices (especially if dark patterns remain pervasive). As such, any implementation of PFP must include a clear set of legal and ethical guardrails to prevent misuse and protect families from exploitation.

One major concern is that companies may use PFP offerings to justify excessive data collection in their "free" tiers. The danger here mirrors patterns seen in the digital advertising economy, where platforms optimize for engagement and data extraction, then upsell privacy as a premium feature, effectively turning user vulnerability into a revenue stream.[160] This is the dark side of privacy-by-design, generally, but also of PFP models in which manipulation is the default and autonomy costs extra. Without regulatory constraints, companies may treat PFP as a get-out-of-jail-free card: *We gave parents the option to pay for control; if they didn't, that's on them*. To prevent this, regulators must impose minimum privacy baselines that apply across all service tiers. Every child—regardless of whether their parent pays for the monthly privacy report—should benefit from core protections found in COPPA and its updated Final Rule, such as prohibitions against behavioral ad targeting, strict limits on data sharing, and accessible transparency about data collection.[161]

Additionally, PFP must not be allowed to circumvent consent requirements or obscure notice obligations. For example, a platform should not claim that by subscribing to a PFP plan, a parent has automatically consented to future data uses not clearly disclosed. Nor should a PFP subscription waive the child's rights under existing law. Strong guardrails must prohibit such tactics and ensure that every data practice is independently justified and subject to scrutiny. Moreover, parents, policymakers, and companies must remain attentive to evolving threats. As artifi-

159 ANN CAVOUKIAN, PRIVACY BY DESIGN IN LAW, POLICY AND PRACTICE: A WHITE PAPER FOR REGULATORS, DECISION-MAKERS AND POLICY-MAKERS 11 (2011).

160 *See* Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 634 (2014) (asserting that companies with freemium business models "devote remarkable amounts of attention and investment to the collection of data from and about free-riding consumers of their products").

161 *See* 15 U.S.C. §§ 6501–6506; FTC Finalizes Changes, *supra* note 15.

cial intelligence tools become more sophisticated, companies will undoubtedly be (and already are) incentivized to use them to infer sensitive attributes about children from seemingly innocuous behaviors.[162] In 2025, the FTC noted a recent complaint against Amazon when its voice assistant, Alexa, retained children's voice recordings indefinitely and used the data to train Alexa's algorithm.[163]

But artificial intelligence can also be a benefit to companies and to children's privacy. For example, "emerging AI-based devices and services can automatically detect when a child's online behavior indicates that their well-being might be compromised" and "notify parents or immediately block harmful content."[164] Scholars have suggested that companies should voluntarily provide these tools by design in the absence of parental demand, and proposed "an indirect government approach that would *influence*—rather than oblige—the development, implementation, and education of algorithmic parenting technologies."[165] Perhaps more closely relevant to this Article's proposition, scholars have also suggested that algorithmic parenting technologies should be accessible to all, and a host of stakeholders—from schools to social programs and family courts to government agencies—can collaborate to make these technologies as accessible as possible (even if they never achieve accessibility for all).[166]

Ethical considerations, then, must guide the entire PFP ecosystem. Developers and designers should engage in privacy-centered design processes that foreground the needs and limitations of parents. User testing should include families from diverse socioeconomic and cultural backgrounds. Feedback loops should be built in, allowing parents to flag problems, suggest improvements, and participate in the governance of the tools they rely on. The long-term legitimacy of any PFP framework depends on trust—and trust cannot be commanded by parents, policymakers, or companies alone. It must be earned through shared transparency, usability, consistency, and responsiveness. That means platforms must not only meet their legal obligations but also treat privacy as a moral obligation, especially when it concerns children.

The PFP model this Article proposes is not a license to shift responsibility from companies to parents. It is an opportunity to

---

162 *See* FED. TRADE COMM'N, *supra* note 3, at v–vi.

163 *See* Atleson et al., *supra* note 36.

164 Eldar Haber & Tammy Harel Ben Shahar, *Algorithmic Parenting*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 4 (2021).

165 *Id.* at 49.

166 *See id.* at 54–63.

share that responsibility and empower parents without disempowering children, to offer options without creating inequities, and to build safer digital environments that don't depend on perfect vigilance or disposable income. With proper guardrails and accountability mechanisms, PFP can become a powerful tool for reform. But without those conditions, it's just another product, one that neither parents nor children want or deserve.

IV. A PATH FORWARD: REGULATING CHILDREN'S BEST PRIVACY INTERESTS

A. Divorcing Consent

For over two decades, American privacy law has leaned heavily on the deceptively simple premise that parents can meaningfully control their children's digital lives. At first glance, this premise seems both intuitive and empowering. After all, who knows a child better than their parent? But in the modern digital ecosystem, where parents often lack the time or understanding to meaningfully consent to certain data collection practices and intentionally or unintentionally act against their child's best interests, parental control alone—through parental consent regimes—does not suffice.[167] It is invoked to justify weak statutory protections, to offload corporate responsibility onto parents, and to mask the growing asymmetry between families and tech platforms. The law may say "*ask the parent*," but it rarely gives the parent the tools, time, or leverage to say anything meaningful in return.

This hollowing out of parental authority begins with the structure of consent and the lack of consideration for teens over thirteen under COPPA.[168] The statute assumes that, armed with appropriate disclosures, parents will exercise informed judgment about whether their child's data should be shared. But this assumption is wildly out of step with today's digital environment. COPPA may demand parental consent, but it does little to ensure that consent is informed, and it does little to protect the millions of teens over thirteen who provide their data to streaming services and social media platforms. Moreover, consent mechanisms often rely on frictionless clicks or passive opt-ins, which further dilute the idea of meaningful choice.[169] What's more, even if parents want to exercise control, their time and cognitive bandwidth are limited. For working-class families juggling jobs, transporta-

167 *See* Takhshid, *supra* note 5, at 1417, 1421; Steinberg, *supra* note 6.
168 *See* 15 U.S.C. §§ 6501–6506.
169 *See* Solove, *supra* note 23, at 607–10.

tion, childcare, and household demands, the idea of spending hours poring over settings, policies, and platform disclosures is simply unrealistic.

These challenges are compounded by design choices that frustrate parental engagement. Dark patterns are especially harmful in child-directed contexts.[170] For instance, parents may unwittingly agree to a host of coerced actions, subtly steering them toward the default that benefits the platform.[171] Some platforms even gamify the consent process, suggesting that limiting data access may reduce the child's experience or prevent certain features from working.[172] When consent is manipulated or obscured, the supposed control offered to parents becomes illusory.

Moreover, COPPA's age cutoff—under thirteen—reflects outdated assumptions about children's development and fails to reflect how kids actually engage with technology. Today, children under thirteen are frequent users of general-audience apps like YouTube, Instagram, TikTok, and Discord, which routinely avoid COPPA's requirements by claiming not to "knowingly" target minors.[173] This fiction allows companies to operate in a compliance gray zone, where they avoid responsibility unless they have actual knowledge of a child user. Parents are thus asked to consent on platforms that pretend their children aren't even there.

Complicating matters further is the asymmetry of knowledge between families and platforms.[174] Companies possess a level of information about user behaviors, preferences, vulnerabilities, and patterns of use that users—parents or children—could never hope to match. From a single child's usage, platforms can infer mood states, insecurities, and social anxieties.[175] They use these inferences to curate feeds, serve ads, and shape online experiences in ways that are invisible to parents and regulators alike.

This reality undermines the feasibility of parental control and its moral and legal coherence. How can a parent's one-time consent satisfy the obligation to protect a child's privacy over

170 *See* BUREAU OF CONSUMER PROT., *supra* note 112, at 3, 11.

171 *See id.* at 24–25.

172 *Id.* at 23–25. In the FTC's chart of common dark patterns, these types of dark patterns would likely be considered interface interference or coerced actions. *Id.*

173 *See* MacDonald, *supra* note 92, at 594.

174 *See* Vagle, *supra* note 90, at 79.

175 Fed. Trade Comm'n, Comment Submitted by Fairplay and Center for Digital Democracy (Dec. 1, 2022), https://www.regulations.gov/comment/FTC-2022-0053-1144 [https://perma.cc/76CU-HEQC].

time if platforms are building profiles based on recurring behavioral analytics?

While consent mechanisms remain the primary vehicle through which privacy is ostensibly protected in the U.S.,[176] their effectiveness is further hampered by the piecemeal and outdated nature of federal and state privacy regulation. COPPA remains the central statute governing online data practices for children under thirteen, but it was enacted in 1998—long before the explosion of mobile apps, social media platforms, behavioral advertising, or AI-powered recommendation engines.[177] The statute's definitional scope, enforcement structure, and technological assumptions no longer align with the realities of how children engage with digital services. Although the FTC has taken steps to modernize the rule through updates such as the 2013 Final Rule and the most recent 2025 revisions, these amendments have not been sufficient to close the structural gaps that leave children exposed to pervasive surveillance and manipulation.[178] Without a single statute to govern the full spectrum of data collected from children across platforms, apps, and devices, some states have proposed children-focused privacy laws.[179] Unfortunately these laws have been temporarily enjoined as likely violative of the First Amendment, as most of them restrict children's and teens' speech on these platforms, and it seems likely that "privacy laws aimed at protecting children online have difficulty passing constitutional muster."[180]

B. Regulation as a Surrogate

The FTC's role as enforcer is admittedly limited. Although the Agency has brought high-profile enforcement actions against TikTok, YouTube, and Epic Games for COPPA violations, its overall capacity to investigate and penalize misconduct remains modest. The Agency's budget is small compared to the scale of the surveillance economy, and its authority to penalize violators is handicapped by its statutory authority and procedural hurdles.[181] Moreover, the FTC's reliance on consent orders and negotiated settlements often fails to produce systemic reform. Yet the FTC has been the most active and effective privacy regulator at

176 *See* Solove, *supra* note 23, at 593.
177 *See* 15 U.S.C. §§ 6501–6506; MacDonald, *supra* note 92, at 594.
178 *See* FTC Finalizes Changes, *supra* note 15.
179 *See* MacDonald, *supra* note 92, at 596.
180 *Id.*
181 *See* Solove & Hartzog, *supra* note 130, at 609.

the federal level, and it has shown a renewed commitment to protecting children's privacy.

This Article contends that these realities produce an unclear path forward for children's privacy. The current system could remain because Congress is unable to pass comprehensive privacy legislation and regulate unethical data practices, leaving parents as the sole gatekeepers of their children's privacy through consent-based regimes at the federal and state level—a system that has been well-documented as clearly harmful to parents, children, and society.[182] Or a new system could emerge that refuses to accept a false dichotomy (where privacy is either a commodity or not) and refuses to isolate one or two of the stakeholders as responsible for children's privacy and instead distributes responsibility among parents, regulators, and companies. This Article argues that privacy's value is intrinsically diminished by its commodification and market norms alone cannot dictate privacy regulation.[183] However, this Article also suggests—and the PFP model it proposes would require—a holistic approach to regulating children's privacy centered on accessible, symmetrical information given to the parent, a reasonable fee paid to the company to provide this information, and a proven regulator capable of ensuring equity and fairness.

An emphasis on parental notice and choice, especially in the context of children's privacy, is unrealistic and fundamentally inadequate. What is needed instead is a regulatory paradigm that moves beyond the transactional logic of consent and incorporates structural constraints on data flows, algorithmic practices, and platform design. A PFP model, if properly constructed, could contribute to this shift, but only if it operates within a broader legal framework that limits exploitative defaults and imposes meaningful accountability.

C. Collective Custody of Children's Privacy

In Part I, this Article introduced some of the guardrails that must be in place before a PFP model can be taken seriously. These guardrails will largely fall on the companies to design and the FTC to enforce, in an effort to ease the burden placed on parents, guardians, and caregivers. A functional PFP model requires

182 *See supra* Part II.

183 Vagle, *supra* note 90, at 108 ("[P]rivacy's value is intrinsically diminished by its commodification, and an antitrust approach to addressing information privacy harm depends, at least in part, on the acceptance of user data solely as a commodity to be bought and sold.").

strong regulatory guardrails to prevent coercion and ensure equity. These essential guardrails include design restrictions, pricing caps, public subsidies, and some baseline protections. Companies must not manipulate users into upgrading through dark patterns, misleading designs, or degraded default options. Companies should price PFP services low enough—around three to five dollars per month—for most families to afford them. Low-income families should receive discounted or free access to PFP tools, which schools, social welfare programs, or federally funded nonprofits could help provide. And companies cannot deny essential privacy rights to those who choose not to pay. PFP services must expand transparency and control rather than replace some of the emerging data subject rights found in American privacy laws. With these protections in place, the PFP model offers a transitional tool to help families navigate a complex digital environment while broader reforms continue to take shape.

Of course, this Article describes a non-exhaustive list of guardrails, some of which are as unlikely to be adopted as it is that Congress will pass a drastic reformation of COPPA any time soon. However, this section will touch on some of these guardrails and how the FTC has the momentum and expertise to ensure a regulated, equitable PFP model.

1. Design Restrictions

The vulnerabilities of children in digital spaces are often the result of intentional platform design choices. Companies actively shape children's interests and exploit developmental psychology to maximize engagement and data extraction. As platforms compete for attention in an economy fueled by surveillance, children become both the product and the testing ground for increasingly sophisticated behavioral techniques. These practices raise serious ethical, psychological, and legal concerns, especially when children are treated not as autonomous beings with rights, but as passive data sources to be optimized and monetized.

One of the most pervasive tactics is persuasive interface design, because companies understand that it is hard for someone to prove a privacy harm if neither the user nor the regulator is able to understand how the company's systems or processes work.[184] Social media apps and streaming services deploy mechanisms like infinite scroll, autoplay, algorithmic recommenda-

184 *See* David Choffnes et al., *A Scientific Approach to Tech Accountability*, 37 HARV. J.L. & TECH. 1201, 1203 (2023).

tions, badges, streaks, and gamified rewards to sustain attention.[185] These features may seem innocuous, even entertaining, but their cumulative effect is to create digital dependencies that are difficult for children to recognize or resist. A child who stays up three extra hours to maintain a Snapchat streak or unlock a limited-time reward in Roblox is responding to a system engineered to override impulse control and not simply exercising free choice.[186]

Developmentally, children and adolescents are especially susceptible to such manipulations. Neuroscience research shows that the prefrontal cortex—the region of the brain associated with self-regulation, planning, and risk assessment—continues developing into early adulthood.[187] In contrast, the brain's reward system, which governs the response to novelty and gratification, is highly active during childhood and adolescence and can make adolescents take risks.[188] This mismatch creates a neurological window during which youth are particularly vulnerable to persuasive technologies that offer instant feedback and social reinforcement. Platforms design apps with this imbalance in mind.

For example, TikTok's "For You" page delivers a continuous, algorithmically curated stream of short videos based on micro-engagement data, and it brands itself as the leading destination for short-form mobile video.[189] While marketed as personalized content discovery, this design maximizes time-on-platform and increases exposure to advertisements that more than 70% of users consistently state they do not want.[190] Children cannot understand or control the algorithms that shape what they see, yet those algorithms shape their sense of self.

Compounding the problem is the rise of technologies that track and infer users' emotional states, something that even the United Nations Convention on the Rights of the Child recognizes as particularly harmful to children.[191] In child-directed contexts,

185 *See* FED. TRADE COMM'N, *supra* note 3, at 64.

186 *Id.* ("Further, some researchers believe that social media exposure can overstimulate the reward center in the brain and, when the stimulation becomes excessive, can trigger pathways comparable to addiction.").

187 Mariam Arain et al., *Maturation of the Adolescent Brain*, 9 NEUROPSYCHIATRIC DISEASE & TREATMENT 449, 459 (2013) ("The development and maturation of the prefrontal cortex occurs primarily during adolescence and is fully accomplished at the age of 25 years.").

188 *See id.* at 451.

189 FED. TRADE COMM'N, *supra* note 3, at 42.

190 *See id.* at 40.

191 *See* Comm. on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, ¶ 42, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).

this is even more problematic when algorithms are designed to detect when a child is sad, anxious, or bored and then serve content designed to validate those feelings to increase engagement.[192] It is a form of psychological exploitation that would be unthinkable in the physical world but remains largely unregulated online. Even when platforms offer "kid-friendly" versions of their services, such as YouTube Kids or Messenger Kids, the underlying design logics often remain the same. A parental dashboard may display what videos a child watched, but not why those videos were recommended, what data informed the algorithm, or what behavioral patterns were inferred from the session.

Attempts to mitigate these harms through design codes and voluntary standards have produced mixed results. This Article previously discussed the California AADC,[193] but the United Kingdom's AADC, for instance, requires platforms to consider the best interests of the child and minimize data collection.[194] In the U.S., companies may tout "child safety initiatives," but often those initiatives function more as PR than as substantive reform. Without binding legal standards and robust oversight, persuasive design remains a default rather than an exception.

The U.S. has tried to address these design issues. KOSA would have imposed a duty of care, required platforms to eliminate dark patterns, and disclose algorithmic processes[195] but it unfortunately failed to pass. As a result, platforms can continue to use "opaque algorithms" that exploit developmental vulnerabilities under the guise of personalization and choice.[196] Perhaps the most insidious effect of these design choices is that they normalize surveillance and manipulation as a condition of childhood. Children raised in these environments may come to see them as

---

192 *See* Carolanne Bamford-Beattie, *Understanding Social Media Algorithms: A Guide for Concerned Parents*, KIDSLOX (Sep. 16, 2024), https://kidslox.com/guide-to/social-media-algorithm/ [https://perma.cc/ZU94-X84V] ("[B]ecause the platform's algorithm prioritizes engagement, it could soon start suggesting more extreme content, such as unhealthy dieting practices or body image challenges. Similarly, on YouTube, a child searching for a simple video on coping with anxiety could quickly be led to more distressing content about mental health struggles.").

193 *See supra* Section II.B.

194 *See* Denham, *supra* note 158.

195 *See generally* S. 1409, 118th Cong. (2023) (proposing federal duties of care, safeguards, and design restrictions for platforms used by minors).

196 *Id.* § 13(a)(7)(A) (defining "opaque algorithm" as an algorithmic ranking system that determines the selection, order, relative prioritization, or relative prominence of information that is furnished to such user on a covered internet platform based, in whole or part, on user-specific data that was not expressly provided by the user to the platform for such purpose); *id.* § 13(b)(2)(A) (requiring that platforms disclose when they use an opaque algorithm).

natural. This habituation erodes the very concept of privacy. Children may internalize the idea that being watched is the price of participation, and that their value lies in what they can produce for the algorithm.

This normalization also makes resistance more difficult. Parents who attempt to limit screen time or monitor app usage may be cast as authoritarian or out of touch. Children themselves may be reluctant to challenge the platforms they perceive as sources of identity, sociality, and escape. Without systemic change, the burden falls again on families to battle technologies that are specifically designed to outpace them.

Ultimately, protecting children from design-based manipulation requires a shift from user responsibility to developer responsibility. Platform companies must be held legally accountable for the foreseeable consequences of their design choices, particularly when those consequences exploit known developmental vulnerabilities. This includes obligations to disclose information about and provide audit results of algorithms and eliminate dark patterns that subvert parents' and children's autonomy.

As Part IV continues, it will explore what a regulatory framework might look like and how regulators, companies, and civil society can work together to build it.

2. Proactive Enforcement

A robust privacy framework for children cannot rest solely on the good faith belief that companies will design with children's privacy in mind simply because a parent paid for it. It requires a regulatory agency with the power and expertise to enforce children's privacy rights across platforms. In the U.S., that role falls largely to the FTC, which enforces COPPA and engages in broader consumer protection actions against deceptive or unfair data practices. While the FTC has remained an agency operating under structural constraints and insufficient resourcing,[197] its "privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States"[198] and, at least in recent years, has "set out on a new path" through enforcement and rulemaking to secure baseline protections, combat harmful interfaces, and protect children and teens online.[199] Although the effects of *Loper Bright* and an administration

197 *See* Solove & Hartzog, *supra* note 130, at 605.

198 *Id.* at 583.

199 Khan, Levine & Nguyen, *supra* note 18, at 1380.

change remain to be seen for FTC activity and privacy, rebuilding a proactive enforcement regime should begin by reimagining the FTC as a proactive privacy regulator empowered to investigate systemic risks and impose meaningful consequences.

To establish this paradigm, the FTC would need to promulgate binding rules governing data collection, profiling, algorithmic transparency, and age-appropriate design. Such authority would allow the FTC to go beyond the general "unfair and deceptive acts and practices" framework and create sector-specific rules for services targeting or accessible to minors. Moreover, it would clarify the boundaries of compliance, making it harder for companies to feign ignorance or exploit gray areas.

In addition to formal authority, the FTC needs greater technical expertise and investigative capacity. As platforms employ increasingly complex machine learning systems to drive engagement and data extraction, the FTC must be able to audit and assess these systems effectively. This includes hiring engineers, data scientists, child psychologists, and digital ethicists to supplement its legal staff. As Julie Cohen has argued, meaningful regulation of information systems demands an institutional apparatus capable of understanding and contesting the internal logic of algorithmic decision-making.[200] Without this, regulators will remain at a disadvantage—always one step behind industry innovation.

Further, enforcement must shift from post hoc punishment to proactive oversight. This could include requiring platforms to conduct and submit child impact assessments, similar to the data impact assessments, envisioned in the GDPR and in recent children's privacy bills,[201] prior to launching new features or modifying data practices. These assessments should evaluate foreseeable risks to children's privacy and development, be subject to an FTC audit, and result in penalties if the harms are not adequately mitigated. Public transparency around these documents would also enable civil society to hold platforms accountable and promote a culture of anticipatory responsibility.

---

200 JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 171 (2019).

201 Commission Regulation 2016/679, art. 35, 2016 O.J. (L 119) 1 (EU) ("[T]he controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."); *see also* S. 1409, 118th Cong. § 6(a)–(f) (2023) (providing that this section would have required several assessments describing the reasonably foreseeable risks of material harms to minors).

The FTC could also benefit from building a tiered compliance framework, akin to financial sector regulation, in which platforms with greater scale or more intrusive data practices are subject to enhanced obligations.[202] In children's privacy, companies collecting biometric data or using predictive analytics on children could be required to undergo annual privacy audits, maintain dedicated compliance staff, and face higher penalties for violations, some of which are already recommended by the FTC.[203] This approach would create regulatory asymmetry that matches risk with oversight, rather than treating all digital services as equally benign.

Finally, enforcement must include individual redress mechanisms. One of the major criticisms of current privacy enforcement is that remedies rarely flow to those harmed.[204] While class action suits are theoretically possible under state privacy torts,[205] federal privacy law, like COPPA, lacks robust avenues for families to seek damages or injunctive relief when children's data is misused.[206] Congress should consider adding a private right of action under COPPA or a new comprehensive children's privacy statute, allowing parents and advocates to bring enforcement actions independently or in collaboration with the FTC.

These proposals are ambitious, but not unprecedented. The European Union's GDPR empowers national regulators to issue fines of up to 4% of global revenue for violations and grants data subjects enforceable rights over their personal information, including the right to access, correct, delete, and restrict the pro-

---

202 For example, in 2023, the FTC amended the Safeguards Rule—which requires non-banking financial institutions to develop, implement, and maintain a comprehensive security program to keep their customers' information safe—to expand regulation to non-banking financial institutions. The FTC previously only enforced the Rule and the Gramm-Leach-Bliley Act, generally, against banking financial institutions. *See* Press Release, Fed. Trade Comm'n, FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches (Oct. 27, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches [https://perma.cc/HL4L-8QWP] (announcing amendments to the Safeguards Rule that require nonbanking financial institutions to report certain data security incidents to the FTC). *See generally* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809, 6821–6827 (imposing privacy and data security obligations on financial institutions).

203 FED. TRADE COMM'N, *supra* note 3, at vi–vii.

204 *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 861 (2022).

205 *See* Takhshid, *supra* note 5, at 1451–54.

206 *Id.* at 1420 ("COPPA was enacted in 1998, during a different era with simpler privacy concerns. . . . As such, new privacy initiatives at the federal level should also not rely primarily on parental consent but instead offer privacy protection laws that limit the overreach of . . . companies.").

cessing of data.[207] The United Kingdom's AADC includes requirements for data minimization, profiling restrictions, and high default privacy settings, with enforcement delegated to the Information Commissioner's Office.[208] While U.S. regulators are constrained by different institutional and constitutional contexts, these examples demonstrate that robust enforcement is possible—and that protecting children's privacy requires more than symbolic action. As the next section explores, this vision also requires a shift in how we conceptualize responsibility from individual decisions to structural accountability, and from technical fixes to societal commitments.

Moreover, FTC enforcement must also be equity-aware to prevent the pitfalls of PFP. The default settings that benefit privileged children may not serve others equally well. As previously discussed, children from lower-income families are more likely to rely on free platforms that monetize their data and have limited access to paid alternatives, and parents from underrepresented communities are less likely to have the time or the money to invest in a PFP model. Elvy has astutely argued that PFP models—while potentially valuable in structuring consumer choice—risk reinforcing inequality if privacy becomes a luxury good accessible only to affluent families.[209] To address this, the PFP model must be accompanied by "equity-by-default." Design practices and regulatory safeguards must assume children deserve equal protection regardless of their parents' resources or awareness. This requires baseline protections for all users, regardless of tier.

3. Baseline Protections

Default data minimization and limits on algorithmic personalization should be non-negotiable for platforms accessed by children. Companies can offer premium services on top of these standards, but the floor must be raised industry-wide.

Embedding privacy and equity into the design process requires interdisciplinary collaboration. Legal compliance teams must work with UX designers, engineers, ethicists, and child development experts to ensure that platforms are developmentally appropriate. This includes evaluating whether design choices support healthy habits, enable meaningful parental involvement, and avoid manipulation. When privacy decisions are siloed from product development, the result is often a compliance veneer atop

207 Commission Regulation 2016/679, art. 15–18, 83(5), 2016 O.J. (L 119) 1 (EU).

208 *See* Denham, *supra* note 158.

209 Elvy, *supra* note 31, at 1400–04.

exploitative functionality. Privacy by design demands that ethics be embedded, not bolted on.

Critically, these principles must be auditable. The FTC should be empowered to review a platform's design choices and assess whether the monthly privacy report or any other feature of the PFP model satisfies equity-by-default standards. This would require technical documentation, risk assessments, and transparency reports. These tools are already common in cybersecurity and financial services. However, they are underused in the consumer tech sector, particularly in social media and streaming services.[210] Public access to these materials would also empower researchers and advocates to evaluate claims of compliance and surface gaps.

Without enforceable design standards, companies will continue to optimize for engagement and profit rather than well-being. Dark patterns and interference interfaces will always outpace user education if not structurally curtailed. Protecting children's privacy in this context means confronting these design paradigms directly and insisting that technological systems serve developmental needs rather than exploit them.

At the same time, embedding privacy by design must confront the asymmetry of power between technology firms and end users, particularly in the context of children. Even the most well-intentioned parents face substantial challenges when attempting to audit or adjust the privacy settings on platforms used by their children. The burden of understanding complex policies and maintaining controls across multiple devices and services is a structural design failure, not a reflection of parental inadequacy. By contrast, platforms possess not only vast technical knowledge but also the behavioral data to optimize against user resistance, nudging families toward options that benefit the company rather than the child.

This is particularly troubling when the platforms in question actively obscure their business models. As the FTC's 2024 6(b) report noted, companies—especially large social media platforms and streaming services—are incentivized by and routinely fail to disclose their data practices, including the extent to which children's data is used for algorithmic training, cross-device tracking, and third-party sharing.[211] In such an environment, any notion of meaningful consent is illusory. Embedding privacy and equity in-

210 FED. TRADE COMM'N, *supra* note 3, at v–vii.

211 *Id.* at ii.

to product design is, therefore, not just a better user experience, but a necessary corrective to power imbalances that render families effectively powerless in the face of complex digital systems.

Moreover, digital equity demands a more nuanced understanding of intersectionality in children's experiences online. Black, Latino, and LGBTQIA+ youth often face disproportionate surveillance and harassment online and may be subject to predictive profiling that amplifies systemic biases.[212] Design standards must therefore consider not only generic child safety, but also how different children may experience the same feature in vastly different ways. For instance, scholars have demonstrated that an AI-driven system may disproportionately reinforce feedback effects and provide little opportunity for error correction, leading to over-enforcement or exclusion.[213] Embedding equity into privacy design requires rigorous impact assessments and ongoing monitoring of disparate outcomes.

Educational institutions provide another key frontier for PFP models. As more schools adopt additional "learning" services through YouTube, Google, and other tech giants' services built into existing learning platforms, the risk of normalizing invasive data practices during childhood grows.[214] These technologies often lack transparency and are implemented without meaningful consent from families.[215] A regulated design framework would require schools and EdTech vendors to adopt the same standards applied to commercial platforms.[216] Perhaps more importantly, it would prompt a broader conversation about the role of surveillance in shaping educational environments and whether shifting

212 Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, BROOKINGS INST. (July 18, 2022), https://www.brookings.edu/articles/examining-the-intersection-of-data-privacy-and-civil-rights [https://perma.cc/JFV6-MDW4] (arguing for federal legislation to prohibit "commercial surveillance practices that enable discriminatory advertising, racially biased policing, and the outing or surveillance of historically marginalized groups").

213 Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 865–66 (2017) (noting these risks in the employment context).

214 Takhshid, *supra* note 5, at 1432.

215 *Id.* ("How can a parent use their judgment in deciding what is in the best interests of their child and make an informed choice when it may not even be clear what consequences the use of an application might have for their beloved child?").

216 *Id.* at 1454 ("[T]he EdTech industry is a for-profit industry, albeit one operating at schools, and the contracts between the school and the EdTech companies are of a commercial nature.").

away from parental consent and toward an ostensibly equitable PFP model would align with public policy.[217]

Finally, equity by default should be seen as a precondition for sustainable technological development and not as a constraint on innovation. Although some scholars have called regulatory responses to privacy norms "ill-advised" because technologies and norms constantly change,[218] others have advocated for abandoning the "false choice between regulation and innovation" and encouraging the "legal and institutional reforms that are necessary for tech companies to innovate and for digital societies to thrive."[219] Companies that build with children's rights in mind are better positioned to lead in a market increasingly sensitive to privacy concerns and changing consumer preferences.[220] In this way, embedding these principles becomes a form of risk mitigation, brand differentiation, and long-term value creation.

Equity-by-default is not a silver bullet. It requires clear regulatory mandates but also a meaningful cultural shift in how parents, policymakers, and companies think about childhood and technology. But without it, every other reform becomes more difficult because the default architecture of the digital world continues to undermine even the best intentions of law and policy. The future of children's privacy will depend on building a village of responsibility, one in which law, markets, and families all play coordinated roles in creating a safer digital world.

If the past three decades since the moral panic about children's online activities referenced at the outset of this Article have taught us anything, it's that no single actor can protect children's privacy alone. Parents cannot out-click or out-code billion-dollar platforms, and even when they do, they can hamper their children's autonomy.[221] Policymakers cannot write one law to neutralize every dark pattern. And even the most ethical corporations face market pressures that reward surveillance and

---

217 *Id.* ("[T]he EdTech industry has further become a necessary medium for acquiring education for many children, which underscores the public policy defense that necessitates stepping away from insufficient parental consent forms.").

218 Tal Z. Zarsky, *The Privacy-Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 115, 125–26 (2015) (suggesting regulatory responses to privacy norms are "ill-advised" as technologies and privacy norms will rapidly change and instead advocating for both market innovation and social innovation).

219 Bradford, *supra* note 147, at 377.

220 *See id.* at 409.

221 Steinberg, *supra* note 6, at 470–71 (arguing that children's capacities evolve and any age-appropriate design and/or child-centered policies "must avoid treating all young people the same" and that "their need for protection must make way for their evolving need for autonomy").

personalization over restraint. The solution, then, must be collective. Protecting children's privacy in the digital age will require rebuilding a village around a robust ecosystem of shared responsibility among parents, companies, and regulators.

At the foundation of this village are parents, guardians, and caregivers, who remain children's primary gatekeepers. But the current system sets them up for failure because they—especially those from lower-income and otherwise underrepresented communities—lack the time and digital literacy to effectively manage the dozens of apps, platforms, and services their children use. Many default to blind trust, hoping that schools, regulators, or app stores have done their due diligence. Others attempt to monitor usage through screen time controls or family accounts, only to find themselves outmatched by evolving technologies and evasive interfaces.

The burden placed on parents reflects the broader fallacy of consent-based privacy models, which assume users can rationally evaluate risk and exercise rational decision-making about their privacy.[222] As scholars referenced throughout this Article have noted, this framework ignores both the sophistication of digital systems and the emotional and practical constraints of caregiving.

Parents cannot conduct nightly data audits. They cannot read forty-page privacy policies during dinner. And they should not be expected to navigate three webpages deep into a privacy dashboard just to opt out of harmful data collection, use, and disclosure that their children never asked for in the first place. Real privacy protection doesn't mean reducing the need for parental vigilance, but it means making it a little easier to act once vigilance reveals an issue.

Corporations, for their part, must abandon the myth that protecting children's privacy is bad for business. As the FTC's COPPA Final Rule amendments demonstrate, regulators are now willing to intervene where self-regulation fails and "recognize children and teens as a distinct category of consumers requiring strong protections."[223] But the real opportunity lies in embracing privacy as a market differentiator. Companies that adopt privacy-centric PFP models with accessible monthly privacy reports may be rewarded by consumers, too. A children's privacy arms race, spurred by increased revenue and increased privacy protec-

222 Solove, *supra* note 23, at 611–12 ("Human decision-making is fraught with irrationality and systematic biases and heuristics that can readily be exploited.").

223 Khan, Levine & Nguyen, *supra* note 18, at 1407.

tions, is both possible and overdue. That, combined with the FTC's new emphasis on targeting upstream data collection practices, can help make structural changes "focused on addressing business incentives and preventing injury rather than redressing it after the fact."[224] But more funding, technical staff, and legislative clarity are needed if the FTC is to function as a true digital watchdog. State Attorneys General can also fill gaps in enforcement, especially in states where recent attempts at regulating children's privacy through emerging age-appropriate design codes or social media moderation regimes have faced First Amendment challenges[225] or are reliant on parental consent or overinvolvement.[226]

This collective PFP framework may seem like a children's privacy utopia. Inequities will still arise. The FTC will lag in trying to correct those inequities. Companies will push back. And parents will make mistakes. But the goal is to reimagine shared responsibility between parents, regulators, and companies through a PFP model that recognizes parents as in need of accessible choices and children as developing citizens deserving of protection.

V. CONCLUSION

Children's privacy is a defining issue of our digital era, not just for privacy advocates but for society, generally. This Article has argued that protecting children in today's data-driven society requires more than consent-based and notice-and-choice mechanisms through inadequate federal privacy laws like COPPA and piecemeal, constitutionally problematic state privacy laws. It demands a reorientation of responsibility, one that distributes the burden across the full ecosystem of digital life. Privacy cannot be treated only as a commodity, and policymakers and companies cannot expect parents alone to police the perimeter of a playground they never chose for their children. As the failures of consent-based regimes and notice-and-choice frameworks have shown, the current model of privacy protection is fundamentally mismatched to the realities of how children engage with technology.

---

224 *Id.* at 1410.

225 MacDonald, *supra* note 92, at 591 (describing the recent laws in Arkansas, Texas, and California, all of which were either partially or totally blocked from enforcement "because they were enjoined as unconstitutional violations of the First Amendment").

226 Steinberg, *supra* note 6, at 443 ("State laws vary from state to state, some recognizing that young people need to be able to safely explore the internet while maintaining a right to privacy while other state laws prioritiz[e] giving parents control over a young person's internet use above all else. These varied laws are almost entirely in contrast with the international community's consensus on how children can be best protected in digital environments.").

The PFP model proposed in this Article offers a potential solution to the failures of federal and state privacy laws. It acknowledges the realities of market forces and consumer choice, while demanding baseline protections that ensure equity. A PFP floor must be guaranteed for all children, especially those whose families lack the economic leverage to buy their way into safety. Any framework that treats privacy as a premium feature will deepen existing inequities unless paired with equity-by-default and meaningful regulatory oversight. This Article calls for a collective framework that empowers regulators, equips parents, and enlists companies in shaping children's privacy norms. The village metaphor emphasizes that just as no caregiver can raise a child alone, no one institution can safeguard children's privacy.

Promoting and Protecting the Marketplace of Ideas in the AI Information Age

Jon M. Garon

CONTENTS

Promoting and Protecting the Marketplace of Ideas in the AI Information Age

*Jon M. Garon**

This Article focuses on the historical evolution of communications, primarily the rapid changes of the twenty-first century. The growth of video games, digital publishing, ebooks, video streaming, the metaverse, and synthetic media have undermined the innovations of the twentieth century from landlines to broadcasting. The shift to an influencer and creator economy has displaced mass media, devaluing media's gatekeepers and disaggregating the public. More than a technological change, the consequences have profound implications for the economic and legal structures that underpin society.

Using the metaphor of the marketplace of ideas, this Article addresses key legal implications for the regulation of content, protection of the public, and the need to recalibrate speech norms. This Article explores the history of the marketplace of ideas as understood by the drafters of the Bill of Rights and its evolution through the twentieth and twenty-first centuries as a means of focusing on the range of regulatory authority available to manage information in the age of AI.

* Jon M. Garon, Associate Dean for Technology and Innovation and Professor of Law, Nova Southeastern University Shepard Broad College of Law. Prepared in conjunction with the 2026 *Chapman Law Review* Annual Symposium. The author would like to thank his research assistants, Olivia McHenry and Isabella Randazzo, and the *Chapman Law Review* editorial staff, including Jack Mays and Riya Beri.

I. INTRODUCTION

There never was a Democracy Yet, that did not commit suicide.

— John Adams[1]

Every idea is an incitement. It offers itself for belief and if believed it is acted on unless some other belief outweighs it or some failure of energy stifles the movement at its birth. The only difference between the expression of an opinion and an incitement in the narrower sense is the speaker's enthusiasm for the result.

— Oliver Wendell Holmes Jr.[2]

Each historical era is defined and reshaped by the new technology of that age and the political consequences unleashed by its invention. The Gutenberg Press fueled the publication of indulgences in the Catholic Church and became the weapon of Martin Luther to launch the Protestant Reformation. For England, that conflict triggered civil war, the colonization of North America, and generations of European conflict.[3] In 1644, fresh from the bloodshed of that conflict, the British Parliament enacted a law to license the printing press and control its output.[4] Already famous for *Paradise Lost*, John Milton rose against the law in favor of free speech with arguments that later infused the U.S. Bill of Rights.

---

1 Letter from John Adams to John Taylor (Dec. 17, 1814), *in* THE ADAMS PAPERS (forthcoming), https://founders.archives.gov/documents/Adams/99-02-02-6371 [https://perma.cc/7AGK-XQZJ] ("It is in vain to Say that Democracy is less vain, less proud, less selfish, less ambitious or less avaricious than Aristocracy or Monarchy. It is not true in Fact and no where appears in history. Those Passions are the same in all Men under all forms of Simple Government, and when unchecked, produce the same Effects of Fraud Violence and Cruelty.").

2 Gitlow v. New York, 268 U.S. 652, 673 (1925) (Holmes, J., dissenting).

3 *See, e.g.*, Jane H. Ohlmeyer, *English Civil Wars*, BRITANNICA (Feb. 6, 2026), https://www.britannica.com/event/English-Civil-Wars [https://perma.cc/F6L5-8WR3]; *A Brief History of the 'Wars of the Three Kingdoms*,*'* SKY HIST., https://www.history.co.uk/articles/a-brief-history-of-the-wars-of-the-three-kingdoms [https://perma.cc/R4MY-AXJZ] (last visited Feb. 23, 2026) ("The English Civil War, with its violent clashes between Roundheads and Cavaliers, is a much-mythologised chapter in British history. Yet it was actually part of a larger arc of events known as the Wars of the Three Kingdoms (England, Scotland and Ireland) – which sprawled throughout much of the 17th Century."). *See generally* TREVOR ROYLE, THE BRITISH CIVIL WAR: THE WARS OF THE THREE KINGDOMS 1638–1660 (2004) (discussing the history of the interconnected conflicts across England, Scotland, and Ireland).

4 *See generally* THOMAS C. BERG, RELIGIOUS LIBERTY IN A POLARIZED AGE 119–33 (2023) (arguing that protecting religious freedom is key to combatting polarization in society).

The printing press was one of many inventions of the Industrial Revolution, ushering in a mercantile transformation of Europe. When combined with democratic reforms that evolved from the Protestant Reformation, the reforms and innovations created a capitalist-democratic compact that linked individual electoral power with individual value from labor. This eighteenth-century shift from the sovereign to the individual served as the framework for the American Revolution and for political transformation across the globe. Adam Smith described and defined the model by identifying the invisible hand of the marketplace. The marketplace grew to incorporate both goods and ideas, reshaping the meaning of speech free of censorship, as envisioned by John Milton and John Stuart Mill. The metaphor for a marketplace of ideas was born. In the market, ideas vie for survival of the fittest, which hopefully coincides with truth.

The marketplace of ideas was quickly eclipsed by emerging twentieth-century technology. Film, radio, and television were heavily regulated. For radio and television, the public interest doctrine operated as an express, government-controlled market.

In the Artificial Intelligence (AI) Information Age, both mass media and the public interest doctrine are fading into irrelevancy. The media of the masses has replaced mass media with few practical constraints over the production and dissemination of content. AI has the potential to fuel the content conflagration further and faster than any time in history.

Adam Smith's invisible hand is no longer capable of maintaining an equilibrium in the marketplace of ideas. The philosophical foundations for that marketplace would never have expected it to do so. The current approach by the Supreme Court emphasizes the importance of historical context for modern regulatory review. To help with this endeavor, this Article looks at the influences for content regulation that shaped the Bill of Rights and how those laws have evolved in the centuries since adoption.

A century after the marketplace of ideas reshaped political thought, AI and the exponential growth of the information economy require that society revisit the assumptions underlying the marketplace of ideas. By reflecting on the historical meaning of those foundational principles, this Article asserts that free speech can be protected within the context of the fundamental rights that were equally important, while still addressing the imbalance in the market. From this review, a new model emerges that can lift the invisible hand of the marketplace where needed

to counterbalance the agentic hand of AI automata that are not bound by human ethics, incentives, or needs.

Part II develops the current state of AI content and how that content differs from human-developed content. Part III explores the nature and consequences of the democratization of content, focusing on the evolution of the free speech doctrine during the twentieth century. Part IV explores where the presumptions inherent in twentieth-century free speech must be adapted to reflect the different nature of media, communications, and content that have derived from transformations in the information age.

II. THE INFORMATION AGE: NETWORKED, SOCIAL, AND SYNTHETIC

The combination of exponential growth in the power of computing, global internet-connected communications, wearable technology, and generative AI has come together to usher in a new information age that confounds the ability to predict the future. Since the 1990s, there have been at least three major technological transformations: the internet, social media, and AI.[5] In 2025, streaming usage grew larger than cable and broadcast television combined.[6] YouTube is the largest streaming platform for traditional television content—even before counting the videos and other user-generated content that are watched nearly as much as all television content.[7] "For many, watching YouTube videos has become part of their daily routine. 62% of internet us-

5 Nelson Granados, *How Artificial Intelligence Is Shaping the New Media and EntertAInment Economy*, FORBES (June 7, 2024, at 10:11 ET), https://www.forbes.com/sites/nelsongranados/2024/05/31/how-artificial-intelligence-is-shaping-the-new-media-and-entertainment-economy/ [https://perma.cc/2F7D-9AQN] ("First was the advent of the internet, which in the first decade of the 21st century enabled digital distribution of content, and in the second decade upended the distribution format from downloading to streaming, both live and on demand. The third wave is . . . AI.").

6 *Streaming Reaches Historic TV Milestone, Eclipses Combined Broadcast and Cable Viewing for First Time*, NIELSEN (June 17, 2025), https://www.nielsen.com/news-center/2025/streaming-reaches-historic-tv-milestone-eclipses-combined-broadcast-and-cable-viewing-for-first-time/ [https://perma.cc/JHD6-HN5F].

7 *See* Alex Sherman, *YouTube Dominates Streaming, Forcing Media Companies To Decide Whether It's Friend or Foe*, CNBC (June 26, 2024, at 11:38 ET), https://www.cnbc.com/2024/06/26/youtube-streaming-dominance-media-strategy.html [https://perma.cc/LAH4-FDPL]; Brad Adgate, *Most Young Adults Prefer Free User Generated Social Video than SVOD*, FORBES (Mar. 25, 2024, at 10:47 ET), https://www.forbes.com/sites/bradadgate/2024/03/25/most-young-adults-prefer-free-user-generated-social-video-than-svod/ [https://perma.cc/Z6AE-YA42]; Lyndon Bell, *YouTube: A Social Media Platform or Something More?*, ADLIFT (Apr. 28, 2025), https://www.adlift.com/blog/is-youtube-a-social-media/ [https://perma.cc/UHZ9-HLJF].

ers based in the United States report using YouTube every day. 92% access YouTube on a weekly basis . . . ."[8]

Along with these three changes, the dominant form of entertainment has been shifting toward video games. "The video game industry is $200-plus billion globally—larger than all of film, television and music combined."[9] "[T]here are more than 3 billion active gamers."[10]

The public's increased engagement with video games and the shift to streaming and short-form video is impactful, but minor in comparison to the growth of social media. Beginning in 2025, social media has overtaken both TV news and news websites as the primary source of news for many Americans.[11] "Americans turn to radio and print publications for news less frequently."[12] "In 2025, 11% of U.S. adults say they often get news from radio, and 7% say the same about printed newspapers or magazines . . . ."[13]

The most recent shift has only begun. Although generative AI systems have been under development for many years,[14] the commercial explosion began with the launch of ChatGPT in November 2022.[15] ChatGPT achieved more than 100 million users within two months of its launch, cementing the service's role as the leader in the emerging AI arms race.[16] Generative AI systems combine with other AI technologies to power humanoid robots, to

---

8 Bell, *supra* note 7.

9 Todd Harris, *Georgia's Got Game: Why the Gaming Industry Is Larger than Film, Television and Music Combined*, GA. ENT. (Apr. 16, 2024), https://www.georgiaentertainment.com/2024/04/georgias-got-game-why-the-gaming-industry-is-larger-than-film-television-and-music-combined/ [https://perma.cc/DB6M-9JZT].

10 *Id.*

11 *For the First Time, Social Media Overtakes TV as Americans' Top News Source*, NIEMAN LAB (June 16, 2025, at 19:02 PT), https://www.niemanlab.org/2025/06/for-the-first-time-social-media-overtakes-tv-as-americans-top-news-source/ [https://perma.cc/PLT6-NAXN] (highlighting changes in where Americans obtain their news: social media 54%, TV news 50%, news websites 48%).

12 Christopher St. Aubin & Jacob Liedke, *News Platform Fact Sheet*, PEW RSCH. CTR. (Sep. 25, 2025), https://www.pewresearch.org/journalism/fact-sheet/news-platform-fact-sheet/ [https://perma.cc/ZM2S-5TCJ].

13 *Id.*

14 *See, e.g.*, Jørgen Veisdal, *The Birthplace of AI: The 1956 Dartmouth Workshop*, MEDIUM: CANTOR'S PARADISE (Sep. 12, 2019), https://www.cantorsparadise.com/the-birthplace-of-ai-9ab7d4e5fb00 [https://perma.cc/TFK3-DNPA].

15 *See* Shelley Walsh, *Timeline of ChatGPT Updates & Key Events*, SEARCH ENGINE J. (Oct. 19, 2025), https://www.searchenginejournal.com/history-of-chatgpt-timeline/488370/ [https://perma.cc/SAN7-KZBF].

16 *See* Krystal Hu, *ChatGPT Sets Record for Fastest-Growing User Base – Analyst Note*, REUTERS (Feb. 2, 2023), https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/ [https://perma.cc/HU57-3SE9].

drive new research, and to fundamentally disrupt the modern workplace as industries seek to replace or redefine jobs in search of efficiency and profitability.[17] "[T]he tools are advancing with the integration of generative AI and agentic AI, bringing humanoid robots and other AI-enabled robotic devices out of the realm of science fiction and into modernized workplaces . . . ."[18]

Generative AI brings a particularly powerful challenge to journalism and creative industries. Multiple lawsuits assert that the AI publishers are free-riding off the newsgathering operations of others.[19] Other lawsuits focus on the harm to copyright owners and creative industries.[20] Generative AI can create an essentially unlimited flow of images, text, news, and social interaction. The consequences for those who make a living gathering news or creating original entertainment may be economically dire.

Also in 2025, the same year that social media eclipsed all other forms of media as the preferred source for news and information, Merriam-Webster announced that its official word of the year was "slop."[21] "We define *slop* as 'digital content of low quality that is produced usually in quantity by means of artificial intelligence.'"[22] Merriam-Webster referenced a commentary on CNET called *AI Slop Has Turned Social Media Into an Antisocial Wasteland*.[23]

---

17 *See* Madison Huang, *What Is NVIDIA's Three-Computer Solution for Robotics?*, NVIDIA: COMPANY BLOG (Aug. 8, 2025), https://blogs.nvidia.com/blog/three-computers-robotics/ [https://perma.cc/4WK2-Y6XH]; Tammy Whitehouse, *AI Robots in the Workplace: Preparing for Humanoid Colleagues*, WALL ST. J.: CIO J. (July 25, 2025, at 12:00 PT), https://deloitte.wsj.com/cio/ai-robots-in-the-workplace-preparing-for-humanoid-colleagues-a6753b0a?gaa [https://perma.cc/23UT-K6RF].

18 Whitehouse, *supra* note 17 (quoting Franz Gilbert).

19 *See, e.g.*, Dow Jones & Co. v. Perplexity AI, Inc., 797 F. Supp. 3d 305, 318–19 (S.D.N.Y. 2025) ("Plaintiffs assert two claims of copyright infringement pursuant to 17 U.S.C. § 106 (Counts I and II) and one claim for false designation of origin and dilution of Plaintiffs' trademarks pursuant to 15 U.S.C. § 1125 (Count III)."); Complaint at 1, N.Y. Times Co. v. Perplexity AI, Inc., No. 1:25-cv-10106 (S.D.N.Y. 2025).

20 *See* Cade Metz & Michael M. Grynbaum, *New York Times Sues A.I. Start-Up Perplexity over Use of Copyrighted Work*, N.Y. TIMES (Dec. 5, 2025), https://www.nytimes.com/2025/12/05/technology/new-york-times-perplexity-ai-lawsuit.html [https://perma.cc/KL8V-33EZ] ("Filed in federal court on Friday, the suit joins more than 40 other court disputes between copyright holders and A.I. companies.").

21 *2025 Word of the Year: Slop*, MERRIAM-WEBSTER (Dec. 14, 2025), https://www.merriam-webster.com/wordplay/word-of-the-year [https://perma.cc/WFS3-72CH].

22 *Id.*

23 Abrar Al-Heeti, *AI Slop Has Turned Social Media into an Antisocial Wasteland*, CNET (Nov. 19, 2025, at 05:01 PT), https://www.cnet.com/tech/services-and-software/ai-slop-has-turned-social-media-into-an-antisocial-wasteland/ [https://perma.cc/TM92-V3MG].

To focus on the AI slop, however, is to ignore the transformative potential for generative AI across the media landscape. Within the entertainment industry, leaders have "predicted that AI will enable new business processes and content production workflows that are faster and leaner."[24] TV and film production workflows use AI to create storyboards and previsualization videos at a fraction of the cost and time for completion.[25]

AI also democratizes the creation process. Anyone can input a prompt to generate a picture, short video, story, or musical composition.[26] In its formative stage, the public is not yet completely on board. "Opinions are mixed – ranging from awe at AI's capabilities to skepticism about its originality and emotional depth."[27] "Many creators acknowledge AI's utility but doubt it can fully replicate human creativity."[28]

AI is not only the most recent development in the democratization of content. Social media has played an exceptionally important role as well. Before them, internet, television, radio, and the camera each played a part. But the origins begin with the commercial printing press.

The democratization of content raises two fundamental questions. The first is how society values and evaluates the works created. The second is how society evaluates and contextualizes trust in the technology and media. To return to the metaphor, what makes the marketplace work?

III. TECHNOLOGY AND THE EVOLUTION OF DEMOCRATIZATION IN CONTENT CREATION

Technology has infused and transformed communication since before there were written words. Rocks and skins served as percussion instruments; reeds and hollowed tubes provided flutes; a ram's horn was hollowed out as a trumpet (or shofar); and dried animal intestines enabled the creation of lutes and other stringed instruments.[29] There are archeological remains from nearly 800,000 years ago suggesting that "[s]tories were

---

24 Granados, *supra* note 5.

25 *See id.*

26 *See How AI Is Reshaping Art, Music and Brand Storytelling*, AMPLYFI (Apr. 17, 2025), https://amplyfi.com/blog/how-ai-is-reshaping-art-music-and-brand-storytelling/ [https://perma.cc/TZ5F-8H4T] ("One of AI's most profound impacts is the democratisation of content creation.").

27 *Id.*

28 *Id.*

29 Anton Killin, *The Origins of Music: Evidence, Theory, and Prospects*, 1 MUSIC & SCI. 1, 6 (2018).

frequently accompanied by background music (often performed on musical bows)."[30] Flutes made from bird bones exist from over 40,000 years ago.[31] Writing, in contrast, likely originated only 6,000 years ago.[32]

"Creativity is deeply rooted in all cultures, but its definition and attributes vary across cultures."[33] The technologies of writing, art, and creative works shape human culture and are, in turn, shaped by their culture.[34] Marshall McLuhan explained the relationship between the tools of communication and the content of that communication: "Taken in the long run, the medium is the message."[35] Unstated in this observation is the corollary that each technological innovation has expanded the reach of the speaker to the audience and provided access to new voices vying to compete in the marketplace of ideas.[36]

Context also matters. Western or individualistic cultures tend to celebrate and promote novelty, while Eastern or collectivist cultures value usefulness as the most significant characteristic.[37] This alone suggests that there may be a difference in how AI-generated works are valued in individualistic cultures versus

---

30 *Id.* at 4.

31 *Id.*

32 Ira Spar, *The Origins of Writing*, THE METRO. MUSEUM OF ART (Oct. 1, 2004), https://www.metmuseum.org/essays/the-origins-of-writing [https://perma.cc/5KR4-4GTW] (noting that "proto-cuneiform writing on clay and wood may have existed in Syria and Turkey as early as the mid-fourth millennium B.C.").

33 Yong Shao et al., *How Does Culture Shape Creativity? A Mini-Review*, 10 FRONTIERS IN PSYCH. 1, 2 (2019); *see also* Shilian Shan, *The "Boundary" of Technology, Culture, and Digitalization*, 2 EMERGING MEDIA 34, 42–44 (2024) (noting that culture shapes humanity and its attributes).

34 MARSHALL MCLUHAN, UNDERSTANDING ME: LECTURES AND INTERVIEWS 3 (Stephanie McLuhan & David Staines eds., 2003).

35 *Id.*

> So that when, by group action, a society evolves a new medium like print or telegraph or photo or radio, it has earned the right to express a new message. And when we tell the young that this new message is a threat to the old message or medium, we are telling them that all we are striving to do in our united social and technical lives is destructive of all that they hold dear. The young can only conclude that we are not serious. And this is the meaning of their decline of attention.

Id.

36 G. Michael Parsons, *Fighting for Attention: Democracy, Free Speech, and the Marketplace of Ideas*, 104 MINN. L. REV. 2157, 2166 (2020) ("The fact that consuming content (and producing it) takes time and attention is another axiom that complicates the Court's modern market metaphor.").

37 Shao et al., *supra* note 33 ("The plausibility of such clustering of the East and the West has been substantially supported by several large-scale studies, such as the World Value Survey and the GLOBE project survey." (citations omitted)).

collectivist cultures, with the latter potentially being more receptive to useful generative AI works even if the works do not possess a human's originality or novelty.

Individualism is not an inherent cultural characteristic. Western individualism has a lineage rooted in the technology of communication, specifically the printed text. "Printing was invented over a millennium ago, around the year 700, in China during the Tang dynasty (618–907 [C.E]), before it spread across East Asia, Southeast Asia and the globe . . . ."[38] The first known printed book is *The Diamond Sutra*, published in Sanskrit in approximately 868 C.E.[39] Printing slowly made its way across Europe, but hand-carved wooden type and inefficient presses did not significantly displace scriveners who could create far more elaborate, elegant works.

As commercial trade slowly grew across Europe, however, the market for lower-cost books created an opportunity for improvement. Johannes Gutenberg (1400–1468), who likely had training as a metalsmith, undertook to improve the speed and efficiency of the rudimentary presses available at the time.[40] His most important innovation was the introduction of metal block letters that could be arranged into any word, sentence, paragraph, or page by arranging them in a composing stick, a small, adjustable tray used by typesetters to arrange the lines of text.[41] To improve pressure on the paper, he adapted the screw mechanism of a wine press to get a stronger and more uniform distribution of pressure. He also developed an oil-based ink to improve the flow and saturation of the ink onto the page.[42]

---

38 Ryan Wolfson-Ford, *The History of Printing in Asia According to Library of Congress Asian Collections – Part 1*, LIBR. OF CONG.: BLOGS (June 22, 2021), https://blogs.loc.gov/international-collections/2021/06/the-history-of-printing-in-asia-according-to-library-of-congress-asian-collections-part-1/ [https://perma.cc/99G3-77X5].

39 *Printing Press*, HIST. (Feb. 27, 2025), https://www.history.com/articles/printing-press [https://perma.cc/7HHC-R3HC]; *Buddhist Diamond Sutra*, STAN. HUMANITIES CTR. (Aug. 1, 2009), https://shc.stanford.edu/stanford-humanities-center/news/buddhist-diamond-sutra [https://perma.cc/W9DH-RUNA].

40 Joshua J. Mark, *Johannes Gutenberg*, WORLD HIST. ENCYC. (July 25, 2022), https://www.worldhistory.org/Johannes_Gutenberg/ [https://perma.cc/BZE5-7UW2] ("Although the city of Mainz declared 1400 as Gutenberg's official year of birth in 1900, the date is unknown and generally held to be between 1394-1404.").

41 *The Gutenberg Press*, SPECIAL COLLECTIONS & ARCHIVES RSCH. CTR.: TREASURES OF THE MCDONALD COLLECTION, https://scarc.library.oregonstate.edu/omeka/exhibits/show/mcdonald/incunabula/gutenberg/ [https://perma.cc/XW57-6C5X] (last visited Feb. 23, 2026).

42 *See id.*; *Printing Press*, *supra* note 39.

By 1450, the press was operational.[43] Gutenberg published the prophetic poem, *The Sibyl's Prophecy*, as the first work on the press.[44] In 1454, Gutenberg began to operate the press commercially, "producing thousands of indulgences for the Church. The following year he printed his famous 42-line Bible, the first book printed on a moveable type press in the West."[45] Gutenberg's press opened a new market: "The first printing press came to London in 1476, and by 1500, there were five printers in London. By 1523, there were at least 33 printers and booksellers actively engaged in the trade."[46]

Printing and commercial trade continued to expand during the politically tumultuous period that followed its introduction. The rapid collection and dissemination of knowledge fueled both political upheaval and technological advancement.[47]

The industrial and technological advances began to grow exponentially. The steam engine, first identified in ancient Rome, was commercialized to power factories and railroads.[48] Steam engines made railway systems practical.[49] An engine for spinning cotton or wool was patented in 1770.[50] Scientists explored the development of electricity, magnetism, and radio waves throughout the seventeenth and eighteenth centuries. Wire-based telegraphs began in 1837.[51] In 1895, Guglielmo Marconi sent the first coded wireless message, and Nikola Tesla obtained the first radar patent in 1900.[52] Rapid advances in wireless and other technologies led to the development of commercial radio, telephones, motion

43 Mark, *supra* note 40.

44 *Id.*; *see* JON M. GARON, HOW AI, METAVERSES, CRYPTO, AND CYBER WILL UPEND THE 21ST CENTURY 37 (2024).

45 *The Gutenberg Press*, *supra* note 41.

46 Jessica Buck, *Moving On: From Manuscript to Movable Type*, COME LIVE WITH ME (Feb. 18, 2023), https://comelivewithmeballad.com/moving-on-from-manuscript-to-movable-type [https://perma.cc/EXL2-6VEK].

47 *See generally* Tristan Hughes, *10 Key Inventions During the Industrial Revolution*, HIST. HIT (Sep. 14, 2021), https://www.historyhit.com/key-inventions-of-the-industrial-revolution [https://perma.cc/4RBD-7BC2] (describing inventions from dynamite to the steam engine as stimuli for political and scientific change).

48 *Id.*

49 *See id.*

50 *Id.*

51 *See id.*

52 Pat Hindle, *History of Wireless Communications*, MICROWAVE J. (July 22, 2015), https://www.microwavejournal.com/articles/24759-history-of-wireless-communications [https://perma.cc/S8GZ-BTCX].

pictures, and the oscilloscope, which later became the basis for cathode ray tubes used to receive television signals.[53]

A. The Twentieth Century

Throughout the process, published books, newspapers, and pamphlets enabled researchers to learn from each other and to compete for public attention and financial resources. The Industrial Revolution was supported, at least to a small degree, through "issuing journals with articles on practical inventions and instructions for manufacturing and agriculture."[54]

Those living during the beginning of the twentieth century experienced a world fundamentally different from the previous generations. With wireless technology, the United States entered the industrialization race. David Sarnoff, general manager of Radio Corporation of America (RCA), saw the potential to create mass media networks. He created and described "a chain of national broadcasting stations . . . simultaneously radiating the same program . . . reach[ing] every city . . . [as] a national service."[55]

Sarnoff's RCA built the National Broadcasting Corporation (NBC), operating two national networks.[56] As RCA's president, he led the company to dominate radio broadcasting and lead the production of television.[57] Sarnoff's chief competitor was William Paley. Paley recognized the potential of radio as an advertising medium after he purchased some radio advertising for his fami-

---

53 *See id.*; Jon M. Garon, *Hidden Hands that Shaped the Marketplace of Ideas: Television's Early Transformation from Medium to Genre*, 19 U. DENV. SPORTS & ENT. L.J. 29, 36 (2016).

54 Erik Hornung, Julius Koschnick & Francesco Cinnirella, *The Importance of Access to Knowledge for Technological Progress in the Industrial Revolution*, CTR. FOR ECON. POL'Y RSCH.: VOXEU COLUMN (Dec. 6, 2022), https://cepr.org/voxeu/columns/importance-access-knowledge-technological-progress-industrial-revolution [https://perma.cc/RE7L-YLV9].

55 JEROME B. WIESNER, *Foreword* to DAVID SARNOFF, LOOKING AHEAD, at viii (1968) (quoting letters of David Sarnoff); *see also* ROBERT CAMPBELL, THE GOLDEN YEARS OF BROADCASTING: A CELEBRATION OF THE FIRST 50 YEARS OF RADIO AND TV ON NBC 29 (1976) (noting that Sarnoff predicted that broadcasting would be necessary to "entertain a nation").

56 *See, e.g.*, FCC, No. 5060, REPORT ON CHAIN BROADCASTING (1941) [hereinafter CHAIN BROADCASTING REPORT]; *see also* Nat'l Broad. Co. v. United States, 319 U.S. 190, 197 (1943) (explaining that a sizable number of stations were affiliated with or operated by NBC).

57 *See* CHAIN BROADCASTING REPORT, *supra* note 56, at 10, 19; GEORGE EVERSON, THE STORY OF TELEVISION: THE LIFE OF PHILO T. FARNSWORTH 251 (1st ed. 1949) ("David Sarnoff, taking the leadership for the industry, reported to the F.C.C. that his company had spent $10,000,000 on television development and others had also spent large sums for the same purpose, and he urged the [FCC] to take some action.").

ly's cigar business.[58] In 1928, within a year of his first ad purchase, Paley had taken over the station as its president. Renamed the Columbia Broadcasting System (CBS), Paley moved the enterprise to New York and focused on advertising sales as the revenue model for the new business, focusing on the star power of New York to attract audiences and advertisers.[59]

Through their common vision and fierce rivalry, Sarnoff and Paley shaped the growth of radio and television, investing in independent broadcast journalism and a national model for new content. The Federal Trade Commission (FCC) had strong concerns about the monopoly power held by CBS and NBC. In particular, NBC had two networks, known as the Red network and Blue network, which provided even greater reach than CBS.[60] Through regulatory rulemaking, the FCC forced NBC to divest itself of one of its two network syndicates. The spin-off of the Blue network became the American Broadcasting Company (ABC).[61] CBS, NBC, and ABC defined and exemplified the mass media of the twentieth century.

The three networks were later joined by Fox and cable-based services in the 1970s and 1980s.[62] Most original content flowed through the television networks. The motion picture industry did not compete as a news source, and film companies came to rely on television rebroadcasts for much of their income. Newspapers and magazines also provided news, but none had the reach of a television network.

The concentration of media ownership combined with the regulatory power of broadcast license reviews, public oversight, and the need to access governmental officials as news sources in-

---

58 *See William S. Paley*, BRITANNICA, https://www.britannica.com/biography/William-S-Paley [https://perma.cc/J8TH-USJ7] (last visited Mar. 17, 2026).

59 *See id.*

60 CHAIN BROADCASTING REPORT, *supra* note 56, at 15; *see also Nat'l Broad. Co.*, 319 U.S. at 197–98 (describing the FCC's findings that by 1938, NBC and CBS dominated national broadcasting).

61 *See* Comment, *Radio Program Controls: A Network of Inadequacy*, 57 YALE L.J. 275, 282 n.37 (1947).

62 Larry Schweikart, *Fox Television Network Goes on the Air*, EBSCO (2023), https://www.ebsco.com/research-starters/history/fox-television-network-goes-air [https://perma.cc/24TE-L3M9] ("The Fox Television Network, launched on October 9, 1986, marked a significant development in the U.S. television landscape by establishing a fourth major broadcast network."); Luke Bouma, *53 Years Ago Today HBO First Launched Changing Cable TV for Ever*, CORD CUTTERS NEWS (Nov. 8, 2025), https://cordcuttersnews.com/53-years-ago-today-hbo-first-launched-changing-cable-tv-for-ever/ [https://perma.cc/MW6Q-ZCBR] (highlighting that, launched in 1972, HBO introduced pay-per-view in 1975 and began producing original content in 1983).

variably led to an institutionalist homogeneity in news and entertainment content.[63] The concentration was not only of the market; it reflected a perspective that was congruent with those who hold power and influence in society.[64] A global phenomenon, the leaders of the media industry both support and are supported by the political and economic leaders with whom they share common backgrounds, education, and economic incentives.[65] "[M]assmedia performance. . . . is much closer to a 'free market' . . . [driven by] the workings of market forces. Most biased choices in the media arise from the preselection of right-thinking people, internalized preconceptions, and the adaptation of personnel to the constraints of ownership, organization, market, and political power."[66]

In many ways, the same forces that create an institutionalist, homogenous mass media reflect the same invisible hand of market balance described by Adam Smith and are sufficient to allow the marketplace of ideas to maintain its equilibrium, if not its pursuit of truth. The marketplace, like the limitations of mass media, is not designed to pursue truth in any objective fashion. The forces align to promote consensus and stability. Markets punish outliers.[67]

As Part II noted, the mass media marketplace dominated the twentieth century until it was recently supplanted by the combination of the internet, social media, and generative AI. The Industrial Revolution and the television age have now been supplanted by the AI era.

---

63 Stephen D. Reese & Jae Kook Lee, *Understanding the Content of News Media*, *in* THE SAGE HANDBOOK OF POLITICAL COMMUNICATION 753 (Holli A. Semetko & Margaret Scammell eds., 2012).

64 *See id.*

65 EDWARD S. HERMAN & NOAM CHOMSKY, MANUFACTURING CONSENT: THE POLITICAL ECONOMY OF THE MASS MEDIA 2 (The Bodley Head 2008) ("The elite domination of the media and marginalization of dissidents . . . occurs so naturally that media news people, frequently operating with complete integrity and goodwill, are able to convince themselves that they choose and interpret the news 'objectively' and on the basis of professional news values.").

66 *Id.* at L.

67 *See, e.g.*, Abbas Valadkhani, *A Multi-Pronged Analysis of Common and Market-Specific Equity Outliers Across the G7, China, and Global Markets Using Country ETFs*, 74 FIN. RSCH. LETTERS, no. 106771, 2025, at 1, 4.

B. The Consequences of Democratizing Thought: The Early Years

In discussing the technological revolution of the television, space race, and age of electricity, Marshall McLuhan highlighted the structural transformation that such inventions brought to society. "Print created individualism and nationalism in the sixteenth century."[68] The press also triggered a series of political revolutions.

The press did far more than further the Industrial Revolution and the innovations that followed. The individualism and nationalism resulting from the press and the Protestant Reformation redefined society itself.

Gutenberg's press triggered a large-scale publication of indulgences by the Catholic Church, in which absolution was granted in exchange for the purchase (or donation) of the document. In 1517, appalled by the Church's practice of selling indulgences, Martin Luther published *Disputation on the Power of Indulgences*, or *95 Theses*.[69] That same day, Luther sent a letter to the Archbishop of Mainz, Albert of Brandenburg. In the letter and the *Disputation*, Luther attacked the practice of selling indulgences that had flourished using Gutenberg's press.[70] The invention and the industry it spawned created a market for new books, new authors, new ideas, and new economic opportunities.[71] Luther himself was a prolific publisher, taking full advantage of the tools used by his opponents to call for reform.[72]

The Protestant Reformation focused on the individual's relationship to the Catholic Church and to God.[73] "Broadly speaking, most of the challenges to the Catholic Church revolved around the notion that individual believers should be less dependent on the Catholic Church, and its pope and priests, for spiritual guidance and salvation. Instead, Protestants believed people should

---

68 MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN 19–20 (MIT Press 1994).

69 *See* Eric W. Gritsch, *1517 Luther Posts the 95 Theses*, CHRISTIAN HIST. INST., https://christianhistoryinstitute.org/magazine/article/luther-posts-theses [https://perma.cc/W2WE-DAKG] (last visited Mar. 21, 2026); David B. Morris, *Martin Luther as Priest, Heretic and Outlaw*, LIBR. OF CONG.: RSCH. GUIDES (Dec. 6, 2023), https://guides.loc.gov/martin-luther-priest-heretic-outlaw [https://perma.cc/K36M-5H9B].

70 *Id.*

71 ELIZABETH L. EISENSTEIN, THE PRINTING PRESS AS AN AGENT OF CHANGE 33 (1979).

72 *See* Louise W. Holborn, *Printing and the Growth of a Protestant Movement in Germany from 1517 to 1524*, 11 CHURCH HIST. 123, 124 (1942).

73 *See* Freddie Wilkinson, *The Protestant Reformation*, NAT'L GEOGRAPHIC (Jan. 22, 2025), https://education.nationalgeographic.org/resource/protestant-reformation/ [https://perma.cc/NWN4-852C].

be independent in their relationship with God . . . ."[74] In England, sects within the Protestant movement included Puritan separatists, some of whom traveled to North America aboard the Mayflower and became the United States' early settlers, as did other separatist groups.[75] For England, the religious and political tensions triggered a series of civil wars and conflicts with Ireland, Scotland, and Cornwall, leading to the execution of King Charles I, the failure of the commonwealth, and significant loss of life.[76]

England was not alone. "The 17th century was among the most chaotic and destructive the continent of Europe had ever witnessed in the modern era. From 1618-1648, much of Central Europe was caught in the throes of the Thirty Years War, the violent breakup of the Holy Roman Empire."[77]

Against this backdrop, philosophers Thomas Hobbes and John Locke struggled to articulate the role of the individual in society.[78] The reformation of religious thought created new thinking on the role of the individual within the greater society. Civil wars and political conflict challenged philosophers to rethink the relationship between sovereignty and those governed. To answer the question, both Hobbes and Locke explore the nature of the individual.

Having lived through the English Civil Wars, Hobbes's answer was simple. "[H]uman beings . . . . are all basically selfish, driven by fear of death and the hope of personal gain . . . ."[79] Hobbes saw life as a perpetual warring state. Without an absolute monarch to protect against unrest, a person's life would inevitably be "solitary, poore, nasty, brutish, and short."[80]

---

74 *Id.*

75 *Id.*

76 *See* Paul Pattison, *The English Civil Wars*, ENG. HERITAGE, https://www.english-heritage.org.uk/learn/histories/the-english-civil-wars-history-and-stories/the-english-civil-wars/ [https://perma.cc/PMB5-25K8] (last visited Feb. 23, 2026) ("It is estimated that as many as one in four adult men, from a total population of about 4.5 million people, took up arms and up to 200,000 civilians (men, women and children) and soldiers lost their lives from fighting and diseases spread by moving armies – 4.5% of the population.").

77 Matthew Shea, *Hobbes, Locke, and the Social Contract*, AM. BATTLEFIELD TR. (July 28, 2025), https://www.battlefields.org/learn/articles/hobbes-locke-and-social-contract [https://perma.cc/ET9U-LY8F].

78 *Id.* ("This had the side effect of producing two of the brightest political minds in the English philosophical tradition: Thomas Hobbes (1588-1679) and John Locke (1632-1704).").

79 NIGEL WARBURTON, A LITTLE HISTORY OF PHILOSOPHY 57–58 (2011).

80 THOMAS HOBBES, LEVIATHAN 102 (G.A.J. Rogers & Karl Schuhmann eds., 2005) (1651).

> Whatsoever therefore is consequent to a time of Warre, where every man is Enemy to every man; the same is consequent to the time wherein men live

Liberty for the individual was the postulate that "each man hath, to use his own power, as he will himselfe, for the preservation of his own Nature; that is to say, of his own Life; and consequently, of doing any thing, which in his own Judgement, and Reason, hee shall conceive to be the aptest means thereunto."[81]

John Locke responded to Hobbes with a fundamentally different understanding of humanity. While they mutually agreed that the natural state of a person was unfettered freedom, Locke argued the natural right was an inalienable right that should not and could not be subordinated to a sovereign, except by the consent of the governed.[82] "Locke used the claim that men are naturally free and equal . . . as the result of a social contract where people in the state of nature conditionally transfer some of their rights to the government in order to better ensure the stable, comfortable enjoyment of their lives, liberty, and property."[83]

Locke's arguments pervade the Declaration of Independence, the structure of the U.S. Constitution, and the protections in the Bill of Rights.[84] These themes include the separation of powers; protection of life, liberty, and estate; and the importance of impartial adjudication.[85] Locke also explained that one owns a

---

> without other security, than what their own strength, and their own invention shall furnish them withall. In such condition, there is no place for Industry; because the fruit thereof is uncertain: and consequently no Culture of the Earth; no Navigation, nor use of the commodities that may be imported by Sea; no commodious Building; no Instruments of moving, and removing such things as require much force; no Knowledge of the face of the Earth; no account of Time; no Arts; no Letters; no Society; and which is worst of all, continuall feare, and danger of violent death; And the life of man, solitary, poore, nasty, brutish, and short.

Id.

81 *Id.* at 104.

82 JOHN LOCKE, TWO TREATISES OF GOVERNMENT 326 (Peter Laslett ed., Cambridge Univ. Press 1988) (1690) ("[T]hat *Absolute Monarchy*, which by some Men is counted the only Government in the World, is indeed *inconsistent with Civil Society* . . . ."); Alex Tuckness, *Locke's Political Philosophy*, STAN. ENCYC. OF PHIL. (Oct. 6, 2020), https://plato.stanford.edu/entries/locke-political/ [https://perma.cc/2QY2-YX8N].

83 Tuckness, *supra* note 82.

84 *See* Rob Natelson, *The Ideas That Formed the Constitution, Part 16: John Locke and the Ninth Amendment*, INDEP. INST. (Feb. 10, 2023), https://i2i.org/the-ideas-that-formed-the-constitution-part-16-john-locke-and-the-ninth-amendment/ [https://perma.cc/PG6L-PH4C] ("John Locke (1632–1704) was one of the greatest figures in English scholarship. His influence on the American Founding was enormous. Some have referred to him as a 'Founding Grandfather.'").

85 Eleanor Stratton, *Locke's Influence on the Constitution*, USCONSTITUTION.NET (June 30, 2024), https://www.usconstitution.net/lockes-influence-on-the-constitution/ [https://perma.cc/9QJ9-HBS3].

property right in one's own labor, a concept often used to inform copyright and patent theories.[86]

> Though the Earth, and all inferior Creatures be common to all Men, yet every Man has a *Property* in his own *Person*. This no Body has any Right to but himself. The *Labour* of his Body, and the *Work* of his Hands, we may say, are properly his. Whatsoever then he removes out of the State that Nature hath provided, and left it in, he hath mixed his *Labour* with, and joyned to it something that is his own, and thereby makes it his *Property*. . . . For this *Labour* being the unquestionable Property of the Labourer, no Man but he can have a right to what that is once joyned to, at least where there is enough, and as good left in common for others.[87]

Locke's view of labor has often been overstated,[88] but the simple approach explains the role of the farmer, rancher, and craftsperson quite well. Here is a simple example: A tree stands in nature. When skilled artisans apply their craft to the wood, it creates objects now owned by those artisans. The focus is on the effort and skill, just as it applies to authors and inventors. Most importantly, the finished wooden table does not belong to the feudal lord simply because the tree grew on that lord's property. Like other property rules, there are limitations and exceptions. Nonetheless, Locke's views on press and property, like those of Milton, played an important role in the minds of Thomas Jefferson, John Adams, Alexander Hamilton, and others as they crafted the Bill of Rights.

In addition, the economic philosophy of Adam Smith also influences the marketplace of ideas. Publishing *An Inquiry into the Nature and Causes of the Wealth of Nations* in 1776, Smith described a competition in marketplaces reflecting a survival of the fittest economic competitors. He emphasized that competition in markets—fueled by the natural inclination of self-interest—would lead to efficient use of capital. In other words, competition for goods and services would reward those who produced them with the highest value.[89] Smith described an "invisi-

---

86 *See* Robert P. Merges, *Locke for the Masses: Property Rights and the Products of Collective Creativity*, 36 HOFSTRA L. REV. 1179, 1180 (2008).

87 LOCKE, *supra* note 82, at 287–88.

88 *See* Mala Chatterjee, *Lockean Copyright Versus Lockean Property*, 12 J. LEG. ANALYSIS 136, 136 (2020).

89 *See* ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 423 (Edwin Cannan ed., Modern Library 1937) (1776) ("[I]t is only for the sake of profit that any man employs a capital in the support of industry; and he will always, therefore, endeavour to employ it in the support of that industry of which the produce is likely to be of the greatest value . . . .").

ble hand" guiding markets that would align self-interest into self-regulating, efficient markets.[90] Instead of a battlefield, one could infer from Smith that ideas could compete in the marketplace. Self-interest, however, was not necessarily brutish. "Smith rejected the cynical Hobbesian view that a state of nature is a 'war of all against all,' and held, with Locke, that people are by nature cooperative as well as competitive."[91]

Trying to understand the meaning of the provisions of the First Amendment is sometimes difficult because the constitutional framers avoided lengthy debates on it.[92] Instead, lessons can be learned from the sources used by the framers. This is particularly important for the Free Speech Clause because of the constraints placed on speech in Britain. Since the inception of the commercial printing press in England, authority to control publications has been held by the Star Chamber.[93] However, during the short-lived English Commonwealth, the British government set out to control the threat it perceived from the printing of propaganda and broadsides that were used to fuel the passions of the populace during the Civil Wars. In 1643, Parliament passed a law requiring a license to own a printing press and gave the government the power to review the content of publications prior to their dissemination.[94]

John Milton strongly objected to the Commonwealth's efforts to continue licensing the printing press.

> I deny not, but that it is of greatest concernment in the Church and Commonwealth, to have a vigilant eye how Bookes demeane themselves as well as men; and thereafter to confine, imprison, and do sharpest justice on them as malefactors: For Books are not absolutely

---

90 *Id.*

91 Toni Vogel Carey, *Don't Blame Adam Smith*, PHIL. NOW, May–June 2009, at 19, 20.

92 *See, e.g.*, *Amdt1.7.1 Historical Background on Free Speech Clause*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt1-7-1/ALDE_00013537/ [https://perma.cc/7FPX-NHMA] (last visited Feb. 22, 2026) ("There was relatively little debate over the speech and press clauses in the House, and there is no record of debate over the clauses in the Senate.").

93 *See* Martin Gruberg, *Star Chamber*, FREE SPEECH CTR. (May 22, 2025), https://firstamendment.mtsu.edu/article/star-chamber/ [https://perma.cc/29M8-V2RP] ("The Star Chamber has its origins in the English institution of the same name that tried people too powerful to be brought before the ordinary common-law courts . . . . The jurisdiction of the Star Chamber included forgery, perjury, riots, maintenance, fraud, libel, and conspiracy.").

94 Kevin R. Davis, *Printing Ordinance of 1643 (1643)*, FREE SPEECH CTR. (July 2, 2024), https://firstamendment.mtsu.edu/article/printing-ordinance-of-1643/ [https://perma.cc/ZZ3X-UFDK] ("The 1643 'Ordinance for correcting and regulating the Abuses of the Press' completed Parliament's takeover of the licensing of printers in Britain.").

> dead things, but doe contain a potencie of life in them to be as active as that soule was whose progeny they are; nay they do preserve as in a violl the purest efficacie and extraction of that living intellect that bred them. . . . And yet on the other hand unlesse warinesse be us'd, as good almost kill a Man as kill a good Book; who kills a Man kills a reasonable creature, Gods Image; but hee who destroyes a good Booke, kills reason it selfe . . . .
>
> . . . .
>
> . . . And though all the windes of doctrin were let loose to play upon the earth, so Truth be in the field, we do injuriously, by licencing and prohibiting to misdoubt her strength. Let her and Falshood grapple; who ever knew Truth put to the wors, in a free and open encounter. Her confuting is the best and surest suppressing.[95]

Under Milton, truth will inevitably emerge as the victor on the battlefield of fighting faiths, or perhaps be better understood to mean that whatever reigns victorious in the battle will be the accepted wisdom of the age.

The first major test for the First Amendment came shortly after the Bill of Rights was enacted. John Adams' Federalist Congress enacted four laws, which together formed the Alien and Sedition Acts, embroiling the U.S. election of 1800 with the French Revolution. Thomas Jefferson was considered a strong supporter of the French Revolution, and the laws were a clear political attempt to attack Jefferson's political support in his bid to unseat Adams. Jefferson, along with James Madison, responded by drafting the Virginia and Kentucky resolutions to promote states' rights. In the Virginia and Kentucky resolutions, they went so far as to suggest that the new Constitution was another compact, no different than the Articles of Confederation, making federal laws subject to rejection by the individual states. As part of this effort, Madison and Jefferson highlighted that the Alien and Sedition Acts violated the Free Speech Clause of the First Amendment and "encroached on the reserved rights of the states."[96] After winning the election, Jefferson and his party repudiated the Alien and Sedition Acts, partially repealing them and refunding the fines collected against his political supporters.

The understanding of the First Amendment was next developed during World War I. The constitutional limitation had done

---

95 JOHN MILTON, AREOPAGITICA; A SPEECH OF MR. JOHN MILTON FOR THE LIBERTY OF UNLICENC'D PRINTING, TO THE PARLAMENT OF ENGLAND 4, 35 (1644).

96 PETER S. ONUF, JEFFERSON'S EMPIRE: THE LANGUAGE OF AMERICAN NATIONHOOD 95 (2000); David Harding, *Thomas Jefferson's Conception of States' Rights*, 33 AM. STUD. SCANDINAVIA 3, 7 (2001).

little to stop government laws from criminalizing seditious libel and other political speech. In 1916, President Woodrow Wilson proposed the Espionage Act, "the first law targeting disloyal expression since the infamous Sedition Act of 1798,"[97] which was enacted the next year.[98] The Supreme Court upheld the law in a series of decisions authored by Justice Oliver Wendell Holmes.[99] In *Schenck*, Justice Holmes proclaimed his understanding of the limits of the First Amendment:

> [I]n many places and in ordinary times the defendants in saying all that was said in the circular would have been within their constitutional rights. But the character of every act depends upon the circumstances in which it is done. The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic. It does not even protect a man from an injunction against uttering words that may have all the effect of force. The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent. It is a question of proximity and degree. When a nation is at war many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight and that no Court could regard them as protected by any constitutional right.[100]

Previously, writing for the Massachusetts Supreme Court, Justice Holmes had a similarly cavalier attitude toward the First Amendment. Explaining why a police officer could be fired for political activity, Justice Holmes wrote, "[t]he petitioner may have a constitutional right to talk politics, but he has no constitutional right to be a policeman."[101]

Nonetheless, as the echoes of World War I faded, Justice Holmes pulled the First Amendment toward the thinking of John Milton and perhaps even the natural law of John Locke. Writing in dissent about yet another of the convictions under the Espionage Act, Justice Holmes evoked that understanding of Milton in his famous dissent in *Abrams v. United States*.[102] He rejected the

---

97 Philip A. Dynia, *World War I*, FREE SPEECH CTR. (July 2, 2024), https://firstamendment.mtsu.edu/article/world-war-i/ [https://perma.cc/EH47-YYS2].

98 18 U.S.C. §§ 792–799.

99 *See* Schenck v. United States, 249 U.S. 47, 52–53 (1919); Frohwerk v. United States, 249 U.S. 204, 209 (1919); Debs v. United States, 249 U.S. 211, 215–16 (1919).

100 *Schenck*, 249 U.S. at 52 (citations omitted).

101 McAuliffe v. Mayor of New Bedford, 29 N.E. 517, 517 (Mass. 1892).

102 250 U.S. 616, 629–30 (1919) (Holmes, J., dissenting).

notion that the speech was dangerous, except perhaps to the extent that all opposing views carry a danger within them.[103]

Justice Holmes added an important philosophical gloss to the battle over ideas by suggesting there is a "free trade in ideas" and a competitive market for the best among them.[104]

> Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition. To allow opposition by speech seems to indicate that you think the speech impotent, as when a man says that he has squared the circle, or that you do not care wholeheartedly for the result, or that you doubt either your power or your premises. But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution. It is an experiment, as all life is an experiment. Every year if not every day we have to wager our salvation upon some prophecy based upon imperfect knowledge.[105]

First Amendment jurisprudence evolved very slowly. The turning point came through another aspect of constitutional protection, when the Supreme Court unanimously held that racial segregation of schools deprived students of the equal protection of the laws guaranteed by the Fourteenth Amendment.[106] A decade later, the Court in *New York Times Co. v. Sullivan* held that "the Constitution delimits a State's power to award damages for libel in actions brought by public officials against critics of their official conduct."[107] The Court described the Sedition Act as unconstitutional on free speech grounds.[108] The Court found that like seditious libel, any act of libel by public officials was merely another way of punishing speech critical of the government,

---

103 *Id.*

104 *Id.* at 630.

105 *Id.*

106 Brown v. Bd. of Educ., 347 U.S. 483, 495 (1954), *aff'd in part, rev'd in part*, 349 U.S. 294 (1955).

107 376 U.S. 254, 283 (1964).

108 *Id.* at 276 ("Although the Sedition Act was never tested in this Court, the attack upon its validity has carried the day in the court of history. Fines levied in its prosecution were repaid by Act of Congress on the ground that it was unconstitutional." (footnote omitted) (citing Act of July 4, 1840, ch. 45, 6 Stat. 802, accompanied by H.R. Rep. No. 86, 26th Cong., 1st Sess. (1840))).

which was the heart of the First Amendment's protection against the government's censorious reach.[109]

In *Sullivan*, the Court also moved to repudiate the decisions of *Schenck*, *Frohwerk*, *Debs*, and *Abrams*. The Court quoted the concurrence by Justice Brandeis in *Whitney v. California* for a declaration of the meaning of the First Amendment:

> Those who won our independence believed . . . that public discussion is a political duty; and that this should be a fundamental principle of the American government. They recognized the risks to which all human institutions are subject. But they knew that order cannot be secured merely through fear of punishment for its infraction; that it is hazardous to discourage thought, hope and imagination; that fear breeds repression; that repression breeds hate; that hate menaces stable government; that the path of safety lies in the opportunity to discuss freely supposed grievances and proposed remedies; and that the fitting remedy for evil counsels is good ones. Believing in the power of reason as applied through public discussion, they eschewed silence coerced by law—the argument of force in its worst form. Recognizing the occasional tyrannies of governing majorities, they amended the Constitution so that free speech and assembly should be guaranteed.[110]

Five years later, the Court completed its reversal of the line of cases that ran from *Schenck* to *Whitney*.[111] Public discussion in the marketplace of ideas became the fundamental understanding of free expression in the manner first advocated by John Milton two centuries earlier.

IV. COMPETING MARKET MODELS OF REGULATION

Justice Holmes' dissent in *Abrams* did not have any immediate impact on the First Amendment. Instead, Congress passed the Radio Act and the Communications Act, which included very expansive laws regulating content[112] and used the power of

---

109 *See id.* at 271–72 (noting that the constitutionalization of libel was later expanded to public figures); Curtis Publ'g Co. v. Butts, 388 U.S. 130, 164 (1967) (Warren, J., concurring).

110 *N.Y. Times*, 376 U.S. at 270 (quoting Whitney v. California, 274 U.S. 357, 375–76 (1927) (Brandeis, J., concurring)).

111 Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) ("[L]ater decisions have fashioned the principle that the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.").

112 *See* Radio Act of 1927, ch. 169, 44 Stat. 1162, *repealed by*, Communications Act of 1934, ch. 652, 48 Stat. 1064.

congressional hearings to enforce content codes in the motion picture industry.[113]

Despite the lack of immediate impact, Holmes' suggestion that speech reflected a marketplace gained traction in the regulation of the radio and television markets.

Throughout history, there has been a need to regulate markets. From biblical times, there has been an admonition to keep accurate merchant scales.[114] In the commercialization of the European economy in the Middle Ages, "local and royal anti-fraud regulation proliferated to protect consumers from shoddy products, cheating on quantity, and overinflated prices."[115] Standardizing weights and measures became a royal prerogative.[116] In the United States, the right to standardize weights and measures was incorporated into the constitutional power of Congress.[117]

Such efforts continued in the United States. As the twentieth century dawned, state and federal governments added laws to protect the public from financial and securities fraud,[118] monopoly power, unfair competition, and deceptive competition.[119] As radio became a popular entertainment and news platform, congressional efforts to regulate the medium and the marketplace it

---

113 *See* Mut. Film Corp. v. Indus. Comm'n of Ohio, 236 U.S. 230, 241–46 (1915) (finding that the First Amendment does not extend to motion pictures); *Will H. Hays*, BRITANNICA (Mar. 3, 2026), https://www.britannica.com/biography/Will-H-Hays [https://perma.cc/TCF2-YQBT] (explaining that in response to calls for greater state censorship laws, in 1922, the Motion Picture Producers and Distributors of America hired William H. Hays to enforce self-censorship rules which became the Motion Picture Production Code or Hays Code).

Hays had also been chairperson of the Republican National Committee and Postmaster General. *Id.*

114 *Leviticus* 19, 35–36 ("You shall not commit a perversion of justice with measures, weights, or liquid measures. You shall have true scales, true weights, a true ephah, and a true hin. I am the Lord, your God, Who brought you out of the land of Egypt."); *Deuteronomy* 25:15 ("You shall have a correct and honest weight; you shall have a correct and honest measure, so that your days may be prolonged in the land which the LORD your God is giving you.").

115 Emily Kadens, *The Persistent Limits of Fraud Prevention in Historical Perspective*, 118 NW. U. L. REV. 167, 173 (2023).

116 *See id.*

117 U.S. CONST. art. I, § 8, cl. 5.

118 *See Blue Sky Laws*, ENCYCLOPEDIA.COM, https://www.encyclopedia.com/history/dictionaries-thesauruses-pictures-and-press-releases/blue-sky-laws [https://perma.cc/Q7FA-F6ZY] (last visited Feb. 19, 2026) ("BLUE SKY LAWS are state laws designed to prevent fraud in the sale of corporate securities. These laws preceded federal regulation of securities, which began in 1933. Kansas enacted the first statute in 1911, and by the end of 1923, forty-five of the forty-eight states had followed suit.").

119 Sherman Antitrust Act of 1890, ch. 647, 26 Stat. 209; Federal Trade Commission Act of 1914, ch. 311, 38 Stat. 717.

spawned generated a series of laws beginning in 1912 and culminating in the Communications Act of 1934.[120] Authority was granted to the FCC to administer broadcast licenses.[121] Under the Communications Act of 1934 and continuing under the modern Telecommunications Act of 1996, the first-come, first-served property rights distribution of radio frequencies was replaced with a licensing renewal system that based the availability of a license on the use of that license in the public interest.[122] "In granting or withholding permits for the construction of stations, and in granting, denying, modifying or revoking licenses for the operation of stations, 'public convenience, interest, or necessity' was the touchstone for the exercise of the Commission's authority."[123]

Notably, in *FCC v. Pottsville Broadcasting Co.*, the Supreme Court upheld the regulatory authority of Congress over broadcasting.[124] In its opinion, the Supreme Court never suggests that the public interest, convenience, or necessity standard required any limitation to accommodate the First Amendment's prohibition on laws abridging the freedom of speech or press. The marketplace for access to the airwaves was under the total control of the government.[125]

The Supreme Court found that because the number of channels for broadcasting is severely limited, "the commission must determine from among the applicants before it which of them will, if licensed, best serve the public."[126] In framing the licensing controls as resource allocation, the Supreme Court was able to support the public interest, convenience, or necessity test even as it moved away from censorship for other media.

Given the focus on broadcast scarcity, the government did not rely on the public interest standard to manage the internet. Instead, the legislature focused on protecting minors from inde-

120 Radio Act of 1912, ch. 287, 37 Stat. 302, *repealed by*, Radio Act of 1927, ch. 169, 44 Stat. 1162, *repealed by*, Communications Act of 1934, ch. 652, 48 Stat. 1064.

121 *Id.* § 1.

122 Communications Act of 1934, ch. 652, 48 Stat. 1064, *amended by*, Telecommunications Act of 1996, Pub. L. No. 104–104, § 204, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

123 FCC v. Pottsville Broad. Co., 309 U.S. 134, 137–38 (1940).

124 *Id.* at 137 ("By this Act Congress, in order to protect the national interest involved in the new and far-reaching science of broadcasting, formulated a unified and comprehensive regulatory system for the industry.").

125 *See id.* at 138.

126 *Id.* at 138 n.2.

cent content.[127] The Supreme Court rejected the congressional efforts to manage the emerging internet.[128]

If the only reason for allowing broadcast regulations is scarcity, then the digital retransmission of broadcast signals suggests that the era of the FCC has come to an end.[129] There is, however, another possibility.

> [T]he people as a whole retain their interest in free speech by radio and their collective right to have the medium function consistently with the ends and purposes of the First Amendment. It is the right of the viewers and listeners, not the right of the broadcasters, which is paramount.[130]

The regulation of the airwaves was likely consistent with the views of Adam Smith as well.[131] Smith described a marketplace that was "protected by law"[132] and designed to avoid hurting the interest of one group among the "order of citizens" over that of another.[133] Both the unregulated newspapers and internet sites could compete amongst each other, as could the highly regulated broadcasters. And each requires civil government to sustain order.[134]

Perhaps ironically, the Supreme Court has become increasingly focused on the historical interpretation of the Constitution precisely at the time when precedent is least relevant to the technological transformation of communication. In addition to Smith's acceptance of regulation as part of market operations, history suggests Milton would have strongly opposed FCC regulation of the airwaves. Locke's view of property would need to assess the meaningfulness and engagement of every prompt in or-

---

127 *See* Reno v. Am. C.L. Union, 521 U.S. 844, 849 (1997); Moody v. NetChoice, LLC, 603 U.S. 707, 714 (2024) (addressing state regulations regarding child access).

128 *Reno*, 521 U.S. at 849 ("Notwithstanding the legitimacy and importance of the congressional goal of protecting children from harmful materials, . . . the statute abridges 'the freedom of speech' protected by the First Amendment.").

129 *Cf.* Red Lion Broad. Co. v. FCC, 395 U.S. 367, 385–86 (1969) (upholding the public interest standard pursuant to the scarcity of broadcast licenses).

130 *Id.* at 390.

131 *See* SMITH, *supra* note 89, at 328–29; Fabrizio Simon, *Adam Smith and the Law*, *in* THE OXFORD HANDBOOK OF ADAM SMITH 393, 397 (Christopher J. Berry, Maria Pia Paganelli & Craig Smith eds., 2013).

132 SMITH, *supra* note 89, at 329.

133 *Id.* at 618.

134 *Id.* at 674. Smith makes it clear, however, that order is not equality. *Id.* ("Civil government, so far as it is instituted for the security of property, is in reality instituted for the defence of the rich against the poor, or of those who have some property against those who have none at all.").

der to characterize whether the person prompting a generative AI system had meaningfully contributed to its output.[135]

History lessons can be quite fickle. Yet the current Supreme Court cases suggest that this is now the primary method for understanding new technologies.[136] Since *Dobbs* and *Bruen*, the Supreme Court has embraced history and tradition as the dominant approach to constitutional interpretation and used that framework to free itself from the confines of jurisprudence from the Civil Rights era and beyond.

These concerns come together in the recent decision of *Free Speech Coalition, Inc. v. Paxton*.[137] There, the Supreme Court explained that "[h]istory, tradition, and precedent recognize that States have two distinct powers to address obscenity: They may proscribe outright speech that is obscene to the public at large, and they may prevent children from accessing speech that is obscene to children."[138] This history, the Court notes, includes criminalization of obscenity beginning at least with the eighteenth century.[139] The Court recognizes that minors are more susceptible to the harm of obscenity under both modern precedent[140] and historical precedent.[141] Ignoring its own precedent in *Brown v. Entertainment Merchants Association*,[142] the Court used

---

135 This is similar to the Copyright Office search for authorship in prompt-based AI output as well. *See* U.S. COPYRIGHT OFF., LIBR. OF CONGR., COPYRIGHT AND ARTIFICIAL INTELLIGENCE: PART 2: COPYRIGHTABILITY *passim* (2025); Letter from Robert J. Kasunic, Assoc. Reg. of Copyrights & Dir. of the Off. of Reg. Pol'y & Prac., U.S. Copyright Off., to Van Lindberg (Feb. 21, 2023) (on file with the U.S. Copyright Off.).

136 *See, e.g.*, Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 231 (2022) (relying on history and tradition to reverse the constitutional protection for abortion); N.Y. State Rifle & Pistol Ass'n v. Bruen, 597 U.S. 1, 26 (2022) ("The test that we set forth . . . requires courts to assess whether modern firearms regulations are consistent with the Second Amendment's text and historical understanding."); Kennedy v. Bremerton Sch. Dist., 597 U.S. 507, 534–36 (2022) (repudiating the *Lemon* test application of the Establishment Clause as "'ambitiou[s],' abstract, and ahistorical" (alteration in original)); United States v. Rahimi, 602 U.S. 680, 693, 698–700 (2024) (discussing gun regulations); Loper Bright Enters. v. Raimondo, 603 U.S. 369, 413–14, 416 (2024) (Thomas, J., concurring) (overruling *Chevron* deference to administrative agencies when interpreting administrative regulations, because "*Chevron* deference compromises this separation of powers" by curbing "the judicial power afforded to courts, and simultaneously expand[ing] agencies' executive power beyond constitutional limits").

137 606 U.S. 461, 471–72, 478, 481–82 (2025).

138 *Id.* at 472.

139 *Id.*

140 *See* Ginsberg v. New York, 390 U.S. 629, 641–43 (1968).

141 *See* United States v. Bennett, 24 F. Cas. 1093, 1105 (C.C.S.D.N.Y. 1879) (No. 14,571).

142 *See* 564 U.S. 786, 794–95, 805 (2011) (rejecting efforts to regulate content deemed obscene only to minors).

this historical precedent to establish the rule that "two basic principles govern legislation aimed at shielding children from sexually explicit content. A State may not prohibit adults from accessing content that is obscene only to minors. But, it may enact laws to prevent minors from accessing such content."[143]

Paxton sidesteps many of the decisions of the past two decades, instead focusing on the earlier tradition of regulating content available to minors.[144] It waves aside its own precedent on content regulation—despite the law's express definition of content-based services—by emphasizing that the law only requires age verification rather than operating as a ban on the content itself.[145]

In her concurrence in *Moody v. NetChoice, LLC*,[146] Justice Jackson returned to *Red Lion* for the proposition that "differences in the characteristics of new media justify differences in the First Amendment standards applied to them."[147] Her concurrence did not suggest a retrenchment from First Amendment protection, but it did offer a reminder that each marketplace has unique characteristics that should be taken into account. *Paxton* instead shifted from a strict scrutiny standard for internet regulations to that of an intermediate scrutiny standard, a position the Supreme Court had previously rejected in *Brown*.[148]

The understanding of the founding traditions that gave rise to the First Amendment is not violated by this approach. Minors had very little constitutional recognition until the Supreme Court recognized their speech interests in *Tinker v. Des Moines*.[149] Although the opinion in *Tinker* suggests there was precedent, the decisions on which it relies focus on parental rights, not the rights of the student.[150] As the Supreme Court noted in 1923, "it is the natural duty of the parent to give his children education suitable to their station in life; and nearly all the states, includ-

---

143 *Free Speech Coal.*, 606 U.S. 461, 474 (2025) (first citing Butler v. Michigan, 352 U.S. 380, 383 (1957); and then citing *Ginsberg*, 390 U.S. 629, 637–68 (1968)).

144 *Id.*

145 *Id.* at 495.

146 603 U.S. 707, 748–50 (2024) (Jackson, J., concurring).

147 *Id.* at 749 (quoting Red Lion Broad. Co. v. FCC, 395 U.S. 367, 386 (1969)).

148 *See Brown*, 564 U.S. at 799 ("Because the Act imposes a restriction on the content of protected speech, it is invalid unless California can demonstrate that it passes strict scrutiny . . . ."); *cf.* United States v. Stevens, 533 F.3d 218, 232–33 (3d Cir. 2008) (holding that a content-based restriction on speech must survive strict scrutiny), *aff'd*, 559 U.S. 460 (2010).

149 *See generally* Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969) (analyzing precedent on constitutional rights of students).

150 *See, e.g.*, Meyer v. Nebraska, 262 U.S. 390, 400 (1923).

ing Nebraska, enforce this obligation by compulsory laws."[151] The rights of the students to learn were an invention of the 1960s.

What the new judicial interpretation means for the development of artificial intelligence and the related information marketplaces remains to be seen. When the speech cases of *Paxton* and *Moody* are viewed alongside the Second Amendment decisions of *Bruen* and *Rahimi*, and viewed with the privacy implications of *Dobbs*, a potentially dramatic shift could be contemplated.

This is particularly true if the Supreme Court embraces the idea that the medium is the message and that each medium may require its own regulatory approach because the invisible hand of self-interest operates quite differently across spheres.[152]

Paxton was about limiting minors' access to pornography and obscenity. The next challenges will focus on harms caused by sycophantic AI agents that encourage—or at least fail to discourage—suicide.[153] Nearly two dozen states have enacted laws focused on protecting members of the public from deepfakes that target individuals by creating nonconsensual pornographic images using their likenesses.[154] The jurisprudence of *Sullivan* and *Brown* would make it difficult for policy-based balancing to survive strict scrutiny. *Dobbs*, *Paxton*, *Moody*, and *Bruen* suggest that history and tradition have room to defer to public will on balancing fundamental rights. The invisible hand of Adam Smith is precisely the consequence of enabling members of the public to act in their individual self-interest to aggregate to a greater good. Locke's social contract amongst the governed presumes that the governed have primacy instead of nine appointed members of a modern Star Chamber who sit above the States and Congress as more equal than others.

---

151 *Id.*

152 History also teaches, however, that the arguments of *Milton* and even the initial holding in *Sullivan* were focused on political speech and efforts by government officials to punish disfavored speech. That tradition is deeply rooted in the entirety of the First Amendment. Decisions such as *Brandenburg* are not implicated by marketplace regulations in *Moody* or *Paxton*.

153 *See, e.g.*, Garcia v. Character Techs., Inc., 785 F. Supp. 3d 1157, 1180 (M.D. Fla.) (alleging Character AI produced sexual conversations and promoted suicidal ideation, resulting in a minor's death), *motion to certify appeal denied*, No. 6:24-CV-1903-ACC-DCI, 2025 WL 2581834 (M.D. Fla. July 15, 2025).

154 Vittoria Elliott, *The US Needs Deepfake Porn Laws. These States Are Leading the Way*, WIRED (Sep. 5, 2024, at 06:00 PT), https://www.wired.com/story/deepfake-ai-porn-laws/ [https://perma.cc/56MM-9AKU].

To manage the unknowable future of the AI Information Age, it may be time to let the invisible hand take the lead, requiring the Supreme Court to strike down fewer laws. Instead, history and tradition suggest that the political process for speech should also be allowed to experiment with content-neutral approaches to developing new media, particularly if the publications can lead to harm for minors and intrusions on other fundamental rights.

Only time will tell if the Supreme Court extends these decisions to other forms of AI regulation. But the precedent is there to do so. The history that led to the Bill of Rights suggests this is the intent of the document. And the marketplace of ideas that informed *Sullivan* is vastly different than the media of today.

V. CONCLUSION

In *On Liberty*, philosopher John Stuart Mill recognized that truth does not always win out. "[T]he dictum that truth always triumphs over persecution, is one of those pleasant falsehoods which men repeat after one another till they pass into commonplaces, but which all experience refutes."[155]

The shift from mass media to the media of the masses, the influence of social media, and the launch of generative AI made possible through advances in computing and communications technology[156] may require new approaches to content-neutral regulation. The foundational history of commercial media and the political upheavals it triggered are lessons that should not be forgotten.

The marketplace of ideas—or the battlefield on which competing faiths fight for hearts and minds—may not always produce the best answers. Milton's faith in truth winning the day is perhaps less likely in an age of social media, user-generated content, declining investigative journalism, and growing synthetic content. Nonetheless, markets work. Markets enable the participants to act according to their nature and, through their actions, generate an outcome that is productive and efficient.

---

155 JOHN STUART MILL, ON LIBERTY 52 (Project Gutenberg 2011) (1859).

156 Advances in medicine, automation, transportation, and other fields will undoubtedly play an equally important role, but those are beyond the scope of this Article. *See generally* JON M. GARON, ARTIFICIAL INTELLIGENCE LAW AND REGULATION IN A NUTSHELL (2025) (discussing Artificial Intelligence law and regulations); GARON, *supra* note 44 (discussing the impact that these new technologies will have in the future).

Markets also need regulation. This does not suggest that the broadcast license market of a public interest and necessity standard should be applied to the internet and AI systems, but it does suggest that the political process producing AI and social media restrictions should be allowed its political process rather than being supplanted by a strict scrutiny standard of *Sullivan*, *Stephens*, and *Brown*. Instead, *Moody* and *Paxton* each provide a more nuanced understanding of the competing demands for both free speech and protection from unrestricted harms.

In crafting the Bill of Rights, those drafting the Constitution were aware that their concepts and phrases had been developed through conflict and commerce in Europe. Milton championed free speech, and Locke emphasized that government was a social contract designed to protect life, liberty, and property. This should always remain the goal for all three branches of government. The invisible hand of the market can then flourish in a marketplace protected by law.

The Compliance Stack: A Structural Comparison of the GDPR and the CCPA

Gregory S. McNeal

CONTENTS

The Compliance Stack: A Structural Comparison of the GDPR and the CCPA

Gregory S. McNeal∗

Comprehensive privacy statutes now set the baseline terms for multinational data privacy compliance. Two regimes dominate the attention of scholars and practitioners—the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)—yet the two are not the functional equivalents that corporate compliance discussions sometimes suggest. They differ in regulatory design, doctrinal architecture, and operative assumptions. This Article works through the primary sources to compare them across five dimensions: territorial scope, processing constraints, individual rights, cross-border transfer mechanisms, and enforcement. On transfers, the contrast is especially sharp. The GDPR carves out third-country data flows as a distinct legal question under chapter V, subjecting them to adequacy decisions, approved safeguards, or narrow derogations; the CCPA has no comparable regime and instead governs downstream disclosures through its sale-and-sharing rules and its taxonomy of service providers, contractors, and third parties. The Article's aim is descriptive, seeking to isolate where these regimes align in practice and where their legal triggers diverge.

∗ Gregory S. McNeal, JD/PhD, CIPM; Professor of Law and Public Policy, Pepperdine University Caruso School of Law. With sincere thanks to the organizers of this symposium issue. AI Disclosure: In writing this Article, the author used the following AI tools: Grammarly for proofreading and grammar; Wispr Flow for voice-to-text dictation in lieu of typing (due to a disability); Claude for outlining and organizational assistance; and Perplexity AI for identifying supplemental sources. All prose is original to the author and when AI was used it was for editing, not drafting.

I. INTRODUCTION

The regulatory story of the last decade in privacy law is, at bottom, a story about scope. For most of its history, the United States governed personal information through a patchwork of sector-specific statutes, each tailored to a particular category of risk. HIPAA covered health data. The Gramm-Leach-Bliley Act covered financial data. FERPA covered education records. COPPA covered children. If your data did not fall into one of those silos, you were largely on your own.[1] That model made sense when personal data was generated in discrete, identifiable contexts. It makes considerably less sense when a single smartphone generates and transmits health data, financial data, location data, and behavioral data to dozens of third parties before the user finishes breakfast.

The move toward omnibus privacy regulation reflects this reality. Rather than continuing to draw regulatory boundaries around specific industries, legislators in Europe and California chose to draw them around personal information itself, regardless of who holds it or what sector it came from.[2] The two regimes that emerged from this shift, the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), now function as the dominant reference points for privacy compliance worldwide. They are the frameworks that multinational companies build their data governance programs around. And they are the frameworks that other jurisdictions look to when drafting their own laws.[3]

Part of the reason for their influence is sheer jurisdictional reach. The GDPR applies to any entity that processes personal data in the context of offering goods or services to individuals in the Union, or that monitors their behavior within it, regardless of whether the entity has a physical presence in Europe.[4] The CCPA reaches any for-profit entity doing business in California that meets specified thresholds: (1) annual gross revenues ex-

---

1 *See* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 878–79 (2014) (describing the U.S. sectoral model as being a patchwork of federal and state laws).

2 *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 776–78, 816–17 (2019) (analyzing the EU's comprehensive regulatory model and its influence on global privacy norms).

3 *See generally* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 132–59 (2020) (documenting the GDPR's influence on third-country regulatory adoption).

4 *See* Commission Regulation 2016/679, art. 3, 2016 O.J. (L 119) 1, 32–33 (EU).

ceeding $25,000,000, (2) processing of "personal information of 100,000 or more consumers or households," or (3) deriving 50% or more of annual revenue from selling or sharing personal information.[5] Given the size of these two markets, the practical effect is extraterritorial. Companies headquartered in Tokyo or São Paulo or Austin find themselves subject to one or both regimes simply because they have customers in those jurisdictions. The GDPR and the CCPA regulate their own markets, and they set the terms for global data practice.

But shared ambition does not mean shared architecture. The two regimes start from different legal traditions, operate through different regulatory mechanisms, and reach different conclusions about fundamental questions: what makes data processing lawful, how individual rights attach, whether the geographic movement of data matters, and what role contracts play in extending regulatory standards through the supply chain. This Article works through those differences systematically, drawing on the primary sources of both regimes to identify where they converge and, more often, where they diverge.

The GDPR is grounded in a specific constitutional commitment. Article 8 of the Charter of Fundamental Rights of the European Union recognizes the protection of personal data as an independent fundamental right, distinct from the right to privacy under article 7.[6] That distinction matters. It means the GDPR is implementing a constitutional mandate, and its regulatory architecture reflects that origin. The result is an omnibus framework that applies to virtually all processing of personal data by public and private actors alike, with the dual objective of protecting individual autonomy and facilitating the free movement of data within the internal market.[7] The CCPA comes from a different place entirely. It is a consumer protection statute, enacted through the California legislature and later amended by ballot initiative, situated within a legal tradition that treats privacy primarily as a matter of market regulation and individual choice.[8] The rights it creates attach to the commercial relation-

5 *See* CAL. CIV. CODE § 1798.140(d)(1) (West 2026).

6 *See* Charter of Fundamental Rights of the European Union arts. 7–8, Oct. 26, 2012, 2012 O.J. (C 326) 397.

7 *See* Commission Regulation 2016/679, art. 1, 2016 O.J. (L 119) 1, 32 (EU); *see also* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 123 (2017) (situating the GDPR within the European tradition of treating data protection as a dignity-based right).

8 *See* CIV. §§ 1798.100–.199.100; *see also* Eric Goldman, An Introduction to the California Consumer Privacy Act (CCPA) 3–5 (July 1, 2020) (unpublished manuscript),

ship between a business and a consumer. They are contingent on the nature of the data transaction, and they are designed to give consumers visibility into and control over how businesses use their personal information. The CCPA does not ask whether a particular act of processing is justified. It asks whether the consumer knows about it and has the ability to say no.

That difference in legal origin shapes everything downstream. Because European lawmakers treat data protection as a fundamental right, the GDPR places the burden of justification on the data controller before processing begins. Article 6 provides that processing is lawful only if at least one of six enumerated bases applies: the data subject's consent, contractual necessity, a legal obligation, protection of vital interests, performance of a task in the public interest, or the legitimate interests of the controller.[9] Each basis carries its own conditions. Consent must be freely given, specific, informed, and unambiguous.[10] Legitimate interests, the most flexible basis and the one most commonly invoked for commercial processing, requires a three-part analysis: the controller must (1) identify a legitimate interest, (2) demonstrate that the processing is necessary to pursue it, and then (3) balance that interest against the fundamental rights and freedoms of the data subject.[11] The overall effect is a regime that requires affirmative justification for every category of data activity. California asks nothing comparable. Its framework assumes that commercial data processing is permitted and then layers on disclosure obligations, purpose limitations, and opt-out rights to constrain how that processing occurs. The starting points are different, and so are the compliance architectures that follow from them.

The CCPA takes the opposite approach. It treats commercial data processing as a permitted activity and then imposes conditions on it: disclose what you collect and why, give consumers the ability to opt out of sale and sharing, and honor purpose limitations on downstream use.[12] The model is rooted in consumer protection and unfair competition law, and it shows. The animating

---

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013 [https://perma.cc/CL63-DL7G] (framing the CCPA as consumer protection legislation).

9 *See* Commission Regulation 2016/679, art. 6(1), 2016 O.J. (L 119) 1, 36 (EU).

10 *See id.* art. 4(11), at 34.

11 *See id.* art. 6(1)(f), at 36; *see also* Article 29 Data Prot. Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, at 25–37, 844/14/EN WP 217 (Apr. 9, 2014) (elaborating on the three-part test).

12 *See* CIV. §§ 1798.100(a)–(b), 1798.120–.121.

concern is information asymmetry. Businesses know far more about the data they collect than consumers do, and the CCPA's primary intervention is to close that gap by mandating notice at or before the point of collection and giving consumers meaningful choices about how their information is used.[13] The statute is realistic about how the data economy functions and tries to make it more fair.[14]

These are genuinely different theories of regulation, and they produce different compliance obligations. The European model positions the State as a guardian of individual dignity, intervening before processing begins to ensure that every use of personal data has an affirmative legal justification.[15] The California model positions the State as a referee in a commercial marketplace, ensuring that consumers have enough information to make their own decisions about the tradeoffs involved in sharing personal data. One regime controls the supply side. The other empowers the demand side. Both are incomplete, and both have produced substantial bodies of regulatory detail that reward close reading.

That close reading is what this Article provides. It proceeds in distinct parts, each focused on a specific axis of comparison. Starting with Part II, it maps the regulatory architecture of both frameworks: the GDPR's consistency mechanism and the CCPA's delegation of rulemaking authority to the California Privacy Protection Agency. Part III turns to territorial scope and definitional boundaries, including the GDPR's expansive jurisdictional reach under article 3, the CCPA's threshold-based applicability, and the structural complications created by California's inclusion of the household as a unit of protection. From there, Part IV examines what each regime requires before data can be processed. This is where the lawful basis requirement and the CCPA's reasonable expectations test do their heaviest lifting. Part V compares individual rights and enforcement mechanisms, including the access, opt-out, and appeal rights, as well as the eighteen-category cybersecurity audit framework established in the

---

13 *See id.* § 1798.100(a); CAL. CODE REGS. tit. 11, § 7012 (2026).

14 *See generally* ALICE MARINI ET AL., DATAGUIDANCE & FUTURE OF PRIV. F., COMPARING PRIVACY LAWS: GDPR V. CCPA (2018), https://ec.europa.eu/futurium/en/system/files/ged/gdpr_ccpa_comparison-guide.pdf [https://perma.cc/J7U8-CZBG] (explaining the key provisions in the CCPA that focus on accountability and collection limitations, and how they differ from the GDPR).

15 *See* Schwartz & Peifer, *supra* note 7, at 123–26 (describing the European model as rooted in a conception of data protection as a precondition of individual "self-determination").

CCPA's new Automated Decisionmaking Technology (ADMT). Part VI addresses the most significant structural asymmetry between the two regimes: the GDPR's restrictive cross-border transfer framework versus the CCPA's silence on the geographic movement of data. Part VII closes with the contractual mechanisms both regimes use to extend regulatory standards through the supply chain.

II. REGULATORY ARCHITECTURE

The constitutional ambitions described above would mean very little without institutional machinery to enforce them. Both the GDPR and the CCPA have built that machinery, but they have built it very differently.

The GDPR operates through a distributed enforcement model that spans the entire European Economic Area (EEA).[16] Every Member State is required to establish at least one independent supervisory authority with the power to investigate, correct, and sanction violations.[17] The independence requirement is taken seriously. Article 52 mandates that each authority "shall act with complete independence in performing its tasks and exercising its powers," free from external instruction by government or any other body.[18] This is a design choice with real consequences. It means that data protection enforcement in Europe is structurally insulated from the kind of political pressure that can shape enforcement priorities in other regulatory contexts.[19]

Sitting above these national authorities is the European Data Protection Board (EDPB), a body with its own legal personality, composed of the heads of one supervisory authority from each Member State and the European Data Protection Supervisor.[20] The EDPB's primary function is harmonization. It issues guidelines, recommendations, and best practices on contested doctrinal questions, and it administers the consistency mechanism that prevents the twenty-seven Member States from drifting into incompatible interpretations of the same regulation.[21] That con-

16 *See* Commission Regulation 2016/679, arts. 51–76, 2016 O.J. (L 119) 1, 65–80 (EU); *see also* Agreement on the European Economic Area, art. 36, 1994 O.J. (L 1) 1, 13 (incorporating GDPR into EEA law).

17 *See* Commission Regulation 2016/679, arts. 51(1), 52(1), 2016 O.J. (L 119) 1, 65–66 (EU).

18 *See id.* art. 52(1)–(2), at 66.

19 *See* Schwartz, *supra* note 2, at 790–95 (analyzing the GDPR's independence requirements as a mechanism for preserving the credibility of the fundamental rights framework).

20 *See* Commission Regulation 2016/679, art. 68(1)–(3), 2016 O.J. (L 119) 1, 76 (EU).

21 *See id.* arts. 63–64, 70(1), at 73–74, 76–78.

sistency mechanism is the architecture's pressure valve. When a national authority proposes a decision with cross-border implications, the EDPB can intervene to ensure the outcome is consistent with how the regulation is being applied elsewhere in the Union.[22]

Day-to-day enforcement, though, happens at the national level. Each supervisory authority serves as the frontline regulator for data subjects and businesses within its jurisdiction. For cross-border processing, the GDPR uses what it calls a "one-stop-shop" model: a single lead supervisory authority, determined by the location of the controller's main establishment, serves as the primary point of contact for the business.[23] The idea is efficiency. A company headquartered in Dublin should not have to negotiate simultaneously with twenty-seven different regulators. But the lead authority does not have the final word. Under article 60, it must share its draft decision with all concerned supervisory authorities, and if any of them raises a "relevant and reasoned objection," the lead authority must either accommodate the objection or refer the matter to the EDPB for binding dispute resolution.[24] In practice, this process has been slow and contentious. The Irish Data Protection Commission's (IDPC) handling of complaints against major U.S. tech companies drew years of criticism from other European regulators, and the EDPB has had to use its article 65 dispute resolution power on multiple occasions to override draft decisions it considered too lenient.[25] The result has been persistent tension between the one-stop-shop model's promise of regulatory efficiency and the reality that a single under-resourced authority can become a chokepoint for enforcement across the entire Union.

The article 65 procedure is, in effect, the EDPB's override power. When a concerned supervisory authority raises a relevant and reasoned objection to the lead authority's draft decision and the lead authority declines to follow it, the dispute lands on the EDPB's desk.[26] The Board then adopts a binding decision by a two-thirds majority of its members.[27] The lead authority has no discretion to ignore the result. It must adopt its final decision on

---

22 *See id.* art. 64, at 73–74.

23 *See id.* arts. 4(16), 56(1), at 34, 67; *id.* recitals 127–28, at 23–24.

24 *Id.* arts. 60(3)–(4), 65(1), at 71, 74–75.

25 *See* JOHNNY RYAN, IRISH COUNCIL FOR C.L., ECONOMIC & REPUTATIONAL RISK OF THE DPC'S FAILURE TO UPHOLD EU DATA RIGHTS 1, 4–6, 8–10 (Mar. 2021) (documenting delays in Irish enforcement of cross-border GDPR complaints).

26 *See* Commission Regulation 2016/679, art. 65(1)(a), 2016 O.J. (L 119) 1, 74 (EU).

27 *See id.* art. 65(2), at 75.

the basis of the Board's binding decision "without undue delay and at the latest by one month" of notification.[28] This is a remarkable delegation of authority. A supranational body composed of national regulators can, by majority vote, dictate the enforcement outcome in a case that a national authority investigated, drafted, and attempted to resolve on its own terms. The procedure has been used in several high-profile disputes, most notably in the EDPB's binding decisions directing the IDPC to impose substantially higher fines and broader corrective measures on Meta than the Commission had initially proposed.[29] The costs of this architecture are real. The multi-stage process of draft circulation, objection, Board deliberation, and final adoption routinely extends enforcement timelines by months, and in some cases by years. The IDPC's processing of the original *Schrems II* complaint is a well-known example, but it is hardly unique.[30] Speed is the tradeoff the GDPR makes for consistency. Whether that tradeoff is worth it depends on your perspective, but the structural choice is deliberate. The drafters of the GDPR were more concerned about regulatory fragmentation than regulatory delay, and the architecture reflects that priority. There is also a strategic dimension. The consistency mechanism functions as a check on forum shopping. A company that establishes itself in a Member State perceived as more permissive does not get to keep the benefit of that choice if other regulators object and the EDPB steps in.[31] The article 65 procedure is designed precisely to prevent that outcome: regulatory competition among Member States is limited by the Board's power to impose a uniform floor.

California took a different institutional path, and it took it in two steps.

When the CCPA went into effect in January 2020, enforcement belonged exclusively to the California Attorney General.[32] That was a traditional prosecutorial model: the Attorney General

---

28 *Id.* art. 65(6), at 75.

29 *See* Eur. Data Prot. Bd., Binding Decision 1/2023 on the Dispute Submitted by the Irish SA on Data Transfers by Meta Platforms Ireland Limited for Its Facebook Service (Art. 65 GDPR), ¶¶ 273–74 (Apr. 13, 2023), https://www.edpb.europa.eu/system/files/2023-05/edpb_bindingdecision_202301_ie_sa_facebooktransfers_en.pdf [https://perma.cc/F65G-ZWUE] (ordering the IDPC to impose higher fines due to aggravating factors).

30 *See* Eur. Parliament's Pol'y Dep't for Citizens' Rts. and Const. Affs., *Exchanges of Personal Data After the* Schrems II *Judgment*, § 2.3.1.2, at 31–33, PE 694.678 (2021) (discussing bottlenecks).

31 *See* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 67–68 (Paul Craig & Gráinne de Búrca eds., 2015) (analyzing the one-stop-shop mechanism's vulnerability to strategic corporate location decisions).

32 *See* CAL. CIV. CODE § 1798.155(a) (West 2025).

(AG) could bring civil actions for statutory damages, but there was no dedicated privacy regulator, no rulemaking apparatus beyond the AG's authority to adopt implementing regulations, and no administrative adjudication process.[33] The California Privacy Rights Act (CPRA) changed that. Approved by California voters in November 2020, Proposition 24 created the California Privacy Protection Agency (CPPA), which is described as "the first dedicated privacy enforcement agency in the United States."[34] The statute vests the CPPA with "full administrative power, authority, and jurisdiction to implement and enforce" the CCPA.[35] That is broad language, and the Agency has interpreted it broadly.

What makes the CPPA structurally distinctive is its enforcement mandate and its rulemaking power. The Agency operates under the California Administrative Procedure Act and has used notice-and-comment rulemaking cycles to build out the operational substance of the CCPA in ways the statutory text left open.[36] The ADMT regulations, the cybersecurity audit requirements, the risk assessment framework, and the insurance provisions all emerged from the Agency's regulatory process, not from the legislature.[37] This is a meaningful distinction from the European model. European Data Protection Authorities (DPAs) have investigative, corrective, and advisory powers under GDPR article 58, and they issue guidance that carries significant practical weight. But they do not engage in the kind of quasi-legislative gap-filling that the CPPA performs through formal rulemaking.[38] The CPPA does not just interpret the statute. It finishes writing it.

The Agency is governed by a five-member board, and the appointment structure deliberately fragments political control.[39] The Governor appoints the chair.[40] The AG, the Senate Rules

---

33 *See* CAL. CODE REGS. tit. 11, §§ 999.300–.341 (2026) (effective Aug. 14, 2020).

34 *See* CIV. § 1798.199.10; *see also* CAL. SEC'Y OF STATE, TEXT OF PROPOSED LAWS: CALIFORNIA GENERAL ELECTION §§ 2, 24, at 42–43, 71 (2020), https://vig.cdn.sos.ca.gov/2020/general/pdf/topl.pdf [https://perma.cc/J68E-Q3R6] (describing the CPPA as a first-of-its-kind agency); *CCPA vs CPRA: What Changed in California Privacy Law*, PRYVII, https://pryvii.com/en/compare/ccpa-vs-cpra [https://perma.cc/AU6W-3JV5] (last visited Apr. 17, 2026).

35 CIV. § 1798.199.10(a).

36 *See id.* § 1798.185 (enumerating specific rulemaking directives).

37 *See* tit. 11, §§ 7100–7222.

38 *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1767–75 (2021) (analyzing the CPPA's rulemaking authority as a structurally distinct approach to privacy governance compared to European DPA advisory models).

39 *See* CIV. § 1798.199.10(a).

40 *Id.*

Committee, and the Speaker of the Assembly each appoint one additional member.[41] The fifth member is appointed by the Governor and all members must be Californians with expertise in data privacy.[42] The design is meant to insulate the Agency from any single branch or officeholder, an aspiration that echoes GDPR article 52's requirement that European supervisory authorities act with "complete independence."[43] But the analogy only goes so far. European DPA independence is anchored in EU primary law and the Charter of Fundamental Rights; the CPPA's independence is a creature of state statute, and while Proposition 24 included provisions making amendment difficult, the institutional safeguard is not constitutionally entrenched in the way its European counterparts are.[44] One other structural point worth noting: the AG did not lose enforcement authority when the CPPA was created. The two share concurrent jurisdiction, which means that California's privacy regime now has two independent enforcement actors.[45] The Agency can investigate, hold administrative hearings, impose fines up to $7,500 per intentional violation, and issue cease-and-desist orders.[46] And the AG can still bring civil enforcement actions on a parallel track. That is a considerable amount of enforcement firepower concentrated in a single state.

So far, the comparison has focused on institutional structure: who regulates, how they're appointed, and what powers they hold. But there is another structural difference that shapes how these regimes actually function in practice, and it has to do with who gets to complain and what happens when they do.

Under the GDPR, any data subject has the right to lodge a complaint with a supervisory authority.[47] That complaint triggers a legal obligation: the authority must inform the complainant of the progress and outcome of the complaint, including the possibility of a judicial remedy.[48] If the authority fails to act, the data subject can sue the regulator itself.[49] And the data subject also has an independent right to bring a judicial action directly

---

41 *Id.*

42 *See id.*

43 Commission Regulation 2016/679, art. 52(1), 2016 O.J. (L 119) 1, 66 (EU).

44 *See* Schwartz, *supra* note 2, at 811–16 (discussing the treaty-level foundations of European DPA independence).

45 CIV. § 1798.199.10.

46 *Id.* §§ 1798.199.55, 1798.155.

47 Commission Regulation 2016/679, art. 77(1), 2016 O.J. (L 119) 1, 80 (EU).

48 *Id.* art. 77(2), at 80.

49 *Id.* art. 78(2), at 80 (providing a right to an effective judicial remedy where a supervisory authority "does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint").

against the controller or processor.[50] The practical consequence is that individuals function as a distributed enforcement mechanism. They can force regulatory action through complaints, challenge regulatory inaction through the courts, and pursue their own claims in parallel. The Court of Justice of the European Union (CJEU) has reinforced this architecture repeatedly, treating the right to lodge a complaint and the right to judicial review as essential components of the fundamental right to data protection.[51]

California made a different choice. The CCPA's private right of action is narrow by design. Section 1798.150 permits consumers to bring suit only for unauthorized access, theft, disclosure, or exfiltration of nonencrypted or nonredacted personal information resulting from a business's failure to implement and maintain reasonable security procedures and practices.[52] That covers data breaches, but it does not cover anything else. If a business ignores an access request, denies a deletion request without justification, or deploys dark patterns to prevent consumers from opting out, the consumer's only recourse is to file a complaint with the CPPA or the AG and hope that one of them acts on it.[53] For the full range of substantive CCPA rights, enforcement depends entirely on the discretion of state actors.

The California Legislature has had multiple opportunities to expand the private right of action and has declined each time.[54] Business groups have consistently opposed expansion, arguing that broad private litigation rights would generate abusive class action practice.[55] Whatever one thinks of that argument, the result is a regime where the individual consumer has meaningful leverage only in the breach context. For everything else, the consumer is a complainant, not a litigant. That is a fundamentally different relationship between the individual and the enforcement apparatus than what the GDPR provides, and it has downstream consequences for how effectively each regime's substantive rights translate into actual compliance pressure.

---

50 *Id.* art. 79, at 80.

51 *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 109, 174–76 (July 16, 2020) (emphasizing the obligation of supervisory authorities to act on complaints with "all due diligence"); *see also* LYNSKEY, *supra* note 31, at 177–85 (analyzing the enforcement role of individual complaint rights within the GDPR's institutional design).

52 CAL. CIV. CODE § 1798.150(a)(1) (West 2025).

53 *See id.* § 1798.199.40 (authorizing the CPPA to receive consumer complaints).

54 *See, e.g.*, Assemb. B. 1751, 2021–2022 Leg., Reg. Sess. (Cal. 2022) (proposing the expansion of private right of action to cover all CCPA violations, which failed in committee).

55 *See* Goldman, *supra* note 8, at 8 (discussing the political economy of the CCPA's limited private right of action).

III. TERRITORIAL SCOPE AND DEFINITIONS

Earlier, this Article addressed the normative foundations and institutional machinery of each regime. But none of that matters if the law doesn't reach you. Territorial scope determines who falls within the regulatory perimeter in the first place, and the GDPR and CCPA draw that perimeter in fundamentally different ways.

The GDPR's jurisdictional reach operates through two independent triggers, either of which is sufficient on its own.[56]

The first is the establishment criterion. Article 3(1) provides that the GDPR applies to the processing of personal data "in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place within the Union."[57] The concept of establishment is deliberately flexible. Recital 22 defines it as "the effective and real exercise of activity through stable arrangements," a formulation broad enough to capture a branch office, a subsidiary, or even a single employee operating with a sufficient degree of permanence.[58] But the real bite of article 3(1) comes from the phrase "in the context of the activities of."[59] Processing does not need to be performed by the EU establishment itself. It is enough that the processing is "inextricably linked" to the establishment's activities.[60] The *Google Spain* decision is the leading example. Google's Spanish office sold advertising. Google's servers in the United States processed the data. The CJEU held that the processing fell under EU jurisdiction because the advertising revenue made the Spanish establishment's activities and the U.S. processing "inextricably linked."[61] For any company with a commercial presence in the EU, even a small one, that logic has significant reach.

The second trigger is the targeting criterion under article 3(2), and it extends the GDPR's jurisdiction to controllers and processors with no EU establishment at all. It applies when pro-

---

56 Commission Regulation 2016/679, art. 3, 2016 O.J. (L 119) 1, 32–33 (EU).

57 *Id.* art. 3(1), at 32.

58 *Id.* recital 22, at 4; *see also* Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639, ¶ 31 (Oct. 1, 2015) (holding that even "minimal" real activity through stable arrangements can constitute establishment).

59 Commission Regulation 2016/679, art. 3(1), 2016 O.J. (L 119) 1, 32 (EU).

60 *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶¶ 55–56 (May 13, 2014) (finding that Google Inc.'s processing of personal data was carried out "in the context of" its Spanish subsidiary's advertising sales, even though the subsidiary performed no data processing itself).

61 *Id.* ¶ 56.

cessing relates to offering goods or services to data subjects in the Union, whether or not payment is required, or to monitoring the behavior of data subjects within the Union.[62] The threshold question is intent. A website accessible from Paris does not, by that fact alone, fall under the GDPR.[63] The GDPR requires evidence that the controller intended to direct its activities toward individuals in one or more Member States. Recital 23 lists doctrinal indicators: use of a language or currency associated with a Member State, references to EU-based customers, or use of a country-specific top-level domain.[64] The monitoring prong captures behavioral tracking. Recital 24 specifies that tracking individuals on the internet to build profiles, analyze preferences, or predict behavior constitutes monitoring, provided the behavior takes place within the Union.[65] A U.S.-based analytics company with no office in Europe, no EU customers, and no intent to serve the European market can still fall under the GDPR if it tracks the browsing behavior of individuals located in France or Germany.[66] There is an administrative consequence that follows from article 3(2) jurisdiction: any controller or processor subject to the GDPR solely through the targeting criterion must designate a representative in the Union.[67] The representative serves as a point of contact for supervisory authorities and data subjects and can be held liable for compliance failures.[68] In practice, this requirement has proven difficult to enforce against entities with no EU assets or presence, but the obligation exists and regulators have begun to press on it.[69]

The monitoring prong deserves separate attention because its practical reach is enormous and its boundaries are poorly de-

---

62 Commission Regulation 2016/679, art. 3(2)(a)–(b), 2016 O.J. (L 119) 1, 33 (EU).

63 *See* Eur. Data Prot. Bd., Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), at 17 (Nov. 12, 2019), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [https://perma.cc/2DE6-YKGR] (stating that "the mere accessibility of the controller's, processor's or an intermediary's website in the Union . . . is insufficient" (quoting Commission Regulation 2016/679, recital 23, 2016 O.J. (L 119) 1, 5 (EU))); *cf.* Joined Cases C-585/08 & C-144/09, Pammer v. Reederei Karl Schlüter GmbH & Hotel Alpenhof GesmbH v. Heller, ECLI:EU:C:2010:740 (Dec. 7, 2010) (establishing a similar targeting analysis under the Brussels I Regulation).

64 Commission Regulation 2016/679, recital 23, 2016 O.J. (L 119) 1, 5 (EU).

65 *Id.* recital 24, at 5.

66 *See* Christopher Kuner, *The Internet and the Global Reach of EU Law* 15–17 (Lond. Sch. of Econ. & Pol. Sci. L. Dep't, Working Paper No. 24/2017, 2017) (analyzing the extraterritorial implications of the monitoring criterion).

67 Commission Regulation 2016/679, art. 27, 2016 O.J. (L 119) 1, 48–49 (EU).

68 *Id.* art. 27(4)–(5), at 49.

69 *See* Eur. Data Prot. Bd., *supra* note 63, at 23–24, 28 (discussing the scope and limitations of the article 27 representative requirement).

fined. We have already seen the general framework: recital 24 captures tracking of individuals on the internet for the purpose of profiling, preference analysis, or behavioral prediction, provided the tracked behavior takes place within the Union.[70] What that means operationally is that a non-EU company deploying analytics pixels, behavioral advertising cookies, or fingerprinting scripts on a website visited by individuals in Germany or Italy may be processing personal data subject to the GDPR, even if the company has no office, no customers, and no commercial interest in Europe.[71] The trigger is the purpose of the tracking, not the location of the tracker. If the data collection is designed to analyze user behavior or build predictive profiles, and the users happen to be in the Union, article 3(2)(b) applies.[72] The jurisdictional logic is location-of-the-person, not location-of-the-business, and in a world where tracking scripts are deployed globally by default, the practical consequence is that the GDPR's reach extends well beyond any entity that consciously decided to serve the European market.[73] That breadth is by design. But it also creates enforcement gaps, because asserting jurisdiction over a company with no EU presence, no EU assets, and no EU representative is considerably easier on paper than in practice.

The CCPA draws its jurisdictional perimeter differently. The GDPR asks: are you processing data of people in the EU, and did you intend to reach them or monitor them? The CCPA asks: are you a for-profit business of sufficient commercial scale, doing business in California, and handling the personal information of California consumers?[74] Every element of that question matters. The statute applies only to for-profit legal entities that collect consumers' personal information, determine the purposes and means of processing, and do business in the State of California.[75] But meeting that definitional threshold alone is not enough. The entity must also satisfy at least one of three size-based criteria, as amended by the CPRA: (1) annual gross revenues exceeding $25,000,000; (2) buying, selling, or sharing the personal infor-

70 Commission Regulation 2016/679, recital 24, 2016 O.J. (L 119) 1, 5 (EU).

71 *See* Eur. Data Prot. Bd., *supra* note 63, at 20 (discussing the scope of the monitoring criterion in the context of internet tracking technologies).

72 *See* Lokke Moerel, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, 1 INT'L DATA PRIV. L. 28, 32–33 (2011) (analyzing the extraterritorial implications of behavioral targeting under EU data protection law).

73 *See* BRADFORD, *supra* note 3, at 132–33 (arguing that the GDPR's extraterritorial scope functions as a mechanism of unilateral regulatory globalization).

74 CAL. CIV. CODE § 1798.140(d)(1) (West 2026).

75 *Id.*

mation of 100,000 or more consumers or households annually; or (3) deriving 50% or more of annual revenue from selling or sharing consumers' personal information.[76] The phrase "doing business in California" is not independently defined by the CCPA; it imports the general concept from California tax and corporate law, which turns on whether the entity has sufficient economic nexus with the state.[77] The result is a jurisdictional model anchored in commercial identity and economic scale rather than in the act of processing itself. A small European startup that happens to collect data from a few California users is unlikely to meet any of the three thresholds. A major U.S. retailer with California customers almost certainly does. The CCPA's perimeter is narrower than the GDPR's, and deliberately so.

The three threshold triggers have already been described, so I won't restate them here except to note one detail worth emphasizing. The volume trigger counts consumers *or households*, which means that a smart home provider collecting data from a single connected device used by a four-person family may be counting one household rather than four individuals, but is still accumulating volume toward the 100,000 threshold.[78] The household concept does real jurisdictional work in the Internet of Things (IoT) context, and we will return to it below when discussing definitional scope.

The "doing business in California" requirement deserves a closer look because it is doing more structural work than it might appear. The CCPA does not define the phrase independently. Instead, it imports the concept from California's general corporate and tax law framework, where "'doing business' means actively engaging in any transaction for the purpose of financial or pecuniary gain or profit."[79] Some commentators have analogized this to the constitutional minimum contacts analysis under *International Shoe* and its progeny.[80] The analogy is tempting but im-

---

76 *Id.* § 1798.140(d)(1)(A)–(C); *see also* Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'NS TECH. L. 65, 72–74 (2019) (noting the CCPA's threshold-based applicability is a structural departure from the GDPR's universal coverage model).

77 *See* CAL. REV. & TAX. CODE § 23101 (West 2012) (defining "doing business" for franchise tax purposes).

78 *See* CIV. § 1798.140(d)(1)(B), (q).

79 REV. & TAX. § 23101(a); *see also* AMANDA SMITH, STATE OF CAL. FRANCHISE TAX BD., LEGAL RULING – 2022-01, at 3 (2022) (discussing economic nexus standards for out-of-state entities).

80 *See, e.g.*, Goldman, *supra* note 8, at 3–5 (2020) (noting the jurisdictional ambiguity of the "doing business" requirement).

precise. Minimum contacts is a constitutional floor imposed by the Due Process Clause on the exercise of personal jurisdiction; "doing business" under California law is a statutory coverage criterion that operates at a different level of analysis. The practical question for a non-California entity is whether its economic engagement with the California market is sufficient to bring it within the statute's scope, and administrative interpretations have leaned toward a broad reading that includes sustained digital commerce with California residents.[81] The result is a jurisdictional threshold that is more bounded than the GDPR's targeting criterion but still captures a wide range of entities operating in the digital economy.

Now, definitions. What counts as protected information under each regime? The GDPR's unit of protection is the natural person. Article 4(1) defines "personal data" as "any information relating to an identified or identifiable natural person."[82] The definition is intentionally broad. An identifiable person is anyone "who can be identified, directly or indirectly, . . . by reference to an identifier such as a name, an identification number, location data, [or] an online identifier."[83] That last category is where the definition shows its teeth. IP addresses, cookie strings, device fingerprints, advertising IDs: all of these qualify as personal data if they can be linked, even indirectly, to a specific individual.[84] The definition also maintains its grip on pseudonymized data. If the additional information needed to re-identify a data subject exists and is reasonably accessible, the data remains personal data subject to the full GDPR framework.[85] Only genuinely anonymous data, where the link to the individual has been irreversibly severed, falls outside the regulation.[86] The practical effect is that the GDPR casts an extraordinarily wide net. Almost any da-

---

81 *See California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST.: OFF. OF THE ATT'Y GEN. (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa [https://perma.cc/J3VV-ADYT] (interpreting "doing business" broadly to encompass entities with recurring commercial interactions with California consumers).

82 Commission Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1, 33 (EU).

83 *Id.*

84 *See* Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, ¶¶ 38–49 (Oct. 19, 2016) (holding that dynamic IP addresses constitute personal data where the controller has legal means to obtain additional information enabling identification).

85 Commission Regulation 2016/679, recital 26, 2016 O.J. (L 119) 1, 5 (EU); *see also* Article 29 Data Prot. Working Party, Opinion 05/2014 on Anonymisation Techniques, at 9–10, 0829/14/EN WP216 (Apr. 10, 2014) (setting a high threshold for true anonymization and treating most pseudonymization techniques as insufficient to remove data from the GDPR's scope).

86 Commission Regulation 2016/679, recital 26, 2016 O.J. (L 119) 1, 5 (EU).

ta point that touches an individual, however indirectly, is presumptively within scope.[87]

The CCPA's definition of personal information is comparably broad in scope but structurally different in one important respect. Section 1798.140(v) defines personal information as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[88] Those last two words are where the CCPA departs from the European model. The GDPR's definitional anchor is the natural person.[89] Full stop. The CCPA adds the household as a second, independent unit of protection.[90]

The CCPA defines what "household" means, and the definition is narrower than you might expect. Under section 1798.140, a household is a person or group of people who (1) reside at the same address and (2) share a common device or the same service provided by the business.[91] Both conditions must be met. A family of four sharing a Netflix account at the same address qualifies. Two roommates who each have their own separate accounts with a retailer probably do not, even though they share an address, because the business has not identified them as sharing a common account or identifier.

The household concept matters most in the IoT context, and a pair of examples helps illustrate why. Take a smart meter recording aggregate energy consumption for a residence. Under the GDPR, if the telemetry is aggregated at the household level and cannot be linked to a specific natural person's behavior, it may fall outside the definition of personal data entirely.[92] Under the CCPA, the same data is personal information by definition because it relates to a household.[93] The classification turns on the unit of protection, not the content of the data. Now consider a smart speaker capturing ambient audio in a shared living space.

---

87 *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1836–42 (2011) (analyzing the expansive reach of the EU's identification-based definition of personal data and its implications for regulatory scope).

88 CAL. CIV. CODE § 1798.140(v)(1) (West 2026).

89 Commission Regulation 2016/679, art. 1, 2016 O.J. (L 119) 1, 32 (EU).

90 *Id.*; *see* Schwartz, *supra* note 2, at 773, 816–17 (contrasting the EU's individual-centric data protection model with emerging U.S. approaches that recognize collective data interests).

91 CIV. § 1798.140(q).

92 *See* Article 29 Data Prot. Working Party, *supra* note 85, at 9 (noting that aggregation may, depending on context, prevent identification of individuals).

93 *See* CIV. § 1798.140(v)(1).

Under the GDPR, the controller faces an attribution problem: which natural person is the data subject for a given voice snippet? If attribution is impossible, the controller's obligations become murky.[94] The CCPA sidesteps that problem. The data relates to the household. Every voice snippet is personal information regardless of which family member was speaking.[95]

But the household concept creates its own set of problems, particularly around rights requests, which was recognized in a recent repeal of household specific provisions.[96] The CPPA's regulations initially required that when a consumer does not have a password-protected account with the business, the business may respond to a request to know or a request to delete household-level personal information only if all members of the household jointly submit the request and the business individually verifies each of them.[97] That requirement meant that one household member could not exercise rights over household data unless every other member of the household cooperated. If a spouse refused to participate in the verification process, the deletion request would fail. That is a procedural veto embedded in the rights architecture, and it has no analogue in the GDPR, where each data subject exercises rights independently as an individu-

---

94 *See* Eur. Data Prot. Bd., Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects, ¶ 45 (Oct. 8, 2019), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en [https://perma.cc/7KPP-9KPV] (discussing controller obligations where multiple data subjects are affected by the same processing operation).

95 *See* Lydia de la Torre, *What Is "Personal Information" Under the CCPA?*, CAL. LAWS. ASS'N (Sep. 2019), https://calawyers.org/privacy-law/what-is-personal-information-under-the-california-consumer-privacy-act/ [https://perma.cc/RAS8-NM32].

96 CAL. CODE REGS. tit. 11, § 7031(a) (repealed Mar. 29, 2023).

97 I*d.*; *see also* CYNTHIA COLE, MATTHEW BAKER & KATHERINE BURGESS, WOLTERS KLUWER, THE CCPA: FINAL REGULATIONS AND INSIGHT INTO KEY ADDITIONS EFFECTIVE IMMEDIATELY (Aug. 26, 2020), https://business.cch.com/srd/SP_The-CCPA-Final-Regulations_08-26-2020_final_locked.pdf [https://perma.cc/7N86-2E8V] (noting that "all members of a household must jointly submit requests and individually be verified"); Ken Dreifach et al., *Key Changes in the AG's Updated Proposed CCPA Regulations*, ZWILLGEN: BLOG (Mar. 20, 2020), https://www.zwillgen.com/ftc-state-ag/key-changes-california-ag-updated-proposed-ccpa-regulations/ [https://perma.cc/W2J4-F7RL] (observing that absent a password-protected household account, a business could only process a household request "if every member of the household submits a request, is independently verified by the business, and is able to show that they are currently members of that household").

The CPPA repealed the section as part of its first rulemaking package without replacing it. *See* No. 27-Z Cal. Regulatory Notice Reg. 770–75 (Jul. 8, 2022). The "household" concept survives in the statutory definition of personal information, California Civil Code § 1798.140(v)(1), but no procedural mechanism for household-level rights requests currently exists in the regulations.

al.[98] This tradeoff means the CCPA's household concept captures data that the GDPR's individual-centric model might miss, particularly in shared-device environments where attribution to a single person is difficult or impossible. But in its original form, the CCPA also introduced coordination costs that could prevent any single person from exercising rights over data they helped generate. Whether that tradeoff is worth it depends on how much weight you place on capturing shared-device data versus preserving the frictionless exercise of individual rights. That tension between definitional breadth and rights-exercise friction will resurface when we turn to the mechanics of individual rights in Part V.

IV. LAWFUL PROCESSING VS. PURPOSE LIMITATION

The most consequential difference between the GDPR and the CCPA is not who they regulate or how far they reach. It is the threshold question of what makes data processing permissible in the first place.

The GDPR and the CCPA give radically different answers.

The GDPR starts from prohibition. Article 6(1) provides that processing of personal data is lawful only if, and to the extent that, at least one of six enumerated legal bases applies.[99] No legal basis, no processing. The default state is that data processing is impermissible, and the controller bears the burden of establishing an affirmative justification before any processing begins.[100] This is a deliberate structural choice rooted in the GDPR's origins as a fundamental rights instrument. Articles 7 and 8 of the EU Charter of Fundamental Rights guarantee respect for private life and protection of personal data, and the CJEU has consistently treated the requirement of a lawful basis as the mechanism through which those guarantees are operationalized.[101] The six bases are consent, contractual necessity, legal obligation, vital interests, public interest, and legitimate interests.[102] In practice, most commercial processing relies on either consent or le-

98 *See* Commission Regulation 2016/679, arts. 15–22, 2016 O.J. (L 119) 1, 43–46 (EU) (establishing individual rights exercisable by each data subject independently).

99 *Id.* art. 6(1), at 36.

100 *See* Article 29 Data Prot. Working Party, *supra* note 11, at 9–10 (describing the requirement of a legal basis as one of the most fundamental aspects of EU data protection law).

101 *See* Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 171 (July 16, 2020) (grounding the GDPR's processing requirements in the Charter's fundamental rights guarantees).

102 Commission Regulation 2016/679, art. 6(1)(a)–(f), 2016 O.J. (L 119) 1, 36 (EU).

gitimate interests, and the latter is where the real doctrinal complexity lives.

The legitimate interests basis under article 6(1)(f) is the GDPR's pressure valve for commercial data use, and it is heavily contested.[103] The controller must satisfy a three-part analysis. First, it must identify a specific legitimate interest being pursued, which can be commercial in nature; direct marketing, fraud prevention, network security, and similar purposes all qualify.[104] Second, the processing must be "necessary" for the purpose of that interest.[105] The Article 29 Working Party interpreted this as requiring that there be no reasonable, less intrusive alternative available to achieve the same objective, though the standard is closer to a proportionality analysis than a strict least-intrusive-means test.[106] Third, the controller must balance its interest against the fundamental rights and freedoms of the data subject, and the data subject's interests must not override those of the controller.[107] This balancing exercise is not optional and it is not informal. The accountability principle under article 5(2) requires that the controller be able to demonstrate compliance, which in practice means documenting the legitimate interest assessment in writing.[108] For companies processing personal data at scale across multiple product lines, each with its own purpose and risk profile, the procedural burden is substantial.[109]

The CCPA takes a structurally different approach. There is no requirement that a business identify a lawful basis before collecting or processing personal information. Processing is permitted as a default commercial activity.[110] The constraints come after the fact, through disclosure obligations, purpose limitation, and proportionality requirements, rather than through an up-

---

103 Eur. Data Prot. Bd., Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR, ¶¶ 12–18 (Oct. 8, 2024), https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en [https://perma.cc/5DDF-2BNA].

104 *Id.* art. 6(1)(f), at 36; *see also id.* recital 47, at 9 (recognizing direct marketing as a potential legitimate interest).

105 *Id.* art. 6(1)(f), at 36.

106 *See* Article 29 Data Prot. Working Party, *supra* note 11, at 11, 29–30 (distinguishing the necessity requirement from absolute indispensability and framing it as a proportionality inquiry).

107 Commission Regulation 2016/679, art. 6(1)(f), 2016 O.J. (L 119) 1, 36 (EU).

108 *Id.* arts. 5, 24(1), at 35–36, 47; *see also* Eur. Data Prot. Bd., *supra* note 103, ¶¶ 12, 68 (public consultation version).

109 *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1247–51 (7th ed. 2020) (discussing the compliance costs associated with the GDPR's lawful basis requirements).

110 *See* CAL. CIV. CODE § 1798.100(a)–(c) (West 2023).

front gatekeeping function. Section 1798.100(c) provides that a business's collection, use, retention, and sharing of personal information must be "reasonably necessary and proportionate" to the purposes for which the information was collected or processed.[111] The CCPA regulations operationalize this through section 7002's reasonable expectations framework: the five-factor test for determining whether processing is consistent with consumer expectations, the compatibility analysis for secondary uses, and the proportionality analysis that requires the business to use the minimum information necessary.[112] The difference from the GDPR is structural, not just tonal. The GDPR asks: do you have permission to process this data? The CCPA asks: are you being transparent about what you're doing with it, and is what you're doing reasonable? Both questions constrain processing, but they constrain it at different points in the lifecycle and through different mechanisms.[113]

It is worth pausing on what section 7002 accomplishes structurally, because the CCPA's critics sometimes describe it as a regime without meaningful processing constraints. That characterization is wrong.

The reasonable expectations test under section 7002(b) does not operate like a lawful basis. A business does not need to select from an enumerated list of justifications before processing begins.[114] But the five-factor inquiry imposes a functional discipline that is more rigorous than a pure notice-and-choice model would suggest. The question is not simply whether the business disclosed what it planned to do. The question is whether a reasonable consumer, given the nature of the relationship, the type and source of the data, and the clarity of the disclosures, would have expected the processing to occur.[115] That is a contextual, fact-intensive standard, and it has teeth. An email address collected to fulfill a purchase order cannot be quietly redirected into a cross-context behavioral advertising program. The consumer's

111 *Id.* § 1798.100(c).

112 CAL. CODE REGS. tit. 11, § 7002(b)–(d) (2026).

113 *See* Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations*, 11 INT'L DATA PRIV. L. 125, 128–30 (2021) (contrasting ex ante authorization models with ex post accountability frameworks in data protection regulation).

114 *Cf.* Commission Regulation 2016/679, art. 6(1), 2016 O.J. (L 119) 1, 36 (EU) (requiring selection of one of six enumerated legal bases).

115 tit. 11, § 7002(b)(1)–(5).

expectations at the point of collection anchor what the business is permitted to do afterward.[116]

The compatibility analysis for secondary uses adds another layer. When a business wants to repurpose personal information for a new purpose, section 7002(c) requires it to evaluate the relationship between the original collection context and the proposed new use.[117] The regulation is explicit about where the line falls. A cloud storage provider that decides to feed user files into a facial recognition training pipeline is the kind of contextual leap that fails the compatibility standard.[118] And where neither the expectations test nor the compatibility analysis supports the new purpose, the business must obtain the consumer's consent before proceeding.[119] At that point, the CCPA starts to look structurally similar to the GDPR's treatment of secondary processing, which generally requires either a compatible purpose under article 6(4) or fresh consent.[120] The mechanisms are different. The GDPR routes the inquiry through a formal lawful basis framework; the CCPA routes it through expectations, compatibility, and consent as sequential filters. But the analytical destination is closer than the structural differences might suggest.

The proportionality standard in section 7002(d) reinforces this convergence. Even where the purpose is permissible, the business must demonstrate that its collection, use, and retention of personal information are reasonably necessary and proportionate to achieve that purpose, measured against the minimum information required, the potential negative impacts on consumers, and any additional safeguards.[121] The CCPA does not impose the GDPR's formal documentation requirements under the accountability principle.[122] But a business that cannot articulate why it needed the volume and type of data it collected, and why less intrusive alternatives would not have sufficed, will have difficulty defending itself in an enforcement proceeding before the

---

116 *See* CIV. § 1798.100(c) (requiring that collection, use, retention, and sharing be "reasonably necessary and proportionate" to disclosed purposes).

117 tit. 11, § 7002(c).

118 *Id.* (using the cloud-storage-to-facial-recognition scenario as an illustrative example of incompatible secondary use).

119 *Id.* § 7002(e).

120 *See* Commission Regulation 2016/679, art. 6(4), 2016 O.J. (L 119) 1, 37 (EU) (setting out factors for assessing compatibility of secondary purposes); Article 29 Data Prot. Working Party, Opinion 03/2013 on Purpose Limitation, at 21–26, 00569/13/EN WP 203 (Apr. 2, 2013) (analyzing the compatibility assessment under EU law).

121 tit. 11, § 7002(d).

122 *Cf.* Commission Regulation 2016/679, arts. 5(2), 24(1), 2016 O.J. (L 119) 1, 36, 47 (EU) (requiring controllers to demonstrate compliance through documented measures).

CCPA.[123] The absence of a formal documentation mandate does not mean the absence of compliance pressure. It just means the pressure comes from a different direction. The processing constraints described here define what businesses are permitted to do with personal data. The next question is what happens when individuals push back.

V. INDIVIDUAL RIGHTS AND ENFORCEMENT

The individual rights granted by both regimes look similar on the surface. Both provide access, deletion, and portability, and since the CPRA, the CCPA also recognizes a right to correction.[124] But the mechanics differ in ways that matter. The GDPR's right of access under article 15 entitles the data subject to a copy of their personal data along with detailed information about the purposes of processing, the categories of data concerned, the recipients, and the envisaged retention period, among other disclosures.[125] The CCPA's access right under section 1798.110 allows consumers to obtain both the categories and specific pieces of personal information a business has collected, though it does not require the same breadth of contextual detail about processing operations.[126] A CCPA response tells you what was collected. A GDPR response is supposed to tell you enough to evaluate whether the collection was lawful. On deletion, both frameworks impose conditions, but they structure them differently. The GDPR's right to erasure under article 17 is triggered only when one of several specified grounds is met, for instance, that the data is no longer necessary or that consent has been withdrawn, and is then subject to its own exceptions.[127] The CCPA's right to delete is triggered by a consumer request alone but is carved back by a broad set of statutory exceptions, including completing a transaction, detecting security incidents, and complying with legal obligations.[128] The GDPR places the initial burden on the data subject to establish a ground; the CCPA places it on the

123 *See* Chander, Kaminski & McGeveran, *supra* note 38, at 1780–85 (arguing that the CCPA's regulatory framework creates de facto accountability obligations through the mechanism of enforcement risk).

124 Commission Regulation 2016/679, arts. 15–17, 20, 2016 O.J. (L 119) 1, 43–44, 45 (EU); CAL. CIV. CODE §§ 1798.100, .105, .106, .130 (West 2023).

125 Commission Regulation 2016/679, art. 15(1)(a)–(h), 2016 O.J. (L 119) 1, 43 (EU); *see* Case C-434/16, Nowak v. Data Prot. Comm'r, ECLI:EU:C:2017:994, ¶ 57 (Dec. 20, 2017) (emphasizing that the access right serves the data subject's ability to verify lawfulness of processing).

126 CIV. § 1798.110(a)(1)–(3).

127 Commission Regulation 2016/679, art. 17(1)(a)–(f), (3)(a)–(e), 2016 O.J. (L 119) 1, 43–44 (EU).

128 CIV. § 1798.105(a), (d)(1)–(8).

business to establish an exception.[129] That allocation shapes how deletion disputes play out in practice.

The regulation of automated decision-making technology represents an area where the regulatory impetus was there as a concept, but in practice, the ambition diverged structurally. Under the GDPR, article 22(1) provides that a data subject has the right not to be subject to a decision based solely on automated processing that produces legal effects or similarly significant effects.[130] Whether this operates as a self-executing prohibition or a right the data subject must invoke remains contested, but the practical effect is a default restriction on fully automated consequential decisions.[131] Where an exception applies (contract necessity, authorization by EU or Member State law, or explicit consent), the controller must implement suitable safeguards, including at minimum the right to obtain human intervention, to express a point of view, and to contest the decision.[132] California's approach, finalized in the CPPA's 2025 ADMT regulations, takes a different path.[133] Rather than imposing a default restriction, the regulations require businesses that use automated decision-making technology to make a "significant decision," defined as a decision concerning financial services, housing, education, employment, or health care, to provide pre-use notice, offer consumers the right to opt out, respond to access requests concerning the logic and output of the technology, and make available a process to appeal automated decisions to a qualified human reviewer.[134] Both regimes want consequential automated decisions subject to human oversight and individual challenge. The divergence is in the mechanism. The GDPR starts from restriction and carves out exceptions. California starts from permission and layers on transparency, opt-out, and appeal rights.

The California framework does not reach as broadly as earlier drafts proposed. The CPPA's initial rulemaking would have captured technology that merely *facilitated* human decisions, but the final regulations narrowed the definition of ADMT to tech-

129 *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 978–82 (2017) (analyzing the structural significance of burden allocation in privacy rights frameworks).

130 Commission Regulation 2016/679, art. 22(1), 2016 O.J. (L 119) 1, 46 (EU).

131 *See* Article 29 Data Prot. Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, at 19–20, 17/EN WP251rev.01 (Feb. 6, 2018) (interpreting article 22(1) as a prohibition).

132 Commission Regulation 2016/679, art. 22(2)–(3), 2016 O.J. (L 119) 1, 46 (EU).

133 *See* CAL. CODE REGS. tit. 11, §§ 7220–7222 (2026).

134 *Id.* §§ 7001(ddd), 7200(a), 7220–7222.

nology that "replace[s] . . . or substantially replace[s] human decisionmaking."[135] This is a more constrained trigger than the facilitation standard, yet it still addresses the hybrid decision-making problem that makes article 22 difficult to apply in practice. The regulations define "human involvement" to require that the reviewer understands the technology's output, affirmatively evaluates it, and has genuine authority to override it.[136] A human who is present in the decision chain but merely ratifies an algorithmic recommendation without independent analysis does not satisfy this standard, meaning the underlying technology would still qualify as ADMT, and the business would remain subject to the regulations' notice, opt-out, access, and appeal requirements. In this way, California targets the same concern that animates article 22: the risk that nominal human oversight masks substantively automated decision-making, but does so through a definitional mechanism rather than a default prohibition. The practical result is that businesses cannot insulate themselves from the ADMT framework simply by inserting a human reviewer into the process; they must demonstrate that the reviewer exercised meaningful discretion.[137]

The 2025 regulations operationalize these protections through specific notice and rights requirements for ADMT used in significant decisions.[138] Before using ADMT to make a significant decision about a consumer, a business must provide a pre-use notice that explains, in plain language, the purpose for which it will use the technology and how the technology processes personal information to reach the decision.[139] The consumer then has the right to opt out of that processing—a right that applies to decisions concerning employment, education, financial services, housing, and health care—and that enables consumers to prevent their personal information from being fed into automated systems that determine access to core economic and social opportunities.[140] Separately, consumers may request access to information about the business's use of ADMT, including the logic of the technology, its output, and how that output was used in the

135 *Id.* § 7001(e); Christine Lyon et al., *California Privacy Agency Narrows Proposed AI-Related Regulations*, FRESHFIELDS (May 14, 2025), https://blog.freshfields.us/post/102kb60/california-privacy-agency-narrows-proposed-ai-related-regulations [https://perma.cc/BKQ8-QG2G].

136 tit. 11, § 7001(e).

137 *See id.* §§ 7221–7222.

138 *Id.* §§ 7220–7221.

139 *Id.* § 7220.

140 *Id.* § 7221.

decision-making process.[141] This access right is subject to limitations: businesses are not required to disclose trade secrets or information that could compromise physical safety.[142] The GDPR imposes a parallel but differently structured transparency obligation. Article 15(1)(h) requires that data subjects receive meaningful information about the logic involved in automated decision-making, along with its significance and envisaged consequences, a standard that is broader in framing but less granular about specific outputs and their application to individual decisions.[143] The practical burden on California businesses is nonetheless substantial: they must be prepared to document and explain the logic of their automated systems, the data inputs, and the decisional pathway on a per-consumer basis upon a valid request.

The cybersecurity audit regulations represent one of the places where California has moved ahead of the GDPR, and it is worth being specific about what the state now requires. Beginning in 2027, businesses must conduct annual cybersecurity audits if their data processing presents a "significant risk" to consumer security.[144] Two independent triggers define the threshold. The first captures data brokers: businesses deriving 50% or more of annual revenue from selling or sharing personal information.[145] The second is conjunctive, requiring both annual gross revenues exceeding approximately $26,625,000 and the processing of personal information of more than 250,000 consumers or households, or sensitive personal information of more than 50,000 consumers.[146] A business that meets either trigger must have a professional—who is qualified, objective, and independent—conduct an annual audit, using recognized auditing standards.[147] That professional can be internal or external, but independence is mandatory either way.[148] The GDPR has nothing comparable. Article 32 requires controllers to implement appropriate technical and organizational security measures, and article 35 mandates data protection impact assessments for high-risk

141 *Id.* § 7222.

142 *Id.*

143 Commission Regulation 2016/679, art. 15(1)(h), 2016 O.J. (L 119) 1, 43 (EU).

144 tit. 11, § 7120(a).

145 *Id.* § 7120(b)(1).

146 *Id.* § 7120(b)(2).

147 *Id.* § 7122(a).

148 *Id. See generally* DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED!: WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT (2022) (arguing that data security regulation should move from reactive, breach-focused enforcement toward proactive systemic oversight mechanisms, including auditing requirements).

processing.[149] But neither provision requires a standardized annual audit, performed by an independent professional, with results certified to a regulator. California built a recurring compliance cycle. Europe left security implementation to the controller's judgment, subject to enforcement after the fact.

The scope of these audits is broad but flexible. The regulations enumerate eighteen categories the auditor must assess "if applicable" to the business's information system: authentication, encryption, access controls, vulnerability scanning, penetration testing, network monitoring, audit-log management, incident response, data retention and disposal, personnel security training, and several others.[150] The phrase "if applicable" is doing important work. The auditor exercises professional judgment in determining which categories are relevant to a particular business. A small e-commerce company and a cloud infrastructure provider will not face identical assessments.[151] The audit report documents the scope of the review, the policies assessed, the criteria applied, and the auditor's findings, which the business retains for at least five years.[152] But here is the part that matters for the regulatory relationship: what the business files with the CPPA each year is a signed certification of completion, not the full report.[153] The certification is due by April 1, with phased deadlines running from 2028 to 2030 depending on revenue tier.[154] The full report stays with the business unless the CPPA or the AG comes looking for it in an enforcement proceeding.[155] That creates an interesting incentive structure. The business knows the regulator can demand the report at any time, which means the report needs to be thorough and defensible even though no one outside the company may ever read it.[156]

VI. CROSS-BORDER TRANSFERS: THE STRUCTURAL ASYMMETRY

The widest structural gap between the GDPR and the CCPA has nothing to do with processing requirements or individual rights. It concerns the regulation of cross-border data flows, and the gap is not a difference of degree. One regime treats the geo-

149 Commission Regulation 2016/679, arts. 32, 35, 2016 O.J. (L 119) 1, 51–52, 53–54 (EU).

150 tit. 11, § 7123(c).

151 *See id.* § 7120.

152 *Id.* §§ 7122(g), 7123(e).

153 *Id.* § 7124.

154 *Id.* § 7121(a).

155 *See id.* §§ 7123–7124.

156 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 630–35 (2014) (discussing how the threat of regulatory action creates compliance incentives that operate independently of formal enforcement).

graphic movement of personal data as an independent regulatory event requiring its own legal justification. The other does not regulate it at all.

The GDPR's position follows from its constitutional foundations. If data protection is a fundamental right guaranteed by articles 7 and 8 of the Charter, then that right cannot be extinguished simply because personal data crosses a border.[157] The CJEU made this explicit in *Schrems II*, holding that the level of protection guaranteed by the GDPR and the Charter must travel with the data.[158] Chapter V of the GDPR operationalizes that principle through a restrictive framework governing transfers to countries outside the EEA.[159] California took a fundamentally different path. The CCPA regulates the commercial character of the downstream disclosure, governing data flows through its definitions of sale, sharing, and the service provider, contractor, and third-party taxonomy, without regard to where the recipient sits.[160] Geography is simply absent from the analysis.[161]

Chapter V follows the same prohibition-with-exceptions logic that runs through the rest of the GDPR. Article 44 restricts all transfers to third countries unless one of the regulation's prescribed mechanisms is satisfied.[162] The most comprehensive is an adequacy decision under article 45. The Commission examines the third country's legal framework and, if it concludes that the country provides a level of protection "essentially equivalent" to that of the Union, adopts a decision permitting transfers without additional safeguards.[163] That is a high bar. It requires more than formal legal protections; it requires effective enforcement, independent supervision, and adequate redress.[164] Where no adequacy decision exists, the exporter must provide "appropriate

157 Charter of Fundamental Rights of the European Union arts. 7–8, Oct. 26, 2012, 2012 O.J. (C 326) 391.

158 Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 105 (July 16, 2020).

159 Commission Regulation 2016/679, arts. 44–49, 2016 O.J. (L 119) 1, 60–65 (EU); *see* BRADFORD, *supra* note 3, at 132–38 (analyzing chapter V as a mechanism for projecting EU regulatory standards onto third countries through the adequacy process).

160 CAL. CIV. CODE § 1798.140 (West 2026).

161 *See* Paul M. Schwartz, *supra* note 2, at 830–35 (2019) (contrasting the EU's data sovereignty model with U.S. approaches that treat cross-border flows as a commercial rather than constitutional question).

162 Commission Regulation 2016/679, art. 44, 2016 O.J. (L 119) 1, 60 (EU).

163 *Id.* art. 45, at 61–62; Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 73 (Oct. 6, 2015) (establishing the "essentially equivalent" standard).

164 *See* Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post* Schrems, 18 GERMAN L.J. 881, 893–97 (2017) (analyzing the substantive demands of the adequacy standard after *Schrems I*).

safeguards" while ensuring that enforceable data subject rights and effective legal remedies remain available.[165] Standard contractual clauses adopted by the Commission are the most widely used instrument, establishing binding obligations on the data importer and enforceable rights for data subjects as third-party beneficiaries.[166] Binding corporate rules, approved codes of conduct, and certification mechanisms are also available, though less commonly relied upon.[167] And where neither adequacy nor appropriate safeguards are in place, transfers may proceed only under the narrow derogations of article 49: explicit consent, contractual necessity, important reasons of public interest, and a handful of other limited bases.[168]

The stakes of this framework became concrete in *Schrems II*. The CJEU struck down the EU-U.S. Privacy Shield adequacy decision, holding that U.S. law failed to provide an essentially equivalent level of protection for personal data transferred from the Union.[169] The Court identified two deficiencies: the lack of proportionality constraints on U.S. surveillance programs operating under section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, and the absence of effective judicial redress for EU data subjects whose data was accessed by U.S. intelligence authorities.[170] But the Court went further. It held that exporters relying on standard contractual clauses bear an independent obligation to assess whether the legal framework of the recipient country permits the importer to comply with the protections set out in the clauses.[171] Where the answer is no, the exporter must implement supplementary measures sufficient to close the gap, or suspend the transfer entirely.[172] The practical consequence is that every cross-border transfer decision now requires something close to a country-level legal risk assessment. Compliance teams must evaluate foreign surveillance authori-

165 Commission Regulation 2016/679, art. 46(1), 2016 O.J. (L 119) 1, 62 (EU).

166 *Id.* art. 46(2)(c), at 62.

167 *Id.* arts. 46(2)(e)–(f), 47, at 62–64.

168 *Id.* art. 49(1), at 64.

169 Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶¶ 65, 201 (July 16, 2020).

170 *Id.* ¶¶ 178–185; *see also* Kuner, *supra* note 164, at 900–05 (anticipating the redress gap as a structural vulnerability in transatlantic transfer mechanisms).

171 Case C-311/18, *Schrems II*, ECLI:EU:C:2020:559, ¶ 134.

172 *Id.* ¶ 135; *see also* Eur. Data Prot. Bd., Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (June 18, 2021), https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf [https://perma.cc/NR3G-W9R6] (explaining that when relevant legislation is lacking a party may decide to suspend, transfer, or implement supplementary measures).

ties, judicial independence, and the enforceability of contractual protections in legal systems they may know nothing about.[173]

The Commission's response was the EU-U.S. Data Privacy Framework (DPF), adopted in July 2023.[174] Its foundation is Executive Order 14086, which introduced necessity and proportionality constraints on U.S. signals intelligence activities and established a two-tier redress mechanism.[175] At the first tier, the Civil Liberties Protection Officer (CLPO) within the Office of the Director of National Intelligence investigates complaints alleging that U.S. surveillance activities violated the safeguards established by the Executive Order.[176] At the second tier, the complainant may appeal to the Data Protection Review Court (DPRC), a newly created body authorized to review the CLPO's determinations, obtain access to classified information, and issue binding remedial orders directed at U.S. intelligence agencies.[177] The entire apparatus is, candidly, an institutional workaround. The United States has no comprehensive data protection authority and no tradition of treating intelligence oversight as a judicial function in the European sense. So the Executive Order constructed a bespoke tribunal designed to satisfy a foreign court's requirements for effective judicial protection under article 47 of the Charter.[178] The European General Court upheld that conclusion in September 2025, dismissing a challenge to the adequacy decision and finding that the DPRC's fixed terms, removal protections, access to classified evidence, and obligation to issue reasoned decisions satisfied EU independence and impartiality

---

173 *See generally* Peter Swire & DeBrae Kennedy-Mayo, *The Risks to Cybersecurity from Data Localization — Organizational Effects*, 8 ARIZ. L.J. EMERGING TECHS. 1 (2025) (documenting the operational burdens that post-*Schrems II* compliance requirements impose on organizations managing cross-border data transfers); PETER SWIRE & DEBRAE KENNEDY-MAYO, FIVE CONCERNS ABOUT HARD DATA LOCALISATION WITHIN THE EUROPEAN UNION 2–3 (2020), https://peterswire.net/wp-content/uploads/Comments-to-EDPB-Recommendations-by-Swire-and-Mayo-2020.pdf [https://perma.cc/6E9H-KGY3] (criticizing the practical feasibility for many organizations of the EDPB's approach to supplementary measures and its implicit localization pressure).

174 *See* Commission Implementing Decision 2023/1795, 2023 O.J. (L 231) 118 (EU).

175 *See* Exec. Order No. 14086, 87 Fed. Reg. 62283 (Oct. 14, 2022).

176 *See id.* § 3(c).

177 *See id.* § 3(d); 28 C.F.R. pt. 201 (2022).

178 *See* Theodore Christakis, *Schrems III? First Thoughts on the EDPB Post-*Schrems II *Recommendations on International Data Transfers (Part 1)*, EUR. L. BLOG (Nov. 13, 2020), https://www.europeanlawblog.eu/pub/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/release/1 [https://perma.cc/V85A-A4FL] (characterizing the DPF as an attempt to construct functional equivalence with EU judicial protection standards through executive rather than legislative action).

standards.[179] That ruling provides stability for now. But the EDPB has already flagged concerns about government acquisition of personal data from commercial data brokers, a channel that falls entirely outside Executive Order 14086's scope and therefore outside the DPF's protective architecture.[180]

The CCPA has no equivalent to chapter V. California does not condition the movement of personal information on the legal adequacy of the destination country, and it draws no distinction between domestic and international transfers as a regulatory matter.[181] What California regulates is the commercial character of the downstream disclosure. The statute defines "sale" as disclosing personal information to a third party for monetary or other valuable consideration, and "sharing" as disclosing personal information for cross-context behavioral advertising; each carries its own notice and opt-out obligations.[182] Disclosures to service providers and contractors are permitted without opt-out rights so long as the recipient is bound by a written contract restricting its use of the data to the business purposes specified in the agreement.[183] None of these restrictions turn on geography. A business that discloses consumer data to a service provider in Texas faces exactly the same obligations as one that discloses to a service provider in Bangkok or Berlin. If the contractual and transactional requirements are satisfied, the location of the recipient is legally irrelevant.[184] The GDPR treats the cross-border movement of personal data as an independent regulatory event requiring its own legal justification. The CCPA treats it as a non-event, fully governed by the same sale, sharing, and service provider rules that apply to any other disclosure.

That indifference to geography runs deep. Nothing in the CCPA or the California regulations requires a business to assess the privacy laws of a foreign jurisdiction before transferring per-

---

179 Case T-553/23, Latombe v. Eur. Commission, ECLI:EU:T:2025:831, ¶ 38–63 (Sept. 3, 2025).

180 *See* Eur. Data Prot. Bd., EDPB Report on the First Review of the European Commission Implementing Decision on the Adequate Protection of Personal Data Under the EU–U.S. Data Privacy Framework, at 20 (Nov. 4, 2024), https://www.edpb.europa.eu/system/files/2024-11/edpb_report_20241104_reportonfirstreviewofeu-u.s.dpf_en.pdf [https://perma.cc/Y9SK-3SW6].

181 *See generally* CAL. CIV. CODE §§ 1798.100–.199.100 (West 2026) (containing no provision analogous to GDPR articles 44–49).

182 CIV. § 1798.140(ad)(1), (ah)(1), 1798.120–.121.

183 *See id.* § 1798.140(ag)(1), (j)(1).

184 *See* Anupam Chander, *Is Data Localization a Solution for* Schrems II*?*, 23 J. INT'L ECON. L. 771, 779–82 (2020) (contrasting regulatory approaches that condition data flows on destination-country adequacy with those that rely on transactional controls).

sonal information there.[185] The same goes for transfers to other U.S. states. There is no transfer impact assessment, no equivalence finding, no supervisory approval. The CCPA's theory of protection runs through the contract, not the border. Service providers and contractors are bound by written agreements that prohibit them from retaining, using, or disclosing personal information outside the direct business relationship, from selling or sharing it, and from combining it with personal information obtained from other sources.[186] If those contractual constraints hold, California treats the data as adequately protected. It does not matter whether the server is in Sacramento or Singapore.[187]

The GDPR operates on a fundamentally different premise. Chapter V is not just a compliance mechanism. It is a tool of regulatory projection, and frankly, it works. The adequacy process creates direct incentives for third countries to reshape their domestic privacy frameworks to secure an adequacy finding. Japan revised its Act on the Protection of Personal Information before obtaining its adequacy decision.[188] South Korea and the United Kingdom undertook similar reforms.[189] That is a remarkable amount of leverage for a single chapter of a regulation. California has no comparable provision and, to be clear, is not trying to have one. Its regulatory energy is directed inward, toward the contractual supply chain, not outward toward the legal systems of trading partners. The result is a gap that goes beyond regulatory design. It reflects two different theories of what data protection law is for. The GDPR pursues a form of data sovereignty rooted in fundamental rights, seeking to ensure that protection follows the data wherever it travels. The CCPA pursues transactional integrity. It wants to make sure businesses honor the terms of the commercial relationship through which the data was collected. Neither approach is obviously wrong. But the structural consequences for multinational compliance are significant, and

185 *See generally* CIV. §§ 1798.100–.199.100 (failing to contain a provision requiring consideration of foreign laws before transfer of data); CAL. CODE REGS. tit. 11, §§ 7000–7102 (2026) (failing to contain a provision requiring consideration of foreign laws before transfer of data).

186 CIV. § 1798.140(ag)(1)(B), (j)(1).

187 *See* Hoofnagle, van der Sloot & Borgesius, *supra* note 76, at 88–90 (noting the absence of any cross-border transfer restriction in the CCPA as a fundamental structural departure from the European model).

188 *See* Commission Implementing Decision 2019/419, 2019 O.J. (L 76) 1, 31–32 (EU); *see also* BRADFORD, *supra* note 3, at 132–38 (documenting the adequacy mechanism as a driver of regulatory convergence in third countries).

189 Commission Implementing Decision 2022/254, 2022 O.J. (L 44) 1, 29 (EU) (South Korea); Commission Implementing Regulation 2021/1772, 2021 O.J. (L 360) 1, 2–3 (EU) (United Kingdom).

companies attempting to operate under both regimes simultaneously will discover that the two frameworks cannot simply be stacked on top of each other.

VII. CONTRACTUAL FLOW-DOWNS AND PRIVATE GOVERNANCE

Both regimes have converged on the same basic insight: if you want privacy law to mean anything downstream, you have to write it into the contracts. The GDPR and the CCPA each require businesses to impose data protection obligations on the entities that process personal information on their behalf. But they do it differently, and the differences reflect the broader architectural choices each regime has made.[190]

The GDPR's approach runs through article 28, which requires that any processing carried out by a processor be governed by a binding contract or legal act.[191] The required terms are specific and nonnegotiable. The processor must act only on the controller's documented instructions. It must ensure that authorized personnel are bound by confidentiality. It must implement article 32 security measures. It must comply with the rules on subprocessor engagement, including obtaining the controller's prior authorization. It must assist the controller with data subject rights requests, breach notifications, impact assessments, and prior consultations with supervisory authorities. At the end of the relationship, it must delete or return all personal data. And it must submit to audits.[192] Eight mandatory clauses, oriented around a single principle: the processor is an extension of the controller, and the contract exists to keep it on a leash.

The CCPA takes a different angle. Its contract requirements exist not to govern the relationship between a controller and its agent, but to prevent a business disclosure from being reclassified as a sale or sharing of personal information.[193] If a business

---

190 *See* W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAW. 221, 226–27, 233 (2017) (analyzing the GDPR's contractual flow-down requirements as a mechanism for extending regulatory standards through private ordering).

191 Commission Regulation 2016/679, art. 28(3), 2016 O.J. (L 119) 1, 49–50 (EU); *see also* Eur. Data Prot. Bd., Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, ¶¶ 108–43 (Sep. 2, 2020), https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf [https://perma.cc/BPU2-KW5G] (interpreting the mandatory content requirements of article 28 contracts).

192 Commission Regulation 2016/679, art. 28(3), 2016 O.J. (L 119) 1, 49–50 (EU).

193 CAL. CIV. CODE § 1798.140(j)(1), (ag)(1) (West 2026); *see* Christy Harris & Charlotte Kress, *Examining Industry Approaches to CCPA "Do Not Sell" Compliance*, FUTURE OF PRIV. F. (Dec. 19, 2019), https://fpf.org/blog/examining-industry-approaches-to-ccpa-do-not-sell-compliance/ [https://perma.cc/NW8J-PGED].

discloses personal information to a service provider or contractor without a qualifying written contract, that disclosure may trigger the CCPA's opt-out rights. That is the last thing most businesses want.[194] So the contract does real work. It must prohibit the recipient from selling or sharing the personal information, retaining or using it for any purpose other than the business purposes specified in the agreement, using it outside the direct business relationship, and combining it with personal information obtained from other sources.[195] The CPPA's regulations add further layers, requiring the contract to obligate the service provider or contractor to comply with the CCPA, provide the same level of privacy protection as the statute requires of businesses, and grant the business monitoring and audit rights.[196] Contractors must also certify that they understand and will comply with these restrictions.[197] The orientation is different from article 28. The GDPR's contract regime is about ensuring the processor follows the controller's instructions and cooperates with regulatory obligations. The CCPA's regime is about preventing unauthorized commercialization of consumer data. The GDPR asks: is the processor doing what it was told? The CCPA asks: is the recipient doing something with this data that the consumer did not sign up for?

Both regimes require these obligations to flow downstream. It is not enough to bind your immediate vendor. The obligations have to follow the data through the entire processing chain.

Under the GDPR, article 28(4) is explicit: where a processor engages a sub-processor, the same data protection obligations from the controller-processor contract must be imposed on the sub-processor by way of a separate contract.[198] If the sub-processor fails to meet those obligations, the initial processor remains fully liable to the controller.[199] That is a strict liability chain. The controller does not get to plead ignorance about what is happening three levels down. California's regulations take a parallel approach. Section 7051(b) requires that a service provider or contractor who subcontracts with another person must enter into a contract with the subcontractor that complies with the

194 See CAL. CODE REGS. tit. 11, § 7050(e) (2026).

195 CIV. § 1798.140(ag)(1)(A)–(D), (j)(1)(A)(i)–(iv).

196 *See* tit. 11, § 7051(a)(6)–(7).

197 CIV. § 1798.140(j)(1)(B).

198 Commission Regulation 2016/679, art. 28(4), 2016 O.J. (L 119) 1, 50 (EU).

199 *Id.*; see *also* Eur. Data Prot. Bd., *supra* note 191, ¶¶ 147–55 (discussing the cascading liability structure for sub-processing under article 28(4)).

full set of CCPA contractual requirements.[200] The statute separately requires that if a contractor engages any other person to assist in processing, the engagement must be pursuant to a written contract binding the subcontractor to the same restrictions.[201] On both sides of the Atlantic, the result is the same: compliance obligations cascade down through the supply chain, and every link in the chain must be papered.[202]

What this creates, in practice, is a system of private governance. Both regimes have conscripted businesses into performing a regulatory function.[203] The GDPR's audit rights under article 28(3)(h) require the processor to make available all information necessary to demonstrate compliance and to allow for and contribute to audits and inspections.[204] The CCPA's regulations go further in one specific respect: they tie the business's own legal exposure to whether it exercises its oversight rights. Section 7051(c) provides that a business's due diligence of its service providers and contractors is a factor in determining whether the business had reason to believe the service provider was violating the CCPA.[205] A business that never enforces its contract terms, never audits, and never tests its vendor's compliance posture may lose the ability to argue that it did not know the vendor was misusing consumer data. That is a regulatory incentive to police your own supply chain, and a penalty for looking the other way. No agency has the resources to audit every data processing relationship in a modern digital economy. The GDPR and the CCPA both recognize this, and their shared solution is to turn the businesses themselves into the front line of enforcement, using contracts as the delivery mechanism for regulatory standards. The question that neither regime has fully answered is what happens when the business at the top of the chain lacks the technical capacity or commercial leverage to meaningfully audit the entities further down it.[206]

---

200 tit. 11, § 7051(b).

201 CIV. § 1798.140(j)(2).

202 *Cf.* Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMMC'N L. & POL'Y 405, 425–28 (2010) (examining the enforceability of terms of use agreements imposed on passive online users).

203 *Cf.* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 286–87 (2011) (documenting the emergence of corporate privacy management as a form of decentralized regulatory implementation).

204 Commission Regulation 2016/679, art. 28(3)(h), 2016 O.J. (L 119) 1, 49 (EU).

205 tit. 11, § 7051(c).

206 *See* Solove & Hartzog, *supra* note 156, at 640–45 (discussing the gap between regulatory expectations of corporate oversight and the practical capacity of businesses to monitor third-party data practices).

VIII. CONCLUSION

This Article set out to do something straightforward: read the primary sources of both regimes side by side and map where they align and where they diverge. The answer, in short, is that they diverge more than most compliance discussions acknowledge.

The GDPR is built on a fundamental rights architecture. It requires an affirmative legal basis before any processing begins. It treats cross-border data flows as an independent regulatory event, conditioning them on the adequacy of foreign legal systems or the adoption of binding contractual safeguards. It projects its standards outward, using the adequacy mechanism to reshape the domestic privacy laws of trading partners. And it backs all of this with a contractual flow-down regime that turns every processor agreement into a vehicle for regulatory enforcement. The intellectual commitment is to continuity of protection: the rights of the data subject should not diminish because a server sits in a different country.

The CCPA starts from a different place. It does not require a lawful basis for processing. It does not care where the data goes, as long as the commercial terms governing the disclosure are met. Its theory of protection runs through transparency, purpose limitation, and the contractual supply chain. The 2025 regulations on automated decision-making technology, cybersecurity audits, and risk assessments represent a significant maturation of the California model, but they do not change its fundamental orientation. California is regulating commercial conduct. The EU is regulating the conditions under which personal data may exist outside its borders.

That is a difference of kind, and it has practical consequences that anyone doing business across both regimes will recognize. A multinational company cannot simply map its GDPR compliance program onto its CCPA obligations and call it done. The triggers are different. The contractual architectures serve different purposes. The enforcement mechanisms point in different directions. The two regimes share vocabulary, and they sometimes reach similar outcomes, but they are answering fundamentally different questions about what data protection law is for.

I also want to be honest about the limitations of both models. The GDPR's ambition comes at a cost: a compliance burden that can be paralyzing for smaller organizations, a transfer regime that has been invalidated twice by its own court, and an accountability framework that sometimes prioritizes documentation over

substance. The CCPA's pragmatism has its own blind spots. A framework that ignores the geographic movement of data may prove inadequate as governments increasingly treat data flows as instruments of geopolitical leverage. Both regimes are works in progress. Both will continue to evolve. The value of comparing them with this level of granularity is that it gives scholars and practitioners an honest map of what each regime actually requires, where they overlap, and where the gaps between them create compliance risk.

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 online at www.chapmanlawreview.com or by e-mail at chapman.law.review@gmail.com. Submission inquiries can be sent to chapmanlawreview.submissions@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.