Narrowing Data Protection's Enforcement Gap

Filippo Lancieri

Follow this and additional works at: https://digitalcommons.mainelaw.maine.edu/mlr

Part of the Comparative and Foreign Law Commons, Internet Law Commons, Law and Economics Commons, and the Privacy Law Commons

Recommended Citation
Filippo Lancieri, Narrowing Data Protection's Enforcement Gap, 74 Me. L. Rev. 15 (2022). Available at: https://digitalcommons.mainelaw.maine.edu/mlr/vol74/iss1/3

This Article is brought to you for free and open access by the Journals at University of Maine School of Law Digital Commons. It has been accepted for inclusion in Maine Law Review by an authorized editor of University of Maine School of Law Digital Commons. For more information, please contact mdecrow@maine.edu.
Narrowing Data Protection's Enforcement Gap

Cover Page Footnote

Post-Doctoral Fellow, ETH Zurich Center for Law and Economics; Research Fellow, The George J. Stigler Center for the study of the Economy and the State, UChicago Booth. I would like to thank Lior Strahilevitz, Omri Ben-Shahar, Lisa Bernstein, Adam Chilton, William Hubbard, Brian Leiter, Peter Swire, Travis Crum, Ari Ezra Waldman, Spencer Smith, Nicolo Zingales, Julian Nowag, Joris van Hoboken, Jens Prüfer, Jens Frankenreiter, Giorgio Monti, Inge Graef, Nik Guggenberger, Justin Hemmings, Emilie Aguirre, Erin Miller, Roger Ford, Oles Andriychuk, Angela Daly and participants of the 2021 Privacy Law Scholars Conference, the 25th annual Conference of the Society for Institutional and Organizational Economics, The University of Tilburg TILT/TILEC Workshop on Regulating Digital Markets: Enforcement and Remedies, The 38th Annual Conference of the European Association of Law and Economics, the Yale ISP Ideas Lunch Workshop, the University of Chicago Junior Scholars Colloquium, the University of Chicago Legal Scholarship Workshop, the University of Strathclyde Law School Centre for Internet Law and Policy Workshop, the 16th Annual Conference of the Italian Association of Law and Economics and of the University of Sao Paulo Antitrust Law and Digital Technology Workshop for insightful comments and discussions. I would also like to thank Blake McCartney and the Maine Law Review team for terrific editing. All errors are my own, of course.

This article is available in Maine Law Review: https://digitalcommons.mainelaw.maine.edu/mlr/vol74/iss1/3
NARROWING DATA PROTECTION’S ENFORCEMENT GAP

Filippo Lancieri

ABSTRACT

INTRODUCTION

I. THE RISE OF DATA PROTECTION LAWS
   A. Data Protection on the Books
   B. An Underwhelming Track-Record (So Far)

II. HOW DESIGN FAILURES UNDERMINE DATA PROTECTION ENFORCEMENT
   A. Market Forces
      1. Markets Can Force Companies to Reflect the Privacy Preferences of Consumers
      2. The Heightened Information Asymmetries in Data Protection
      3. Market Concentration Further Hinders Exit and Voice
   B. Torts
      1. Tort Liability as a Complement to Market Forces
      2. Information Asymmetries and Market Power Undermine the CCPA
      3. Information Asymmetries and Market Power Undermine the GDPR
   C. Regulatory Enforcement
      1. Command-and-Control Regulation as a Third Enforcement Mechanism
      2. The Risks of Regulatory Capture in Data Protection
         a. Information Asymmetries and Market Power Increase the Risks of Capture in Data Protection
         b. The Systems Lack Appropriate Counterweights
      3. Data Authorities are Under a Heightened Risk of Being Chronically Underfunded

III. NARROWING DATA PROTECTION’S ENFORCEMENT GAP THROUGH INSTITUTIONAL DESIGN
   A. Multiplying Monitoring and Enforcement Resources
   B. Bringing Data Protection Violations to Light
   C. Increasing Governmental Accountability

CONCLUSION

APPENDIX

Impacts on the Ground: A Survey of the Empirical Evidence on How the GDPR and CCPA Impacted Data Protection
NARROWING DATA PROTECTION’S ENFORCEMENT GAP

Filippo Lancieri*

ABSTRACT

The rise of data protection laws is one of the most profound legal changes of this century. Yet, despite their nominal force and widespread adoption, available data indicates that these laws recurrently suffer from an enforcement gap—that is, a wide disparity between the stated protections on the books and the reality of how companies respond to them on the ground. Indeed, Appendix I to this Article introduces a novel literature review of twenty-six studies that analyzed the impact on the ground of the GDPR and the CCPA: none found a meaningful improvement in citizen’s data privacy. This raises the question: what accounts for this gap and what can be done to improve the performance of these laws?

This Article begins by describing three core building blocks of data protection regimes in the United States and Europe—namely, market forces, tort liability and regulatory enforcement—that these jurisdictions combine in different ways to ensure that companies act in accordance with consumers’ privacy preferences. It then identifies two key reasons—particularly deep information asymmetries between companies and consumers/regulators, and high levels of market power in many data markets—that enable companies to behave strategically to protect private interests and undermine legal compliance.

The conclusion looks at the institutional design of antitrust and anti-fraud laws—two regulatory regimes that face similar challenges in their implementation—to argue that an effective online privacy regulatory system should be built around three key principles. First, the system must multiply monitoring and enforcement resources, and antitrust demonstrates how litigation can fund sophisticated civil-society intermediaries that safeguard consumers. Second, the system must bring violations to light, and anti-fraud policies demonstrate the importance of establishing effective whistleblower programs for data protection. Third, the system must

* Post-Doctoral Fellow, ETH Zurich Center for Law and Economics; Research Fellow, The George J. Stigler Center for the study of the Economy and the State, UChicago Booth. I would like to thank Lior Strahilevitz, Omri Ben-Shahar, Lisa Bernstein, Adam Chilton, William Hubbard, Brian Leiter, Peter Swire, Travis Crum, Ari Ezra Waldman, Spencer Smith, Nicolo Zingales, Julian Nowag, Joris van Hoboken, Jens Prufer, Jens Frankenreiter, Giorgio Monti, Inge Graef, Nik Guggenberger, Justin Hemmings, Emilie Aguirre, Erin Miller, Roger Ford, Oles Andriychuk, Angela Daly and participants of the 2021 Privacy Law Scholars Conference, the 25th annual Conference of the Society for Institutional and Organizational Economics, The University of Tilburg TILT/TILEC Workshop on Regulating Digital Markets: Enforcement and Remedies, The 38th Annual Conference of the European Association of Law and Economics, the Yale ISP Ideas Lunch Workshop, the University of Chicago Junior Scholars Colloquium, the University of Chicago Legal Scholarship Workshop, the University of Strathclyde Law School Centre for Internet Law and Policy Workshop, the 16th Annual Conference of the Italian Association of Law and Economics and of the University of Sao Paulo Antitrust Law and Digital Technology Workshop for insightful comments and discussions. I would also like to thank Blake McCartney and the Maine Law Review team for terrific editing. All errors are my own, of course.
increase governmental accountability, and antitrust provides examples on how to promote public transparency without sacrificing enforcement capacity.

INTRODUCTION

The 2016 European General Data Protection Regulation (GDPR)\(^1\) was hailed as ushering in a new era for digital privacy. It led companies and European countries to invest significant resources in designing regulatory compliance programs.\(^2\) It also influenced many other online privacy laws adopted across the world—including, to some extent, the groundbreaking California Consumer Privacy Act of 2018 (CCPA).\(^3\) Yet, years later privacy advocates are growing increasingly frustrated with firms’ lack of compliance and countries’ lax enforcement. Indeed, the gap between the law on the books and the law in action appeared to be so great that by the end of 2020 many of the GDPR’s strongest supporters warned that it risked becoming a “fantasy law”—something firms paid lip service to but nonetheless widely failed to comply with.\(^4\) Frustration with the CCPA was equally widespread, leading privacy advocates to immediately start drafting a new law to strengthen its enforcement mechanisms—the California Privacy Rights Act (CPRA) passed the ballot vote in November 2020 and will come into force in 2023.\(^5\)

Concerns around an enforcement gap in data protection laws are sensible. Older digital privacy regimes in Europe and the United States have largely failed to ensure that companies comply with consumers’ preferences for increased control over their personal data.\(^6\) While it is too early to decree the failure of newer regimes such as the GDPR and the CCPA, most of the available analyses point to underwhelming results. Since both laws entered into force, none of the twenty-six independent empirical studies conducted to assess their impact on the ground found meaningful legal compliance.\(^7\) For example, a 2019 academic survey found that 92% of Europe’s most accessed websites tracked users before providing any notice, and 85% maintained or increased tracking even after the users opted-out—both clear

---

1. See generally Commission Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) (EU) [hereinafter GDPR]. This paper uses interchangeably the phrases “data privacy,” “online privacy,” “data protection,” and “digital privacy” refer to limits on the collection and processing of personal data.


6. See infra Section I.B, Appendix.

7. See infra Appendix.
violations of the GDPR.\(^8\) A cookie sweep of thirty-eight large data processors performed by the Irish Data Protection Commission found that more than eighteen months after the GDPR had come into force, 95% violated the law in at least one meaningful way.\(^9\) Another report exposed how European data authorities are underfunded and poorly staffed.\(^10\) There are fewer comprehensive analyses for the CCPA (it only came into force in January 2020), but the law apparently led to no changes to Facebook’s data collection and processing practices.\(^11\) A January 2020 survey of the websites of the six hundred largest companies in the U.S. found that even among the richest, most sophisticated American companies, a majority did not offer CCPA portals for users to access their information, and in some important sectors such as technology, media, telecommunications, and health services, only around 40% of companies did so.\(^12\) Another survey of business-to-consumer companies found that these businesses are receiving an average of eleven data-related requests per month for every million California consumer identities they hold, meaning that the CCPA was only used by 0.001% of Californian consumers.\(^13\) The very passage of the CPRA represented an admission that, despite its broad promises, the CCPA is unlikely to meaningfully improve consumer data privacy.

These findings raise two questions for academics and policymakers. First, are there important gaps in the enforcement mechanisms of data protection laws? Second, if yes, what can be done to improve their performance?

This Article helps answer both questions. First, it suggests that modern data protection laws largely fail to anticipate how exceptionally large information asymmetries and market power that are present in many data markets undercut legal compliance in the shadows of the law. Second, it examines the institutional design of antitrust and anti-corporate fraud laws—both established legal regimes that face similar challenges with regards to information asymmetries and market power undermining compliance—to propose legal and institutional changes that can help narrow this enforcement gap in data protection.

In order to address these questions, this Article is divided into three parts. Part I briefly outlines the rise of data protection laws in the U.S. and the EU and reviews the empirical literature on their (so far limited) impact on the ground.

---


Part II, the core of the Article, explores how Americans and Europeans designed their legal regimes to harness different combinations of market forces, tort liability, and regulatory enforcement as mechanisms to ensure that companies reflect consumers’ privacy preferences. Yet, if consumers cannot understand price-to-quality ratios in products that produce or rely on personal data, they cannot take advantage of the traditional options of exit (switching suppliers) and voice (complaining to management) as strategies to force companies to comply with their preferences. Similarly, if consumers and lawyers cannot identify problems in products and services or link them to recognizable legal harms, then they cannot rely on tort lawsuits as an alternative to punish non-compliant companies. Finally, the opacity and complexity of data markets undermines regulatory enforcement in two distinct manners: (i) it increases the opportunities for companies to distort regulations to their advantage without facing significant political backlash, and (ii) it expands the public resources needed to maintain a regulatory regime dedicated to discovering and successfully prosecuting violations. Lawmakers also failed to anticipate how market power allows some companies that collect and process a significant amount of personal data to behave strategically to protect private interests and undermine legal compliance in the shadows of the law. In particular, dominant digital platforms rely on the economic and political capabilities associated with their market power to: (i) design data markets in ways that exacerbate their inherent information asymmetries, (ii) further undermine consumer exit and voice strategies, (iii) combat tort litigation and regulatory enforcement, and (iv) influence governmental policy to their advantage.

While these are relevant flaws in the design of data protection laws, they are not insurmountable. Part III explores what experiences with the enforcement of antitrust and anti-corporate fraud laws can teach policymakers in terms of institutional design changes that can narrow this enforcement gap. Focusing on the institutional alternatives to diminish information asymmetries in the enforcement of data protection laws, Part III suggests that online privacy regulatory systems should be built around at least three key principles.

First, the system must multiply monitoring and enforcement resources. In particular, sophisticated civil-society intermediaries such as privacy non-governmental organizations (NGOs), independent think-tanks, investigative journalism outlets, and class-action plaintiffs play an outsized role in ensuring deterrence and protecting consumers in opaque and complex markets. These organizations have the incentive and the capacity to understand the complexity of data collection and denounce violations. In doing so, these organizations can also monitor the performance of regulatory agencies and increase the costs of regulatory capture. A comparative look at antitrust policy provides a valuable example of how regulatory agencies can use the resources raised by public fines, grants, and cy pres

---

14. Antitrust scholars are increasingly focused on tackling the market power of digital platforms. See Filippo Lancieri & Patricia Morita Sakowski, *Competition in Digital Markets: A Review of Expert Reports*, 26 STAN. J. L. BUS. & FIN. 65, 65 (2021) (consolidating expert reports proposing antitrust and regulatory interventions to diminish the market power of companies such as Google, Facebook, Apple, and Amazon).
awards imposed by data protection laws to properly fund their enforcement efforts, while ensuring their independence from industry interests.

Second, the combination of broad scope, opacity, and complexity that characterizes data protection encumbers the detection of legal violations, increasing the resources needed for society to identify non-compliance. To counteract this, the enforcement system should be designed to bring violations to the attention of monitors. Antitrust and anti-corporate fraud policies have long relied on leniency and whistleblower programs to encourage insiders to reveal wrongdoing. Data protection laws should learn from these policies and develop a solid whistleblower program to help bring violations to light.

Third, public enforcement systems must ensure that regulators are accountable to civil society. Governments have a legitimate interest in enabling the widespread collection of personal data because data is a key input to national security and to companies competing in a digital world. A combination of governmental interests, the market power of large digital platforms, and the complexity and opacity that characterizes many data markets increases the risk that regulators will promote industry rather than consumer interests. Modern data protection regimes lack institutional safeguards that can help thwart regulatory capture. While transparency is key to help societies fight powerful vested interests, many data protection agencies are opaque. Antitrust regimes provide an example of how to design a regulatory framework that increases transparency without sacrificing enforcement capacity.

I. THE RISE OF DATA PROTECTION LAWS

A. Data Protection on the Books

The United States and Europe first developed privacy rights to safeguard individual dignity, autonomy, and to preserve some form of information self-determination.15 A right to privacy naturally includes the protection of personal information that citizens do not want disclosed, and the “right to be left alone.”16 The increasingly important role that databases containing personal data played in the lives of citizens during the second half of the 20th Century influenced the expansion of this “right to informational privacy” to incorporate some form of “right to data protection.”17

17. Fred H. Cate, The Failure of Fair Information Privacy Principles, in CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 343, 345-46 (Jane K. Winn ed., 2006); see also Riley v. California, 573 U.S. 373, 391 (2014) (concluding that modern day smartphones hold so much personal data that law enforcement needs a warrant to search them). The U.S. led this recognition of a right to data protection by passing the Fair Credit Reporting Act of 1970 and the Privacy Act of 1974, as well as a series of statutes that oversee the collection of specific data such as health (the Health Insurance Portability and Accountability Act of 1996) or children (the Children’s Online Privacy Protection Act of 1998). In the EU, this transition started with a 1981 convention, a 1995 directive, and then Article 8 of the EU Charter on Fundamental Rights, which affirms data protection as a fundamental right. Lancieri, supra note 15, at 30-31.
The EU was among the first jurisdictions to enact an economy-wide directive specifically focused on imposing limits on the collection and processing of personal data.\textsuperscript{18} However, widespread concern around the directive’s lack of effectiveness motivated the passage of the GDPR in 2016.\textsuperscript{19} The GDPR grants EU citizens strong rights with regard to their data and also imposes a series of obligations on governments and companies that handle such data.\textsuperscript{20} Noteworthy provisions of the GDPR include: (i) requirements that data are processed in a lawful, fair, and transparent manner;\textsuperscript{21} (ii) requirements that users grant explicit consent to enable the collection and processing of data;\textsuperscript{22} (iii) data minimization and purpose limitation;\textsuperscript{23} (iv) a right to be forgotten and to data portability;\textsuperscript{24} (v) data protection by design and by default;\textsuperscript{25} (vi) minimum requirements around data security;\textsuperscript{26} (vii) an obligation that companies perform impact assessments for new technologies or new uses of data and notify users about data breaches;\textsuperscript{27} (viii) the strengthening of data protection authorities;\textsuperscript{28} and (ix) a right for citizens to go to court to directly obtain full compensation for damages associated with violations of data protection laws.\textsuperscript{29}

The U.S. lacks a similar economy-wide data protection regime, historically relying on the Federal Trade Commission (FTC) as a de-facto online privacy regulator.\textsuperscript{30} The FTC enforces a regime of informed consent, where it primarily ensures that companies disclose to consumers how the company collects and processes data so that consumers can make an informed decision on whether to accept these terms in a take-it-or-leave-it fashion.\textsuperscript{31} The FTC does not impose general limits on how personal data is collected or processed. Further, the agency lacks power to impose fines or other non-voluntary punishments, except in specific contexts,\textsuperscript{32} and the Supreme Court recently curtailed the FTC’s power to mandate

\textsuperscript{18} See Chris Jay Hoofnagle et al., The European Union General Data Protection Regulation: What it is and What it Means, 28 INFO. & COMM’NS TECH. L. 65, 69-72 (2019) (summarizing the developments that led to the GDPR in the EU). Directive 95/46/EC required EU member states to impose limits on the basis under which companies can collect and process personal data, created rights of access and rights of rectification, and required the creation of dedicated regulators (among others). It is complemented by Directive 2002/58/EC (the “ePrivacy Directive”) which requires that users are properly informed and consent to being tracked by certain types of cookies and other online tracking methods, among other protections for electronic communications. \textit{Id.}

\textsuperscript{19} \textit{Id.} at 71.

\textsuperscript{20} See generally \textit{Id.}

\textsuperscript{21} See GDPR, supra note 1, art. 5.

\textsuperscript{22} GDPR, supra note 1, arts. 6, 7. While consent is the first, and likely most important, of the potential bases for the lawful collection and processing of personal data, it is only one of six. See \textit{Id.}

\textsuperscript{23} \textit{Id.} arts. 5(1)(b)-5(1)(c)

\textsuperscript{24} \textit{Id.} arts. 17, 20.

\textsuperscript{25} \textit{Id.} art. 25.

\textsuperscript{26} \textit{Id.} arts. 32-34.

\textsuperscript{27} \textit{Id.} arts. 33-35.

\textsuperscript{28} \textit{Id.} arts. 51-59.

\textsuperscript{29} \textit{Id.} arts. 77-83. EU Data Protection authorities can fine companies up to 4% of their worldwide turnover for violations of data protection laws. \textit{Id.} art. 83.

\textsuperscript{30} See Lancieri, supra note 15, at 32.


\textsuperscript{32} \textit{Id.} at 604-05.
the disgorgement of illegal profits. Enforcement is ex-post and focused on fraud or clear misstatements.

The lack of a federal law combined with the fact that most large tech platforms are based in California means that the CCPA is the leading U.S. consumer data privacy regulation. The CCPA is both narrower in scope than the GDPR and reflects fundamental differences in the role privacy plays in society. Nonetheless, it represents a significant expansion over the simple informed consent doctrine. Noteworthy provisions include: (i) stronger notification requirements for the collection and processing of personal data, (ii) a right of access and of erasure, (iii) a right to object against the selling of personal information, (iv) an obligation that companies create “data portals,” (v) a right to data portability, (vi) and a direct right of action for damages in cases of data breaches (up to $750 per incident or actual damages, whichever is greater). The Office of the California Attorney General holds exclusive powers to enforce most CCPA provisions (apart from data breaches) and is also responsible for updating the terms of the regulation.

In 2020, Californians passed the CPRA through a direct ballot, amending and expanding the CCPA to strengthen its enforcement mechanisms. The CPRA’s main additions include: (i) the creation of a subgroup of sensitive personal data; (ii) the expansion of disclosure requirements; (iii) the expansion of the consumers’ “right to know” to include all personal data that businesses sell or share for purposes of digital advertisement (including the right to opt-out of both processes through a “do not sell or share” and a “limit the use of my sensitive personal information” button); (iv) the right to limit the use and disclosure of sensitive personal data; (v) the creation of the California Privacy Protection Agency (a regulatory agency with powers to enact regulations and impose administrative fines); and (vi) the determination that 9% of a fund that collects data protection fines should be annually distributed to civil society as grants.

The GDPR, CCPA, and CPRA are distinct bodies of law that differ in many important manners. Yet, at their core they reflect a general belief that companies

34. Chander et al., supra note 3, at 1769.
35. Lancieri, supra note 15, at 32 (explaining how Europeans treat data as a fundamental right, while Americans treat data as an asset).
36. CAL. CIV. CODE §§ 1798.100, 1798.105, 1798.110, 1798.125, 1798.130, 1798.150, 1798.155, 1798.185 (effective until Jan. 1, 2023). Penalties vary between $2,500 per routine violation and $7,500 per intentional violation. Id. § 1798.155.
37. Id § 1798.155.
38. Id. §§ 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140, 1798.160, 1798.199. Like the California Attorney General, the California Privacy Protection Agency can also impose administrative fines of up to $2,500 per each non-intentional violation of the law and $7,500 per each intentional violation. Id. § 1798.155.
39. See Chander et al., supra note 3, at 1746-62 (comparing the GDPR and the CCPA and concluding that they offer “a fundamentally different regime [for data privacy]”).
were not responsive to citizens’ preferences for increased control over how their personal data is collected and processed.\(^\text{40}\)

The GDPR was passed partially in response to widespread concerns by European citizens regarding the collection and processing of personal data. For example, 67% of Europeans were concerned about not having complete control over their personal data, 69% were concerned about mismatches between information collection and processing, and 90% believed it was important to have similar data protection rights across the EU.\(^\text{41}\) The GDPR states that a central tenet of data protection is that Europeans have a right to know what type of personal data is being collected about them and how it is processed.\(^\text{42}\) The GDPR is expressly designed to address short-comings with the enforcement of older European data protection regimes by creating a system that protects these fundamental privacy rights and ensures compliance.\(^\text{43}\)

Similarly, a majority of Americans are concerned about data harvesting by corporations—81% of respondents to a 2019 survey indicated that they lacked control over their personal data and that the risks of data collection outweighed the benefits while 79% were concerned that their data was being misused.\(^\text{44}\) By passing the CCPA, California’s legislature explicitly intended to give California consumers “an effective way to control their personal information” by giving them the right: (i) “to know what personal information is being collected about them”; (ii) “to know whether their personal information is sold or disclosed and to whom”; (iii) “to say no to the sale of personal information”; (iv) “to access their personal information”; and (v) “to receive equal service and price, even if they exercise their privacy rights”.\(^\text{45}\) The CCPA was initially slated to be subject to a public vote and the wide expectation of its passage forced the industry to cut a legislative deal.\(^\text{46}\) The CPRA, which proposed to strengthen these enforcement mechanisms, ultimately won the public vote by a landslide and expressively states that consumers are not aware of how companies collect and process personal data, that they need stronger laws to

\(^{40}\) GDPR recitals 7 and 11 expressly state that “[n]atural persons should have control of their own personal data” and that this requires the development of a strong regime to ensure compliance. GDPR, supra note 1, recitals 7, 11. The CCPA Section (2)(h) states that “[p]eople desire privacy and more control over their information. California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information.” A.B. 375, Gen. Assemb., Reg. Sess. (Cal. 2018).

\(^{41}\) See GDPR, supra note 1, recitals 7, 9, 11; EUR. COMM’N, SPECIAL EUROBAROMETER 431 - DATA PROTECTION 4, 10, 15 (2015).

\(^{42}\) GDPR, supra note 1, recital 39; Chander et al., supra note 3, at 1750.

\(^{43}\) See GDPR, supra note 1, recitals 9, 11.


protect their fundamental privacy rights, and that the Government of California must strengthen the enforcement of these rights over time.47

Some have discounted this clear preference for increased data control, asserting that while citizens submit that they want increased protection, they trade their personal data for small incentives—an apparent contradiction known as the privacy paradox.48 Yet, while some disconnect between stated privacy preferences and actual personal behavior does exists,49 there is also “ample and enduring” evidence that consumers recurrently act to protect their privacy in both online and offline scenarios;50 and many paradoxical cases can be explained by the fact that data protection is “extraordinarily difficult to manage, or regulate, in the internet age” as firms explore known limitations in consumer rationality to extract as much personal information as viable.51

That is not to say that every citizen has strong preferences for increased data protection, nor that these laws are perfect—the GDPR and the CCPA have been praised by many,52 but criticized by some who believe they harm innovation, replace consumers’ preferences with regulators’ preferences, and stifle free expression.53 Rather, they reinforce the notion that consumers’ persistent call for better data protection should be accounted for.54 A key reason driving the passage of the largely popular CCPA, CPRA and GDPR by the democratically elected governments in California and the EU is exactly because they found a disconnect exists between citizens preferences for increased protection and control of their personal data, and market practices ignoring these preferences. Equally important, these laws are leading to billions of dollars of investments in compliance programs.55 Societies must ensure that these expenditures are not simply wasted, but actually change market practices.

47. Annotated Text, supra note 46 (Sections 2(E)-(H)).
50. Acquisti et al., supra note 48, at 737; Acquisti et al., supra note 44, at 477-78. These scenarios range from simple analysis of consumer behavior to surveys, field studies, experiments and other pieces of data.
52. Schwartz, supra note 3, at 772-73.
54. Acquisti et al., supra note 48, at 750.
55. See PwC, supra note 2; Ari Ezra Waldman, Privacy Law’s False Promise, 97 WASH. U. L. REV. 773, 777, 803-07 (2020) (describing the large “paper trails” created by privacy compliance programs, but that do not materially improve data protection).
B. An Underwhelming Track-Record (So Far)

Despite these bold ambitions, the historical track-record of data protection laws in the EU and the U.S. is underwhelming. A solid body of work shows how private parties never complied with the commands of two European data protection directives that preceded the GDPR. By one account, an average of 74% of EU websites constantly violated the rules without suffering any form of punishment. Across the Atlantic, even governmental authorities have deemed the FTC as incapable of ensuring meaningful regulatory deterrence because of its lack of power to fine firms for data-related violations. This criticism came before the Supreme Court largely gutted the FTC’s capacity to disgorge illegal profits, leaving the agency almost powerless. A general diagnosis is that the Fair Information Privacy Principles (the foundation of legacy data protection regimes on both sides of the Atlantic) have largely failed to achieve their stated goals of aligning the privacy preferences of consumers and companies and increasing data protection. Private self-regulation has not fared any better. That is mainly because these older laws were “toothless” or “paper tigers.”

The GDPR and the CCPA were partially designed to address these shortcomings. Changes in the GDPR, for example, were specifically aimed at bringing data protection closer to antitrust regulation in terms of enforcement, fining capacity, etc. Issuing a definitive judgment on the performance of these laws is complicated for at least two reasons. First, because these are new and complex regulatory regimes, it is possible that enforcement will initially be suboptimal, but will improve as the laws mature. Second, because many data protection markets are so opaque, reliable evidence for empirical studies is hard to obtain.

Still, notwithstanding these limitations, the Appendix contains a comprehensive survey of studies that independently assess compliance with the commands of the GDPR and, to a lesser extent, the CCPA. The available evidence consistently indicates an underwhelming impact of these new regimes. Out of twenty-six

57. Martino Trevisan et al., 4 Years of EU Cookie Law: Results and Lessons Learned, 2019 PROC. ON PRIV. ENHANCING TECHS. 126, 127, 133, 140 (2019) (surveying 35,000 popular EU websites and finding that 49% placed tracking cookies before receiving consent—a violation of the directive).
58. A wide review of FTC enforcement actions by the Government Accountability Office concluded that all but a handful of FTC cases resulted in settlements and recommended the development of a strong regulator with the capacity to regulate the market and impose broad civil penalties. U.S GOV’T ACCOUNTABILITY OFF., GAO-19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY 37 (2019); see also AMG Capital Mgmt., LLC v. Fed. Trade Comm’n, 141 S. Ct. 1341 (2021).
59. Cate, supra note 17, at 344.
61. Sebastian J. Golla, Is Data Protection Law Growing Teeth: The Current Lack of Sanctions in Data Protection Law and Administrative Fines Under the GDPR, 8 J. INTELL. PROP. INFO. TECH. & E-COMMERCE L. 70, 70 (2017); see also Hoofnagle et al., supra note 18, at 93 (stressing how “directive [95/46] was plagued by ineffective sanctions”). Both refer to European data protection laws, but the conclusion can easily be extended to the FTC.
62. Hoofnagle et al., supra note 18, at 67, 92.
independent evaluations, none found that these laws led to meaningful increases in data protection. For example, a survey of privacy protection policies of almost two hundred large firms before and after the GDPR found that while the legislation led to textual changes, "the overall level of compliance [with GDPR provisions] is not high in absolute terms."  

A 2019 review of the EU’s two thousand most-accessed websites found that 92% of those websites tracked users before providing any notice and 85% of users were unable to opt out of being tracked—violating the Regulation. These findings are supported by another study analyzing the five hundred most visited websites in each EU country, which concluded that the amount of user tracking pre and post-GDPR stayed the same, and warned against a false sense of GDPR compliance. Even EU authorities are finding widespread violations, as shown by a survey of thirty-eight large data processors performed by the Irish data protection authority, which found that more than eighteen months after the GDPR had come into effect, 95% presented at least one significant violation of the law. A similar study of 175 websites by the Dutch data protection authority found that the vast majority of those websites assessed did not comply with the law. There are less independent data on CCPA compliance, but the trend is similar. A February 2020 PwC survey of the websites of the six hundred largest companies in the U.S. reported that a majority did not offer portals for users to access their information. A 2021 survey of business-to-consumer companies found that these businesses are receiving on average eleven data-related requests per month for every million California consumer identities they hold, which means that the CCPA was used by 0.001% of Californian consumers. A September 2020 scan of more than eighty-thousand of the world’s most popular websites found that tracking remains ubiquitous around the world, including the U.S., even for highly sensitive websites such as those searching for abortion providers or resources for victims of sexual violence. A follow-up article noted that third-party tracking is as pervasive now as it was ten years ago, but it has only “become creepier and more difficult to stop.”

These conclusions are backed by other evidence. After a detailed analysis of the internal data protection compliance practices of certain companies, Professor Ari Waldman described the GDPR and the CCPA as a “house of cards” that is failing to
deliver its promised protections because formal compliance with privacy law is prioritized over actual substance.\textsuperscript{72} European data protection agencies received more than 275,000 complaints in the first eighteen months after the GDPR came into force, but issued only 785 fines in the same time period.\textsuperscript{73} Data protection agencies are generally underfunded and poorly staffed.\textsuperscript{74} “Nearly every European government underfunds its [data protection agency]” and regulators in all jurisdictions (except Germany) lack tech specialists.\textsuperscript{75} The head of the Irish data protection agency,\textsuperscript{76} Helen Dixon, graded her own agency’s two-year GDPR enforcement performance as an “A for effort” but a “C-plus/B-minus in terms of output.”\textsuperscript{77} The chairman of the German data protection authority, Ulrich Kelber, summarized the situation as: “we have a lack of enforcement.”\textsuperscript{78} The head of the Hamburg data protection authority said that they are “completely critical of the enforcement structure of the GDPR,” and that “[t]he . . . whole system doesn’t work.”\textsuperscript{79} On the other side of the Atlantic, when asked about the enforcement of the CCPA, the California Attorney General stated that the lack of resources would force the agency to look kindly on companies that simply “demonstrate an effort to comply.”\textsuperscript{80} Californians passed the CPRA to fill-in what they identified as substantial gaps in the enforcement structures of the CCPA.

As Professor David Erdos aptly summarized: “with ever increasing digitization, the gap between the [privacy] law on the books and the implementation and enforcement on the ‘virtual’ ground [initially described as very large] is almost certainly increasing.”\textsuperscript{81} Given this somewhat discouraging background, academics and policymakers hoping to improve the performance of data protection laws must ask themselves: (i) are there important gaps in the design of data protection laws that enable companies to ignore their commands, and, if yes, (ii) what legal and institutional changes can help improve the performance of these laws?

Parts II and III below help tackle these difficult problems.

\begin{itemize}
  \item \textsuperscript{72} Waldman, \textit{supra} note 55, at 776, 786, 803.
  \item \textsuperscript{73} \textsc{Eur. Comm’n, Commission Staff Working Document: Communication from the Commission to the European Parliament and Council—Data Protection as a Pillar of Citizens’ Empowerment and the EU’s Approach to the Digital Transition—Two Years of Application of the General Data Protection Regulation 20, 5 (2020)}.
  \item \textsuperscript{74} See \textsc{Ryan \& Toner, supra} note 10, at 3, 6.
  \item \textsuperscript{75} Id.
  \item \textsuperscript{76} The Irish data protection agency is the authority responsible for overseeing Google, Facebook, Apple, Twitter, and other large tech platforms. \textsc{See Satariano, supra} note 4.
  \item \textsuperscript{77} Id.
  \item \textsuperscript{78} Id.
  \item \textsuperscript{79} Vincent Manancourt \& Mark Scott, \textit{Two Years into New EU Privacy Regime, Questions Hang Over Enforcement}, \textsc{POLITICO} (May 25, 2020), \url{https://www.politico.eu/article/europe-data-protection-privacy-gdpr-anniversary/} [https://perma.cc/BQ7C-UZHR].
  \item \textsuperscript{80} Nandita Bose, \textit{California AG Says Privacy Law Enforcement to be Guided by Willingness to Comply}, \textsc{REUTERS} (Dec. 10, 2019), \url{https://www.reuters.com/article/us-usa-privacy-california-idUSKBN1YE2C4} [https://perma.cc/C5AV-MSF5].
  \item \textsuperscript{81} David Erdos, \textit{Acontextual and Ineffective? Reviewing the GDPR Two Years On}, \textsc{Inforrm} (May 5, 2020), \url{https://inforrm.org/2020/05/05/acontextual-and-ineffective-reviewing-the-gdpr-two-years-on-david-erdos/} [https://perma.cc/U7KL-SXK3].
\end{itemize}
II. HOW DESIGN FAILURES UNDERMINE DATA PROTECTION ENFORCEMENT

Online privacy laws such as the GDPR and the CCPA are sophisticated pieces of legislation that rely on different combinations of market forces, tort liability, and public regulation to ensure that companies act in accordance with consumers’ privacy preferences. Yet, a particularly pervasive combination of large structural information asymmetries and market power, which is present in many data markets, undermines all three mechanisms as drivers of legal compliance.

A. Market Forces

1. Markets Can Force Companies to Reflect the Privacy Preferences of Consumers

Markets are the most cost-effective mechanism to ensure that companies reflect the preferences of consumers. Yet, information asymmetries and economic power can prevent markets from delivering such outcomes.

More specifically, markets represent the aggregate of two different types of strategic behavior consumers adopt when faced with a decline in the quality of a given good, service, or organization: exit or voice. Exit is a binary choice that reflects the invisible hand working at its best. Whenever the quality of a good or service goes down, consumers shift to another supplier. Voice is protest, where consumers continue buying from the firm but complain to management that the quality is going down. Exit and voice are not mutually exclusive, but exit is the foundation of consumers’ ability to discipline companies because voice requires at least a threat of exit to work. Exit and voice are powerful. If markets are competitive and consumers are well-informed, a combination of customers switching and complaining will force companies to supply what consumers desire and ensure allocative efficiency. This aggregation of consumer behavior is a cheap, effective, and decentralized mechanism that conveys information to firms and enforces heterodox consumer preferences.

Data protection laws have historically endeavored to harness the power of markets as a mechanism to ensure that companies reflect consumers’ data preferences. As seen above, notice and consent obligations have long been a backbone of data protection laws, even before the passage of modern regimes. Albeit differing in important ways, both the CCPA and the GDPR further strengthened these notice and consent provisions by enabling consumers to access, correct, and delete the information companies hold about them, and to withdraw consent to stop the collection of personal data at any point in time. Both laws also establish (different)

82. See generally ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES 4, 21, 30 (1970).

83. See Keith Dowding, Albert O. Hirschman, Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States, in THE OXFORD HANDBOOK OF CLASSICS IN PUBLIC POLICY AND ADMINISTRATION 257 (Steven J. Balla et al. eds., 2015).

84. Id.; see also Adrian Kuenzler, Direct Consumer Influence—The Missing Strategy to Integrate Data Privacy Preferences into the Market, 39 Y.B. EUR. L. 423, 427-29 (2020) (providing examples for some segments of the digital economy).

85. See Chander et al., supra note 3, at 1750-55 (explaining how both the GDPR and the CCPA contain different provisions to increase transparency over data collection and processing); see
minimum levels of information that must be supplied to users before companies can collect their data, including what type and the extent of personal data that is amassed and how it will be processed. Rights to data portability present in both laws—which generally enable consumers to transfer their personal data to alternative suppliers—are another mechanism to release consumers from a potential lock-in due to a company’s control over their data. Well-informed, unrestrained consumers can then trigger exit and voice as strategic responses to a bad bargain involving their personal data, forcing companies to account for their preferences.

Markets, however, only work if there is meaningful competition: voice without a credible threat of exit is ineffective, as a monopolist can dismiss consumer discontentment and continue to appropriate rents without much economic loss. Markets also fail when large information asymmetries increase consumers’ search costs: The exercise of exit and voice depends on consumers perceiving a decline in quality and acknowledging that alternative suppliers offer better terms. This acquisition of information, however, is costly and often subject to collective action problems. This is particularly true for complex and opaque goods where it is hard to perceive relative quality. These failures are also found in many markets where data is a key input and where deep information asymmetries, opacity, and economic concentration prevent meaningful consumer exit and voice.

2. The Heightened Information Asymmetries in Data Protection

Information asymmetries are common in data protection and negatively impact consumers’ capacity to effectively manage online privacy. Privacy policies run for thousands of words and are generally not designed to optimize consumer understanding. It would take a typical user several weeks to read all of the privacy policies they sign in one year. As a result, these policies—the main technique to

**also** Wolfgang Kerber & Karsten K. Zolna, The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law 15-19 (Sept. 20, 2020) (on file with SSRN.com) (explaining how the GDPR focuses on addressing information and consumer behavior market failures in data markets, but ignores concentration aspects, such as what they call a dual market failure).

86. For example, the GDPR requires that consent should be specific and unambiguous. Whenever the data processing has multiple purposes, a specific consent must be given to each purpose, and that clear imbalance between the data subject and the controller may imply that consent was not freely given. GDPR, supra note 1, recital 43. Heightened consent requirements apply to specific types of sensitive personal data, such as sexual orientation, religion, and others. Id. art. 9. The CCPA just requires general notices. CAL. CIV. CODE § 1798.100(b) (effective until Jan. 1, 2023).

87. See Dowding, supra note 83, at 2-3, 10; see also HIRSCHMAN, supra note 82, at 82, 97.
88. See Dowding, supra note 83, at 10.
89. See Acquisti et al., supra note 48, at 742; see also Acquisti et al., supra note 44, at 448.
90. For example, an investigation by the British Competition and Markets Authority (CMA) concluded that consumers hardly engage with the privacy controls of Google and Facebook because both companies have strong incentives to maximize consumer data collection, and they actively do so by amplifying information asymmetries and abusing choice architectures in ways that harm consumer choice and consumer privacy. See COMPETITION & MKTS. AUTH., ONLINE PLATFORMS AND DIGITAL ADVERTISING 149 (2020).
91. Alecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & POL’Y FOR INFO. SOC’Y 543, 563 (2008) (estimating that it would take the average American 244 hours per year, or forty minutes per day, to read all the online privacy policies they encounter).
inform consumers about the collection and processing of their personal data—are all but ignored.92

Even in an ideal world where companies optimized consumer understanding and consumers read all policies, it would be all but impossible for users to fully comprehend what is done with their data. Data-intensive industries tend to be extremely complex and companies have strong economic incentives to invest in gathering an increasing amount of consumer information.93 Companies use different and obscure means to collect user data, including sign-in and subscription tracking, cookies, web tags, ad tags, pixels, fingerprinting, mobile apps, and cellphone tracking.94 A traditional user is tracked by an average of at least eighteen different companies in their regular web browsing alone,95 and most mobile apps and devices also collect and share a large amount of personal data.96 For example, Google collects, by default, a significant amount of personal data from all Android users. Surveys have found that apps downloaded from the Google Play Store host a median of five different trackers and 88% of Google Play apps share data back with Google (43% with Facebook).97

Even if users could comprehend the complexity of this data collection network, some forms of surveillance cannot be prevented by consumers alone. Data collection mechanisms such as pixels, web bugs, and fingerprints are effectively invisible to the user.98 For example, Google does not allow Android users to become fully anonymized to advertisers.99 In addition, all major mobile carriers in the U.S. were fined for selling real-time user location data without consent.100 Many of these companies, such as Google and Facebook, responded to data protection laws not by diminishing data collection but rather by embedding their third-party code in first-

---

92. The CMA found that between zero and 5% of Google UK users accessed the company’s privacy policies, and 85% of those who did, spent less than ten seconds on the page—these numbers are so low that one must conclude that they were mis-clicks (though the CMA does not conclude that). Similarly, between zero and 5% of Facebook users accessed its privacy control features over a twenty-eight day period. COMPETITION & MKTS. AUTH., supra note 90, at 173-75.

93. See Acquisti et al., supra note 48, at 745; see also Acquisti et al., supra note 44, at 463.


95. Steven Englehardt & Arvind Narayanan, Online Tracking: A 1-million-site Measurement and Analysis 1396 (Oct. 24, 2016) (on file with ACM.org) (surveying one hundred random websites out of the five hundred most accessed websites in sixteen categories and finding an average of eighteen different third parties tracking users per site).


98. Acquisti et al., supra note 44, at 463-64.

99. See AUSTRALIAN COMPETITION & CONSUMER COMM’N, supra note 94, at 130.

100. See Klint Finley, The FCC Fines Wireless Companies for Selling Users’ Location Data, WIRED (Feb. 28, 2020), https://www.wired.com/story/fcc-fines-wireless-companies-selling-users-location-data/ [https://perma.cc/QP2E-EW8D]. Given that cellphones are designed to connect to the network, the only way to not be tracked would be to avoid using the phone’s network capabilities. Even anonymized cellphone data can be easily re-identified. See Yves-Alexandre de Montjoye et al., Unique in the Crowd: The Privacy Bounds of Human Mobility, SCI. REPS., Oct.-Mar. 2013, at 4.
party applications, a practice that users cannot easily block. In theory, “privacy labels” or other similar alternatives can help consumers by conveying information that users can easily process and incorporate in their decision-making. However, privacy labels have failed in other markets in general, and data markets in particular. Privacy labels cannot address the many externalities involved in data processing. Dark patterns employed in design interfaces can also greatly influence consumer decision-making, sometimes without significant awareness or pushback.

Once personal information is collected, it can behave as a public good—a non-rival, non-excludable good that can be easily and cheaply copied and quickly spread through a complex web of companies and data brokers. Once data has been shared, it is hard to purge it from this complex system. In addition, advances in computer power and mining techniques mean that companies find new uses for old data that even the companies themselves did not anticipate at the time of collection.

In such a context, the sophisticated disclosure and consent obligations of the CCPA and the GDPR cannot wash away the fact that mandated disclosure and other provisions aimed at increasing consumer data awareness have failed. As previously addressed, multiple studies have confirmed the high levels of information asymmetries and opacity in data collection and processing. The vast majority of people do not read privacy policies and do not understand data collection and processing, and simplification attempts have not changed that. As of October 2019, only 29% of Americans knew that Facebook owned Instagram and WhatsApp, and only 26% understood that Facebook created user profiles to target

---

101. See COMPETITION & MKTS. AUTH., supra note 90, app. G at G107-08 (explaining this shift and how it enables continued tracking despite decreases in third-party cookies).

102. See Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 U. PA. L. REV. 647, 650-51 (2011) (describing how “[m]andated disclosure is ubiquitous . . . [but] [n]ot only does the empirical evidence show that mandated disclosure regularly fails in practice, but its failure is inevitable”).

103. Omri Ben-Shahar & Adam Chilton, Simplification of Privacy Disclosures: An Experimental Test, 45 J. LEGAL STUD. S41, S41-42 (2016); see also Christine Utz et al., (Un)informed Consent: Studying GDPR Consent Notices in the Field 974 (Oct. 22, 2019) (on file with arXiv.org) (reporting on results showing how consent can be easily manipulated by dark patterns such as the consent notice’s position on the browser and the colors used).


105. See Jamie Luguri & Lior Jacob Strahilevitz, Shining a Light on Dark Patterns, 13 J. LEGAL ANALYSIS 43, 44 (2021).

106. Acquisti et al., supra note 44, at 446 (affirming that shared personal data behaves like a public good, while one of the core tenets of data protection is to be able to exclude access to certain types of data); see generally Englehardt & Narayanan, supra note 95, at 1394-95 (finding more than 81,000 tracking third parties).

107. See Acquisti et al., supra note 44, at 444, 447, 481.

108. Id. at 479 (“[N]umerous empirical studies have highlighted the limitations of transparency mechanisms [to increase data protection].”)

ads. If consumers cannot grasp even the basics of the data collection network, they will not understand that when they use a cellphone app, their real time location data is being sold to a complex network that enables the U.S. Federal Government to enforce immigration laws or track potential terrorist threats, and journalists to track the private lives of public officials (among other obscure uses of personal data).

Uninformed consumers cannot exercise exit or voice, undermining the role of markets as mechanisms to help promote compliance with privacy laws.

3. Market Concentration Further Hinders Exit and Voice

Information asymmetries, however, provide only a partial explanation for why market solutions appear to be failing to meet consumers’ privacy preferences. Another problem is that the economic structure of many data markets pushes them into winner-takes-all or winner-takes-most scenarios, where only one or several leading companies thrive. Indeed, reports from expert panels and antitrust authorities from around the world highlight the role of network effects, large economies of scale and scope (in part due to network effects), low marginal costs, and low distribution costs in inducing concentration in different data markets. Many of these dynamics are connected to the crucial role data plays as an input to products and services of the digital economy.

More importantly, these conclusions are supported by detailed analyses of particular competitive conditions in different relevant markets, including: (i) search engines, (ii) social media, (iii) search advertising, (iv) display advertising, (v) mobile app stores and mobile operating systems, (vi) online marketplaces, and (vii) mobile mapping services.

In addition, concentration is growing in the infrastructure and backbone of the internet. Amazon Web Services commands the internet cloud industry.
Maps API has an estimated 85% global market share.\textsuperscript{122} Google Font API has a 88% market share.\textsuperscript{123} Google Tag Manager, including Google Analytics, covers more than 80% of popular websites, while Facebook covers around 40% of the same websites.\textsuperscript{124} These are all avenues for companies to collect consumer data. Many companies also obtain sensitive data directly from providers. For example, Google has direct access to credit card data;\textsuperscript{125} 61% of mobile apps transfer data to Facebook the moment a consumer opens the app, even if the user does not have a Facebook account;\textsuperscript{126} and approximately 88% of Google Play Store apps transfer data back to Google.\textsuperscript{127} To avoid the collection of personal data due to backbone concentration or business-to-business deals, consumers would have to all but stop using the internet.\textsuperscript{128}

The provisions of the CCPA and the GDPR on data portability are aimed at facilitating consumer exit in markets where data is a key input. However, porting the data of a single consumer at a specific point in time—what is normally allowed by data portability rights—will do little to weaken the significant market power of leading digital platforms and enable consumer exit. Although individual data portability may be coordinated into a larger effort that could have such power, this coordination faces a chicken-and-egg problem. Competitors struggle to obtain the critical mass that would trigger a natural migration, and consumers face a collective action problem to independently organize such migration. In addition, data portability rights usually do not include constant portability of updated and accurate data, a problem for markets that require a constant flow of fresh data.\textsuperscript{129} As such, simple data portability is unlikely to enhance consumers’ exit strategies.

An alternative approach is to establish a broader obligation of data interoperability—that is, the automated and constant transfer of personal data between two service providers (e.g. between Facebook and a smaller social network).\textsuperscript{130} This solution, however, has its own shortcomings. First, in the absence of a clear legal mandate, interoperability faces legal hurdles. For example, U.S. antihacking laws may be used by companies to prevent third parties from accessing

\begin{itemize}
\item \textsuperscript{123} Web Fonts Software Market Share, DATANYZE, https://www.datanyze.com/market-share/web-fonts [https://perma.cc/289Z-58AK] (last visited Dec. 23, 2021). Google Fonts is a free, open-source web fonts software that websites use for formatting. While Google states it does not collect data in exchange for the fonts, the control over the infrastructure allows the company to change the practice anytime. \textit{Id.}
\item \textsuperscript{124} \textit{COMPETITION & MKTS. AUTH., supra} note 90, app. G, at G99-G100.
\item \textsuperscript{126} \textit{AUSTL. COMPETITION & CONSUMER COMM’N, supra} note 94, at 391.
\item \textsuperscript{127} Binns et al., \textit{supra} note 97, at 27.
\item \textsuperscript{128} See \textit{Gunes Acar et al., THE WEB NEVER FORGETS: PERSISTENT TRACKING MECHANISMS IN THE WILD} 674-89 (2014) (surveying the one hundred thousand most popular Alexa websites in 2014 for online tracking techniques that cannot be stopped by users, such as fingerprinting, and finding that even very sophisticated users cannot protect themselves without significant trade-offs in terms of website functionality).
\item \textsuperscript{130} See \textit{Lancieri & Sakowski, supra} note 14, at 155.
\end{itemize}
computer systems and databases. Second, while legally mandated interoperability may enable consumer exit in some markets, the required sharing of personal data can harm personal privacy. Interoperability is complex and costly, and research has shown that large bodies of anonymized personal data can be reidentified. At the same time, the value of databases is their volume, complexity, and time-sensitivity. On the one hand, an interoperability system based on consent faces the same collective action challenges of data portability. On the other hand, a system that relies on differential privacy or other similar privacy preserving protocols to enable the mandatory sharing of personal data will probably be so restricted that it will not effectively promote exit.

Voice only functions if consumers can threaten exit. However, many data markets tend to monopoly, allowing companies to impose unfavorable data collection and processing terms, notwithstanding consumer preferences. Facebook, for instance, has been condemned in both Germany and Italy for such practices.

Data collection and processing is complex, but the following example helps convey how information asymmetries and market concentration might prevent consumers from fully exercising exit and voice in data markets. To help contact tracing programs during the COVID-19 pandemic, the U.K. government asked restaurants to keep a record of the names and cellphone numbers of consumers.

131. Facebook, for example, has previously leveraged federal criminal law to prevent the development of a potential competitor in social network markets called Power Ventures, whose goal was to create an interoperable meta-social network. See Thomas E. Kadri, Essay, Digital Gatekeepers, 99 Tex. L. Rev. 951, 971-74 (2021). The legality of Facebook’s very strict interpretation of federal anti-hacking laws is currently under discussion, in particular after the Supreme Court’s decision in Van Buren v. United States. In that case, the Court adopted a narrower interpretation of when violations of access rights (or when a practice “exceeds authorized access”) lead to a violation of federal laws. However, the Court refused to rule on whether its interpretation extended to violations of private companies’ terms of service (as opposed to public uses, the case in question), leaving a legal limbo. Van Buren v. United States, 141 S. Ct. 1648, 1659 n.8 (2021).

132. See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701, 1716 (2010) (describing how new methods made reidentifying databases much easier); Luc Rocher et al., Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models, 10 Nature Comm’ns 1, 2-3 (2019) (stating that “numerous supposedly anonymous datasets have recently been released and re-identified” and estimating that their model can leverage an incomplete database of 1% of the U.S. population to reidentify almost 90% of the population).

133. See Daniel Kifer et al., Guidelines for Implementing and Auditing Differentially Private Systems 1, 7-8 (May 14, 2020) (on file with arXiv.org) (describing the restricted “privacy budget” that is essential to ensure that personal data remains anonymized in Facebook’s Social Sciences One project). Effective anonymization requires restricting access to data, but this restricted access would not help promote competition.

134. See Acquisti et al., supra note 48, at 456. See generally Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist’s Journey Towards Pervasive Surveillance in Spite of Consumers’ Preference for Privacy, 16 Berkeley Bus. L.J. 39 (2019) (describing how Facebook reflected at least some consumer privacy concerns while social media markets were competitive but stopped doing so once it dominated the market).

Some restaurant staff used this information to harass female customers by sending messages asking them out on dates.\(^{136}\) This was a clear violation of GDPR requirements, such as specific consent for data processing or purpose limitations, and of the obligation to fully inform consumers under the CCPA (had this taken place in California). In theory, consumers could rely on markets as an enforcement mechanism that can punish the violating restaurants—and this is independent from the legal characterization of data privacy as a fundamental right (in the EU) or as a largely consumer right (in the US).\(^{137}\) Consumers could demand that management fire the harasser (voice), or they could go to different restaurants and force the violating restaurant to go out of business (exit). However, data can be easily shared without the consumer’s knowledge. Any restaurant staff can easily copy the consumer’s name and telephone number or even send it to a friend without the consumer knowing. If consumers provided their information to different restaurants, they would not know which establishment to punish unless the wrongdoer revealed themselves. Similarly, if only one restaurant exists in their city, consumers have no exit options. Owners can ignore complaints and force consumers to choose between discounting the violation or avoiding the restaurant altogether.

The complexity of data markets aggravates information asymmetries and market concentration concerns. Consumers share similar data with multiple providers without even knowing that their data is being collected and, ultimately, they may need to decide between sharing personal data or giving-up the use of their smartphones, online search engines, or digital mapping services altogether. Under such circumstances, markets do not work as a mechanism to ensure that companies reflect the privacy preferences of consumers.


\(^{137}\) The strength of markets as an enforcement mechanism is independent from discussions on what types of data processing activities are a violation of the data protection rights of citizens in the EU or of consumers in the US. By characterizing data privacy as a fundamental right, European nations removed from consumers the ability to contract in relation to certain aspects of privacy, increasing the realm of potential violations. For example, purpose limitation is an un-waivable right that companies must respect whenever they are processing personal data, independent of whether they are in direct contact with citizens or not (the consumer cannot “consent” them away). On the other hand, the consumer-driven nature of data protection in the U.S. decreases the helm of potential violations—companies may obtain direct consent to process personal data in a manner that is much broader than what is allowed in the EU and without the need to respect data minimization principles (for example). This distinction, however, should not impact the theoretical effectiveness of markets as an enforcement mechanism. If citizens/consumers consistently switch suppliers to more privacy preserving alternatives, they will effectively increase data privacy notwithstanding its legal characterization as a fundamental right or as a consumer good. For more information on how data privacy violations are characterized between Europe and the U.S., see Joris Van Hoboken, From Collection to Use in Privacy Regulation? A Forward-looking Comparison of European and U.S. Frameworks for Personal Data Processing, in EXPLORING THE BOUNDARIES OF BIG DATA 231, 233-34, 243-46 (1 ed. 2016).
Tort-based statutory causes of action can complement markets by ensuring that companies account for the preferences of consumers without many of the downsides of top-down and command-and-control public regulation.

Tort liability has many virtues. It directly empowers consumers by allowing for decentralized and often low-cost enforcement.\(^{138}\) Damages encourage users to monitor companies and bring violators to court.\(^{139}\) Moreover, when coupled with fee-sharing arrangements and collective redress mechanisms (such as class actions or punitive damages), tort liability can sometimes overcome the problems of information asymmetries or low value claims. Injunctions and damage awards may force powerful companies—including monopolies—to internalize consumer preferences by compelling or making it unprofitable for corporations to violate the law.\(^{140}\)

In theory, consumers can rely on different torts such as intrusion upon seclusion, public disclosure of private facts, or even unjust enrichment to safeguard their privacy. Modern data protection laws, however, go far beyond these general torts and establish specific data rights that can be a concrete foundation for the statutory torts that complement markets in promoting consumers’ preferences.\(^{141}\) The CCPA and the GDPR, for example, grant consumers a different combination of individual rights, such as: (i) the right to data rectification and erasure, (ii) the right to opt-out of data sales (CCPA), (iii) the right to be forgotten (GDPR), (iv) the right to be notified about data breaches, (v) the right to object to the processing of some forms of data, and (vi) the right to withdraw consent.\(^{142}\) These are paired with general commands that consumers should be entitled to receive “full compensation” for harms suffered (GDPR), or to obtain injunctions and claim statutory damages against...

---

139. Id.
140. See Ben-Shahar, *supra* note 104, at 124 (stressing how tort law can help overcome market failures by making some claims actionable and relying on torts as private enforcement).
141. Chander et al., *supra* note 3, at 1752 (explaining how the GDPR and the CCPA share “the core elements of a number of additional individual rights (though they differ in the details)”). There are many differences between the individual rights described in the GDPR and those described in the CCPA. See generally *id.* at 1755-62. While the CCPA grants users a series of rights, it does not pair them with the capacity to directly enforce these rights through private rights of action. CAL. CIV. CODE § 1798.150(c) (effective until Jan. 1, 2023). This Article focuses on how abstract legal rights are enforced on the ground, highlighting the separation between laws outlining a type of concrete harm that could qualify as a statutory tort (such as the right to sue when a company prevents the consumer from accessing their data, and failing to allow them to correct information in the company’s database) and laws that remove independent enforcement powers from the consumer—a strategy that hampers the tort system as an effective enforcement mechanism. This separation is explained by Justice Alito in the majority ruling in *Spokeo*: Congress is well positioned to identify intangible harms that meet minimum Article III requirements . . . . Congress’ role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right.
142. See *supra* Section I.A.
some violations of the law (CCPA). Because of the GDPR, citizens harassed by restaurant staff can go to court to obtain injunctions or collect damages for violations of their data protection rights—a complement to exit and voice.

However, there are downsides to relying on statutory torts as a mechanism to enforce consumer preferences. First, and most importantly, torts suffer from many of the same information asymmetries that plague markets: if goods are so complex and opaque that consumers or their attorneys cannot identify violations or cannot prove that a violation took place, then the tort system will not work as intended. In addition, torts are plagued by agency problems in the definition of the tort, and courts sometimes struggle to establish causation, calculate damages, or address negative externalities that go beyond harm to a single individual. Market power may also undermine torts as firms design more opaque products and leverage their deep pockets to hire the best lawyers and economic consultants, prolong the discovery process, and generally raise the costs of litigation.

These shortcomings are not inevitable, instead they depend on the design of the judicial system and the statutory tort. Yet, an analysis of the GDPR and the CCPA reveals important obstacles that prevent both common law and statutory torts from becoming effective data protection enforcement mechanisms. This is because lawmakers fail to consider how information asymmetries, market power, and other hurdles undermine data-related statutory torts when designing these laws.

2. Information Asymmetries and Market Power Undermine the CCPA

Tort liability has historically been a weak mechanism to safeguard the data protection preferences of consumers in the U.S. Many U.S. courts deny Article III standing or actual recovery in privacy violation or data breach lawsuits for lack of a cognizable harm. Privacy class action lawsuits normally target a couple of statutes that allow statutory damages. These class actions face many problems around conflicts of interest between lawyers and consumers. While the CCPA and CPRA could have addressed these shortcomings, some of the same information asymmetries that plague exit and voice also negatively impact tort enforcement under these Acts.

143. GDPR, supra note 1, arts. 78-79; CAL. CIV. CODE § 1798.150 (effective until Jan. 1, 2023).
144. See Steven Shavell, Liability for Harm Versus Regulation of Safety, 13 J. LEGAL STUD. 357, 363 (1984) (listing barriers to effective compensation through tort liability: dispersed harms, lack of economic incentive to sue, discovering the harm, establishing causality, and market power).
145. Torts may reflect the preferences of only a subset of consumers or even of parties other than consumers. For example, mandatory rules may lead to higher quality and higher price combinations that exclude poorer consumers. See Oren Bar-Gill & Omri Ben-Shahar, Regulatory Techniques in Consumer Protection: A Critique of European Consumer Contract Law, 50 COMMON MKT. L. REV. 109, 113 (2013); Waldman, supra note 55, at 793-98 (describing how legal endogeneity is a problem in data protection).
146. See Ben-Shahar, supra note 104, at 125-26.
147. Daniel J. Solove & Danielle Keats Citron, Risk and Anxiety: A Theory of Data-Breach Harms, 96TEX. L. REV. 737, 739 (2018); see also Ben-Shahar, supra note 104, at 126-28. These refusals are bound to become stricter after TransUnion LLC v. Ramirez. 141 S. Ct. 2190 (2021) (holding that the mere existence of inaccurate information or lack of notice cannot qualify as a concrete harm for purposes of Article III standing, even if affirmed by specific statutes).
An effective private litigation system requires consumers to be aware that violations took place. Although this may be easy in the data security realm (given that data breach notifications provide consumers with clear warnings), this is not the case for rights that limit the collection and processing of personal data.\textsuperscript{149} If information asymmetries, opacity, and externalities prevent consumers from understanding what is being done with their data and trigger exit and voice, they also prevent consumers from litigating these matters.

The American class action system is structured to circumvent this problem. The practice of grouping claims allows for the pooling of resources and increases the sophistication of plaintiffs, enabling plaintiffs to take advantage of the extensive civil discovery process in the U.S. However, the complexity and opacity of data markets and the market power of digital platforms undermine data protection class actions by enabling companies to impose terms of use that minimize their liability, design more complex interfaces that hinder characterization of harm, and generally increase the cost of litigation. Not only must plaintiffs hire experts and conduct lengthy investigations to discover violations, but they do so knowing that the other party has nearly endless resources to fight their claim.

Indeed, with the potential exception of the “do not sell my data” button, most of the CCPA’s consumer data rights remain directly linked to the companies’ terms of use.\textsuperscript{150} This allows companies to draft their terms of use in a way that hinders or blocks tort lawsuits by allowing for widespread data collection and processing or by requiring class waivers or mandatory arbitration (among other methods).\textsuperscript{151} The designed complexity and opacity of data collection and processing means that data harms are neither immediate nor visible,\textsuperscript{152} making it even harder for parties to survive a motion to dismiss, certify a class, or prove the causation necessary to trigger liability. In theory, the CCPA statutory damages could provide courts with guidelines for harm calculations and become an important incentive to encourage sophisticated plaintiffs to file the expensive class action lawsuits that dominate this field. However, the CCPA’s statutory damages are mostly a failed opportunity because: (i) they only apply to data breach litigation and not to core data protection rights like the “do not sell my data” feature; (ii) data breach claims are overseen by the Attorney General of California, who may take over the case or simply block consumers from moving forward;\textsuperscript{153} and (iii) they still require plaintiffs to prove some actual harm before they can claim the minimum damages.\textsuperscript{154}

\textsuperscript{149} See supra Section I.A.
\textsuperscript{150} This is a widespread practice among large U.S. companies. See Imre Stephen Szalai, The Prevalence of Consumer Arbitration Agreements by America’s Top Companies, 52 U.C. DAVIS L. REV. ONLINE 233, 234 (2019) (finding that eighty-one Fortune 100 companies used arbitration agreements in connection with consumer transactions between 2010 and 2018, and seventy-eight included class action waivers); Rotenberg & Jacobs, supra note 148, at 313-17 (discussing how class action waivers or mandated arbitration clauses have undermined data protection enforcement). See generally Waldman, supra note 55 (explaining that companies can evade legal liability by modifying terms of use and relying on other forms of hollow compliance).
\textsuperscript{151} Id.
\textsuperscript{152} Ben-Shahar, supra note 104, at 125.
\textsuperscript{153} CAL. CIV. CODE § 1798.150(b)(2), (3) (effective until Jan. 1, 2023).
\textsuperscript{154} Doe v. Chao, 540 U.S. 614, 627 (2004); see also Davis & Marotta-Wurgler, supra note 63, at 682-83 (discussing how expectation damages and other techniques that discourage inefficient breaches in data
Importantly, the CPRA also continues to prevent consumers from directly litigating the core data protection rights that are outlined in the law.\textsuperscript{155} Ironically, both the CPRA and CCPA aim to safeguard consumers’ online privacy by establishing new data protection rights, but then prevent consumers from directly enforcing most of those rights in court, which precludes the tort system from working as a complementary enforcement mechanism.

Returning to the simple restaurant example from above, if consumers do not know that their name and telephone number are being illegally shared, nor which restaurant shared their data, they will not file a lawsuit. Even if consumers are aware that it was restaurant X that shared their information, the small value of potential claims may prevent them from litigating altogether. Courts can dismiss the lawsuit or refuse to provide damages by stating that simply receiving a text message is not a cognizable harm. The restaurant may also prevent the lawsuit by requiring that before consumers receive drinks, they tick an “I agree” box (likely on page thirty) stating that they consent to their name and telephone number being used for any purpose the restaurant sees fit, and that they waive their rights to a class action and agree to private arbitration to resolve disputes. A wealthy restaurant can further discourage lawsuits by hiring the best lawyers and economic experts and by prolonging discovery and appeals. Finally, consumers in a one-restaurant town may not file claims because they are fearful that the aggravated restaurant owner will refuse their patronage in the future.

The restaurant is a stylized example. Most data collection and processing takes place in a more complex and opaquer world filled with intermediaries. In real life, the consumer would not receive a text message from the restaurant. Instead, the consumer would receive it from a call center that bought their information from a marketing agency that, in turn, bought their information from the restaurant. Nonetheless, this simple illustration showcases the many limitations of data protection torts. Indeed, even after the CCPA came into force, high-profile data protection class action lawsuits filed in California did not rely on the Act, but rather relied on other legislation aimed at protecting the safety of private communications, such as the Federal Wiretap Act or the California Invasion of Privacy Act.\textsuperscript{156}

3. Information Asymmetries and Market Power Undermine the GDPR

The GDPR faces different but equally important challenges. Data related tort lawsuits have historically faced large problems in the EU. For example, although Directive 95/46 (the pre-GDPR data protection legislation) created a range of specific data protection rights, issues related to standing, causation, and damages privacy do not accomplish their goals if breaches of data contracts are difficult to detect, prove, or ascertain. See generally Solove & Hartzog, supra note 31 (discussing legal changes that would be necessary to increase private litigation of data breach harms).

\textsuperscript{155} Section 1798.150 on direct consumer lawsuits continues to apply solely to data security violations, while section 1798.155 only allows for administrative enforcement of other provisions. See CAL. CIV. CODE §§ 1798.150, 1798.155 (effective Jan. 1, 2023).

prevented consumers from obtaining effective enforcement of those rights.\textsuperscript{157} Although the GDPR significantly improved the old status-quo,\textsuperscript{158} it also missed opportunities to spur a robust personal data-related tort litigation system.

First, the concerns about information asymmetries and limited consumer awareness that plague data-related torts may be even more pressing under the GDPR because European jurisdictions host fewer sophisticated intermediaries, such as the data privacy NGOs and class-action plaintiffs that exist in the U.S.\textsuperscript{159} Further, European jurisdictions normally lack extensive civil discovery. The GDPR enables not-for-profit bodies, organizations, or associations specifically created for this purpose to represent consumers,\textsuperscript{160} and this, together with broader notions of what is characterized as harm, has been deemed as a way to enable civil litigants to overcome standing challenges in litigation.\textsuperscript{161} Yet, it is ultimately up to member states to determine specific standing rules. The GDPR also leaves some discretion in terms of court selection.\textsuperscript{162}

Details around who has the power to sue, the resources of the organizations involved, which courts have jurisdiction, and which laws are applicable are key for an effective private litigation system. There is vast scholarship in the U.S. about strategic litigation and claim preclusion in class action lawsuits.\textsuperscript{163} These strategies are known to undermine enforcement of data protection rights.\textsuperscript{164} In the EU, consumers have stronger protections against the strategic use of jurisdiction, arbitration, and class action waivers.\textsuperscript{165} However, until the system is fully in place—including the passage and effective implementation of the much discussed EU Collective Redress Directive—the risks of abuse remain.

Another potential drawback is in the calculation of damages. The GDPR establishes that persons should be compensated for “material and non-material

---

\textsuperscript{157} Hoofnagle et al., \textit{supra} note 18, at 93-94 (describing how the former data protection directive had a gap between legal principles and their practical enforcement, and how the GDPR’s main innovation is making enforcement more effective).

\textsuperscript{158} \textit{Id.} at 94.

\textsuperscript{159} Some European intermediaries do exist, such as the NOYB (noyb.eu), an organization founded by privacy activist Max Schrems, and the La Quadrature du Net (laquadrature.net), founded by French activists. However, these organizations have limited funding. \textit{See discussion infra Section III.A.}

\textsuperscript{160} GDPR, \textit{supra} note 1, art. 80, recital 142.


\textsuperscript{162} \textit{See} GDPR, \textit{supra} note 1, art. 79 (establishing that a lawsuit may be filed in the courts of the member state where the company is established or where the consumer resides); GDPR, \textit{supra} note 1, art. 81, recital 144 (establishing that when courts identify multiple proceedings based on a similar fact pattern, parties may request that their cases be consolidated by the court where the first complaint was filed).

\textsuperscript{163} Tobias Barrington Wolff, \textit{Preclusion in Class Action Litigation}, 105 COLUM. L. REV. 717, 746 (2005) (discussing conflicts of interest with plaintiff’s counsel in rapidly securing settlements that preclude the class in exchange for generous fees).

\textsuperscript{164} Rotenberg & Jacobs, \textit{supra} note 148, at 316 (providing examples of this problem).

damages” arising from privacy violations. The problem with this is that the case law of the European Court of Justice (ECJ) in this area is sparse. Again, information asymmetries associated with the complexity and opacity of data protection make it harder for consumers to prove standing, demonstrate causation, or calculate damages, thus undermining the tort system. Some scholars have stressed how private litigation under the GDPR may face at least three important hurdles: (i) identifying who is the controller of the information, (ii) demonstrating the performance of an illegal act by the controller, and (iii) demonstrating causality between the processing of the personal data and damages to the individual involved.

Economic power of companies is another barrier. For example, a previous study on the lack of private litigation under Directive 95/46 indicated that consumers were unaware of most violations, but also that they feared negative consequences from the large companies they relied on if they filed complaints. If consumers cannot credibly threaten to file complaints, tort liability will not force companies to comply with consumer preferences. Data privacy litigation is also bound to be expensive, as lawsuits might involve significant market monitoring, technical preparation, and discovery to ascertain when the opaque data practices of companies are illegal. Unless national laws or European courts award meaningful material and non-material damages for data protection violations, private litigation may not be worth the cost. However, the GDPR does not require minimum statutory damages, punitive damages, or other forms of increased compensation that can encourage sophisticated intermediaries to start costly investigations and file lawsuits. Accordingly, it will be up to member states to establish the value of potential damages.

Ultimately, there is a reasonable risk that the GDPR private litigation system is structured similarly to the European antitrust private litigation system, where the bulk of lawsuits take place only after the government has found undertakings to be in violation of antitrust laws. Moreover, the EU Damages Directive for

166. GDPR, supra note 1, art. 82. Recital 146 complements Article 82 by establishing that “[t]he concept of damage should be broadly interpreted in the light of the case-law of the European Court of Justice in a manner which fully reflects the objectives of this Regulation.”
167. Johanna Chamberlain & Jane Reichel, The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation, 89 MISS. L.J. 667, 679-80 (2020) (stressing how the ECJ has not decided any case on the application of Article 82 and that it will be up to each member state to ensure that the broad principle is indeed effective).
169. Golla, supra note 61, at 73.
170. See Nowag & Tarkkila, supra note 165, at 471-72 (stressing how the small value of awards is a disincentive for individual consumers to pursue antitrust lawsuits).
171. Id. at 457 (asserting that follow-on antitrust claims are likely the most common in the EU). As discussed below, antitrust regulation systems also face significant hurdles in terms of information asymmetries and the potential small value of claims.
competition law violations has so far failed to spur consumer-driven private litigation.\textsuperscript{172} These are bad omens for the success of GDPR private litigation, as not only is antitrust a more mature enforcement system but the consumer-to-business nature of data protection laws limits company-driven litigation. Whenever European online privacy NGOs discover violations, they usually file complaints before EU regulators rather than suing companies in court—showcasing the weakness of the tort system. Indeed, when asked why NOYB would not file complaints directly in court, Max Schrems, the NGO’s head and a renowned privacy activist, stressed that: (i) NGOs do not have the necessary evidence, and European courts lack the investigative powers, that would allow them to file a strong case; (ii) going to court is extremely expensive in most countries, and NGOs lack resources; (iii) loser-pay principles may mean that a loss kills the organization; and (iv) regulators are paid to enforce laws, so they should perform their institutional role.\textsuperscript{173}

Tort liability as a mechanism to promote legal compliance will certainly be weaker in a system where private parties are subordinate to regulators than in one that relies on a mix of public and private litigation. That is because in this subsidiary system the enforcement of legal rights is no longer decentralized and directly in the hands of consumers, rather it is in the hands of government regulators. As a result, tort liability is at risk of becoming merely a way to increase the deterrence value of public fines, rather than the independent enforcement mechanism it initially was. Moreover, as tort liability gets closer to regulatory enforcement, it incorporates the virtues and shortcomings of public regulation.

C. Regulatory Enforcement

1. Command-and-Control Regulation as a Third Enforcement Mechanism

The government’s use of coercive or fining powers to enforce command-and-control regulations is a third and important mechanism to ensure that markets reflect consumer preferences.\textsuperscript{174} Regulatory enforcement represents a decision by governments to remove consumers from the direct determination of quality and pricing in markets, replacing them with commands that impose specific obligations, minimum levels of quality, maximum prices, and other substitutes. In essence, regulatory enforcement is the combination of three components: (i) setting standards of behavior, (ii) monitoring compliance with those standards, and (iii) enforcing the standards against those in non-compliance.\textsuperscript{175} All three are non-trivial, so

\textsuperscript{172} Id. 471-72 (discussing what prevents consumers from directly litigating antitrust violations).

\textsuperscript{173} Stanford Univ., Max Schrems on Transatlantic Data Sharing, Digital Rights and Global Policy, ZOOM, https://stanford.zoom.us/rec/play/u0ZTx-ajBlfguQ6HvRNNrV8ioRb0CkIILktaqmE-kgZDwzwkbsOdpakCuE2iwUJbXghkh2MFS45BB.8v693c2ZwpR7mvR9?continueMode=true&xzmrtaid=9ga19Vj_RtSJNcX2pziG-w.1629137625021.6ccbaac8b42692120359f858ceb2b98f&xzmrtaid=942 [https://perma.cc/7SUZ-HRAY] (last visited Dec. 23, 2021); see Nicholas Vinocur, “We Have a Huge Problem”: European Regulator Despairs Over Lack of Enforcement, POLITICO (Dec. 27, 2019), https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/ [https://perma.cc/H2P3-EYF7] (describing how EU privacy advocates have been filing complaints before regulators, not courts).

\textsuperscript{174} See Kuenzler, supra note 84, at 440-41; Shavell, supra note 144, at 373-74.

\textsuperscript{175} Cane, supra note 138, at 312-13.
governments create bureaucracies dedicated to fulfilling these tasks. Regulators issue rules, conduct investigations, order companies to change behavior, and impose fines to force even the largest businesses to comply with legal and regulatory commands.\textsuperscript{176}

Online privacy laws have long relied on regulators as complements to markets and tort liability to ensure that companies reflect consumer preferences.\textsuperscript{177} Recent statutory and regulatory changes have further strengthened public enforcement. For example, both the GDPR and the CCPA require public authorities to define the content of many data protection rights and effectively enforce those rights.\textsuperscript{178} The newly passed CPRA brings California closer to the EU with the creation of the California Privacy Protection Agency—an independent public bureaucracy responsible for enforcing the CCPA starting in January 2023.\textsuperscript{179} Both EU data protection agencies and their Californian counterpart have the power to impose billions of dollars in fines for non-compliance, and to order companies to change their behavior.\textsuperscript{180}

The option for public regulation, however, leads to important changes that can negatively impact enforcement dynamics. Two are noteworthy. First, the enforcement system now faces two agency problems. Not only do consumers lose their power to establish the content of regulations, as in torts, but they also lose control over when to enforce violations because a governmental employee has discretion to decide when to act. This opens new avenues for regulatory capture, or conflicts of interest between governments (agents) and consumer (principals). Second, the centralization of monitoring and enforcement increases administrative costs and creates the risk that the system may become under-resourced because the government may refuse to fund the costly and complex bureaucracies necessary to properly enforce the regulations.

These two problems are typical of regulatory regimes and can be mitigated through clever institutional design. However, the large information asymmetries and market power that characterize many data markets significantly exacerbates these issues. Indeed, the regulatory systems created through the GDPR and the CCPA lack different and important institutional solutions that could help alleviate these concerns.

2. The Risks of Regulatory Capture in Data Protection

George Stigler’s Nobel Prize winning insight was that the preferences of regulators and consumers may misalign, leading to governmental action that may

\textsuperscript{176} Id. at 317 (describing command-and-control regulations, monetary fines, and orders as key enforcement mechanisms).

\textsuperscript{177} Directive 95/46 required EU member states to establish independent data protection authorities and the FTC has concluded hundreds of settlements with companies for legal violations. See Solove & Hartzog, supra note 31, at 610-14 (analyzing 170 FTC privacy complaints, a number that has only increased since the article was published in 2013).

\textsuperscript{178} See generally Chander et al., supra note 3, at 1759-61 (comparing the role of regulators in the GDPR and CCPA).

\textsuperscript{179} See CAL. CIV. CODE § 1798.199.10 (effective Jan. 1, 2023) (establishing the California Privacy Protection Agency).

\textsuperscript{180} See supra Section I.A.
protect companies while harming consumers. For Stigler, one of the main drivers of regulation is the demand by politically powerful private interest groups who are trying to appropriate economic rents. Effective governmental capture, however, is not easy, not least because it requires coordination among industry members who have private incentives to defect or free ride. The scholarship on regulatory capture has evolved significantly since Stigler wrote his groundbreaking piece. Although many important gaps still remain, we now better understand how agents must expend political capital to influence regulation, relying on multiple mechanisms such as cash payments, revolving doors, shaping of the public discourse through control over the media and academia, the ability to mobilize stakeholders, and control over the human capital required by regulators. Most capture does not take place through direct payments to corrupt bureaucrats. Rather, it relies on a long process of persuasion, in which industry players benefit from information asymmetries and constant interaction, pay consultants and academics, and strategically use revolving doors to convince the authorities that some specific form of regulation that protects the company is actually in the public interest.

Some have argued that certain key market characteristics encourage private capture: (i) the concentration within the industry and the alignment of interests between players, which helps overcome collective action problems; (ii) the opacity and information asymmetries between the industry and regulators; (iii) the level of dispersal of the group paying the rent; (iv) the opacity of the rent payment; and (v) the salience of the topic for the general public. Importantly, this literature indicates that capture is possible, but not that it always happens. The risk increases

---

182. Posner, supra note 181, at 346; Stigler, supra note 181, at 7, 12.
186. *Towards a Political Theory of the Firm*, supra note 184, at 116-19; Carrigan & Coglianese, supra note 183, at 3-6 (describing why firms may have some advantages that enable them to effectively capture public policies and what political processes may facilitate and hinder them).
187. Stigler, supra note 181, at 10; Carrigan & Coglianese, supra note 183, at 7. One can understand the likelihood of a given policy being captured (or the cost of a firm exercising political power against a given community) as a function of: (i) how much the capture damages the community (the more damages,
as the specific industry aligns with the characteristics described above. Political influence is always a matter of degree, and different regulations may well reflect different combinations of public and private interests.

\[ \text{a. Information Asymmetries and Market Power Increase the Risks of Capture in Data Protection} \]

The large information asymmetries and market power found in data markets increases the risk of private capture of these new public enforcement systems. As discussed above, many key data markets are concentrated around a handful of players who usually share preferences in favor of extensive data collection.\(^{188}\) In addition, rent payments in online privacy are both obscure and distributed. This is because data collection is complex, often occurs in the background of regular products and services and has marginal replication and distribution costs. Accordingly, consumers—a heterogeneous and disorganized group—are usually unaware that they are giving up personal data. Finally, understanding the role of data in these industries also requires a particular set of technical skills that are in high demand. Governments, therefore, compete for talent with a profitable, high-paying industry, risking revolving doors undermining enforcement and regulatory agencies lacking the technical personnel to design an effective data protection regime.\(^{189}\) The latter has already been documented in the EU.\(^{190}\)

The same characteristics also increase the risk of public regulatory capture. Governments and citizens have some conflicting priorities in terms of data protection when criminal prosecution, national security, and industrial policy are involved. The surveillance apparatuses of intelligence agencies rely on the processing of personal data (e.g., communications, locations, and bank transfers) so that limitations on data

---

\(^{188}\) See supra Section II.A.3. The potential exception is Apple. However, even Apple has been criticized for recurrently putting profits above privacy, such as when the company accepted billions of dollars from Google to secure the default search engine position on Safari—in that situation, it ignored privacy-friendly alternatives such as DuckDuckGo because Google was willing to pay more to be the default. Another example is its willingness to share personal data with authoritarian governments as a condition of operation in countries such as China and Russia when other tech companies refuse to do so. Apple is also being sued or has been condemned for GDPR violations. Ultimately, Apple may simply not have enough incentive to advocate for strong industry-wide data protection standards because that would weaken its promotion of privacy as a commercial strategy. See Ian Bogost, Apple’s Empty Grandstanding About Privacy, THE ATLANTIC (Jan. 31, 2019), https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/ [https://perma.cc/43SB-5W5F]; Jack Nicas et al., Censorship, Surveillance and Profits: A Hard Bargain for Apple in China, N.Y. TIMES (May 17, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html [https://perma.cc/X49A-7GZ5]; Natasha Lomas, Apple’s IDFA Gets Targeted in Strategic EU Privacy Complaints, TECHCRUNCH (Nov. 16, 2020), https://social.techcrunch.com/2020/11/16/apples-idfa-gets-targeted-in-strategic-eu-privacy-complaints/ [https://perma.cc/2LPM-3ZEK].

\(^{189}\) RYAN & TONER, supra note 10, at 3, 6 (finding that almost all EU data protection agencies lack data scientists).

\(^{190}\) Id.
collection also mean limitations on the agencies’ success. Both the CCPA and the GDPR explicitly exempt criminal enforcement and national security from their application and law enforcement authorities are attacking end-to-end encryption in social networks—undermining one of the most important online privacy conquests of the past decade. Three out of five commissioners of the newly created Brazilian data protection agency are members of the Brazilian armed forces. As perhaps the best example, the governments of some EU countries have challenged a decision by the ECJ imposing limits on data retention, alleging, inter alia, that collecting and withholding data is essential for national security and outside the scope of EU laws.

These conflicting interests in data protection are not solely restricted to technical matters, such as encryption, but include the broader organization of the industry. It is reasonable to assume that governments prefer fulfilling their data access needs by tapping just a handful of companies with large, comprehensive databases, rather than having to access many smaller providers. Large, centralized databases are more reliable, which helps increase the secrecy of the operations (only one backdoor is needed), and are better for future Artificial Intelligence applications. Governments also likely prefer to concentrate compliance in a single company established in their jurisdiction rather than in multiple companies based abroad.

The growing economic importance of digital markets pushes for an equally expanded interconnection between industrial and data policy, which is exacerbated by the market power of some large digital companies. The more personal and non-

192. CAL. CIV. CODE § 1798.145 (effective until Jan. 1, 2023); GDPR, supra note 1, art. 23.
196. DAKOTA FOSTER & ZACHARY ARNOLD, ANTITRUST AND ARTIFICIAL INTELLIGENCE: HOW BREAKING UP BIG TECH COULD AFFECT THE PENTAGON’S ACCESS TO AI 13, 15, 20 (2020) (arguing that (i) “data is a core ingredient” in the development of new AI tools that can bolster national security, (ii) data protection requirements, like “siloeled” data, can hinder AI innovation, and (iii) the potential break-up of large tech companies could negatively impact national security by reducing network effects and deconcentrating data sources necessary for AI developments). The essence of the U.S. PRISM program (the one denounced by Edward Snowden as a surveillance system that violated civil liberties) was that the National Security Agency had direct access to the databases of certain trusted and key internet companies, enabling the surveillance to take place unnoticed.
197. China, for example, explicitly combines data and industrial policy to promote their national companies, particularly in AI. Hung Tran, Industrial Policy War - Capitalism with Chinese Characteristics, FIN. TIMES (Sept. 21, 2019), https://www.ft.com/content/79b242e2-3d21-3bce-8880-59e6f34e96c4 [https://perma.cc/T5UW-RK3Q]. In the U.S., whenever companies like Facebook are
personal data become key inputs for technological development in the digital era, the more governments concerned with the promotion of national champions may want to increase rather than restrict access to data.198 This means that governments may have important economic incentives to undermine data protection enforcement by inducing market concentration, data concentration, or more widespread data collection and processing.

Finally, effective data protection may increase the market power of dominant digital platforms, worsening these dynamics. This is because of increased compliance costs and legislation that restricts access to data and concentrates the remaining data in large providers.199 While access to a large updated database is key in many digital markets, data protection laws have a general goal of limiting data collection and processing, which disproportionately impacts smaller companies with limited direct interaction with consumers.200 It is too early to pass a definitive judgment, but different studies have found that one side effect of the enactment of the GDPR has been increased data and market concentration.201 This data protection and concentration dynamic allows industry players to leverage data protection regulations in order to protect their dominant position by complying with the law.202
For example, Google, Facebook, and Apple announced a series of changes to promote or comply with data protection laws that strengthened their grip on data vis-à-vis potential competitors. Facebook has also previously leveraged access to its databases to prevent the development of competitors, potentially in violation of antitrust laws. Many companies are in a data race, and while these changes are welcome from an online privacy perspective, they further increase data-related barriers to entry. Stronger, more dominant companies are better resourced to capture regulators and can more convincingly argue that they are essential to national economies.

Capture is difficult to identify, but there is growing anecdotal evidence suggesting that it has already taken place in online privacy. Professor Waldman has aptly described how privacy laws in the U.S. and the EU are undergoing a process of legal endogeneity that is highly deferential to industry practice; regulated agents define what the law means rather than the law constraining what private entities can do. This prevents privacy laws from achieving their substantive goals. In the U.S., there have been multiple reports, including by FTC commissioners themselves, that the FTC, has been unwilling to, or incapable of, standing up to large tech companies. In the EU, the ECJ has been a leading institution in helping to promote data protection rights by striking down what it considered to be faulty regulations.
that did not adequately promote data protection.\textsuperscript{209} The ECJ also previously determined that EU countries have not safeguarded the independence of their data protection authorities.\textsuperscript{210} Other studies have shown that data authorities are reluctant to impose sanctions for violations, instead preferring to rely on cooperation.\textsuperscript{211} More recently, European governments have been accused of using COVID-19 to suspend GDPR rights\textsuperscript{212} and of using the GDPR itself as a way to diminish public accountability.\textsuperscript{213} There are many complaints from European activists and other EU regulators that the Irish data protection authority (the leading GDPR enforcer) is dragging its feet on enforcement because of how important digital markets are to the Irish economy.\textsuperscript{214} Facebook famously settled in Ireland partially because of its favorable regulatory reputation.\textsuperscript{215} NOYB published a scathing letter accusing the Irish regulator of being “structurally biased,” and cooperating with Facebook to purposefully delay the enforcement of the GDPR in order to attract foreign investment,\textsuperscript{216} and it has formally accused the agency of corruption for its alleged attempt to illegally safeguard Facebook’s corporate interests over its statutory

\textsuperscript{209} For instance, the decision invalidating the EU-U.S. Safe Harbor was grounded in the fact that regulators did not comply with express legal obligations to monitor transatlantic data transfers, allowing the industry to freely collect and transfer personal data. The subsequent invalidation of Privacy Shield also affirmed that the European Commission failed to properly assess whether the data of European citizens would receive adequate protection if transferred to the U.S. Case C-362/14, Maximilian Schrems v. Data Prot. Comm’r (Schrems I), ECLI:EU:C:2015:650, ¶¶ 88-90 (Oct. 6, 2015); Case C-311/18, Data Prot. Comm’r v Facebook Ire. Ltd. (Schrems II), ECLI:EU:C:2020:559, ¶¶ 184-185, 191 (July 16, 2020).


\textsuperscript{211} See Golla, supra note 61, at 73.


\textsuperscript{213} European countries such as Hungary, Poland, Romania, and Slovakia have apparently attempted to use the GDPR to harass journalists and NGOs who have revealed government wrongdoings. See \textit{Estelle Massé, ACCESS NOW, TWO YEARS UNDER THE GDPR: AN IMPLEMENTATION PROGRESS REPORT 17-19} (2020).


Indeed, the lack of appropriate resources and initiative by Irish regulators has been denounced by other European data privacy regulators, leading commentators to claim that Ireland is a “safe haven for tech giants.”

b. The Systems Lack Appropriate Counterweights

Although capture is a constant threat to regulatory systems, the discussion above showcases how a somewhat exceptional combination of market concentration, complexity, obscurity, consumer dispersion, and the strategic nature of data exacerbates the possibility of capture in online privacy. Yet, the regulatory systems put in place by the GDPR and the CCPA lack institutional counterweights—such as civil oversight, civil lawsuits for failure to act, and competition in enforcement—that can help fend off undue influences.

Beginning with civil oversight, as Louis Brandeis rightly stated, “[s]unlight is said to be the best of disinfectants” when it comes to fighting powerful vested interests. Data protection is certainly in the spotlight in Europe and, to a lesser extent, in the U.S. It is possible then, to design regulatory systems that leverage this public awareness to offset the risk of capture. However, data protection agencies in the EU and the U.S. tend to be extremely opaque. The FTC and the California Office of the Attorney General provide very little public information about ongoing investigations. They also hardly supply information on the reasons behind the opening or closing of cases—most of the information relates to cases that were filed or settled. Similarly, many important EU authorities rely on annual reports, press releases or brief statements to announce the opening or closing of investigations. In particular, stakeholders have complained about the obscurity of the Irish and Luxembourg data authorities, which are among the most powerful in the EU. The Irish Data Protection Commission does not host even basic transparency mechanisms such as a page summarizing the status of ongoing cases or a public agenda for officials. As previously discussed, European privacy NGOs accused the agency of holding numerous confidential meetings with defendants to advise them on how to comply with the law, while simultaneously withholding most of that information

218. See generally Kobie, supra note 214.
219. MASSÉ, supra note 213, at 14.
220. LOUIS D. BRANDEIS, OTHER PEOPLE’S MONEY AND HOW THE BANKERS USE IT ch. 5 (1914) (ebook).
221. For example, the FTC’s annual report on privacy and security provides very little data on ongoing investigations, cases closed but not pursued, and other relevant data. See FED. TRADE COMM’N, PRIVACY AND SECURITY UPDATE: 2019 (2019).
222. The Irish Data Protection Commission has data on open and closed investigations and some case studies but no comprehensible way to access specific information, its reasoning, etc. See generally IRISH DATA PROT. COMM’N, ANNUAL REPORT: 2019 (2020).
223. Vincour, supra note 173.
from complainants and European regulators.\footnote{Schrems, supra note 216, at 3, 8-9.} This lack of transparency impedes effective civil oversight of the government’s enforcement of privacy laws.

Lawsuits for failure to act are another important mechanism in the fight against private capture.\footnote{See generally Case C-362/14, Schrems I, ECLI:EU:C:2015:650, (Oct. 6, 2015); Case C-311/18, Schrems II, ECLI:EU:C:2020:559, (July 16, 2020).} In this area, the GDPR is more advanced than the CCPA and CPRA. The GDPR requires that authorities investigate complaints filed by data subjects, inform them of the status of their complaints after three months of the filing, and allow private parties to file complaints against regulators in case of breach of this obligation.\footnote{GDPR, supra note 1, arts. 57(1)(f), 78(2).} The CCPA and CPRA, on the other hand, have no comparable provisions. Even the GDPR, however, has important flaws connected with the lack of agency transparency and the wide discretion regulators retain in deciding how to handle complaints (complemented by minimum judicial oversight),\footnote{David Erdos, Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe? 6 (Univ. of Cambridge, Working Paper No. 14/20, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521372 [https://perma.cc/FGW3-J6XT].} allowing agencies to potentially game provisions and delay cases indefinitely.\footnote{Authorities can simply provide an update that a case is ongoing, and then delay it indefinitely. This was the issue in the UK when the First-Tier Tribunal decided at least six cases claiming that users only have a right to object against well-defined procedural violations, not the final outcomes. See id. at 8.}

Finally, regulatory systems must always walk a fine line between: (i) relying on a single, authoritative regulator with the appropriate powers and resources to challenge dominant businesses; and (ii) relying on multiple regulatory agencies with overlapping authorities that multiply the number of agents a party must influence to determine the outcome of a policy, which hinders capture. The GDPR and the CCPA and CPRA adopt different strategies. The California law allocates all enforcement of non-data breach violations to the California State Attorney General (or, later, the California Privacy Protection Agency).\footnote{CAL. CIV. CODE § 1798.155 (effective until Jan. 1, 2023).} The GDPR, on the other hand, is enforced by multiple national data protection authorities and allows for “joint investigations” between these agencies to solve disputes.\footnote{See supra note 36 and accompanying text (on the CCPA); GDPR, supra note 1, arts. 60-62.} Although the European dispersion of enforcement power may be a welcome mechanism to increase accountability, the GDPR’s creation of a one-stop-shop system reliant on a “lead supervisory authority,”\footnote{GDPR, supra note 1, art. 56(1).} combined with a convoluted system of joint investigations,\footnote{In GDPR joint investigations, a lead authority can either invite other agencies to a joint investigation or non-lead authorities may request that the European Data Protection Board (EDPB) include them in an investigation. GDPR, supra note 1, art. 62(2). If a conflict between the authorities takes place, the decision by the lead authority prevails, unless two-thirds of the twenty-nine members of the EDPB vote otherwise. However, even if the EDPB overrules it, the initial lead authority will still adopt the final decision based on the outcome of the vote. GDPR, supra note 1, art. 65(2).} effectively concentrates key EU data protection enforcement in just two regulators located in Ireland and Luxembourg (countries that are particularly prone to regulatory capture as they disproportionately benefit from the growth of the digital economy).
This is a serious institutional design flaw that all but nullifies the benefits of the multiple-enforcer system. Early data indicates that this cooperation mechanism renders multi-party investigations ineffective and has led to widespread denouncement of Irish authorities as structurally biased against GDPR enforcement.

3. Data Authorities are Under a Heightened Risk of Being Chronically Underfunded

A second key shortcoming of these systems, which are over-reliant on public enforcement, is the potential lack of resources. While this risk is inherent to all governmental regulations, data protection’s distinctive combination of large information asymmetries, market power, and broad applicability place data authorities under a heightened risk of being chronically underfunded.

The GDPR was partially designed to bring data protection closer to antitrust in terms of enforcement resources, fining capacity, and other regulatory tools. Antitrust and data protection policies share significant concerns around information asymmetries because both competition and online privacy violations are mostly hidden from the public view. Unlike antitrust, however, data protection laws are not (mostly) targeted at a small subset of corporations that possess market power. Rather, they establish a range of complex rights and obligations that apply across the economy to small and large businesses, non-profit organizations, and even individuals. Small, unknown companies can collect and process a significant amount of sensitive personal data. Cambridge Analytica is just one example.

234. See generally Erdos, supra note 228, at 3; MASSÉ, supra note 213, at 13. Both Ireland and Luxembourg are particularly prone to regulatory capture because they disproportionately benefit from the growth of the digital economy. For example, Ireland’s fast-growing digital sector is responsible for 13% of national GDP, 26% of exports, and over 10% of all employment. IRISH BUS. & EMP. CONFEDERATION, BREXIT AND THE IRISH TECHNOLOGY SECTOR 13-17 (2019); see also Lillington, supra note 215, at 4 (noting that Facebook’s Deputy Chief Privacy Officer famously stated that Ireland’s “high standard” regulatory environment is a key reason why the company is based there).


236. Shavell, supra note 144, at 364 (identifying high administrative costs as a key hurdle to the effectiveness of public regulation).

237. Hoofnagle et al., supra note 18, at 67, 92.

238. In antitrust policy, many violations take place when companies secretly collude to raise prices, one dominant company redesigns a specific product, one dominant company contracts to exclude a competitor, or companies in specific sectors merge.

239. See GDPR, supra note 1, art. 4(7); Inge Graef & Sean Van Berlo, Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility, 12 EUR. J. RISK REGUL. 691-92 (2020) (stressing how uniform applicability risks underenforcement in data protection and proposing that regulators privilege actions against large firms).

the digital economy grows, the jurisdiction of data protection authorities will expand, risking that these agents become regulators of a “law of everything.” For example, the FTC pursued a cellphone flashlight app for online privacy violations, the Austrian data protection authority fined a kebab shop for installing a security camera that also covered the public street, and the Spanish authority issued a warning to a secondary school student who recorded and posted a video of another minor on Instagram.

Data collection’s ubiquitous, opaque, complex, and multi-player nature significantly decreases the likelihood that these violations will be exposed. In addition, data protection regulatory regimes lack institutional design solutions that can help diminish information asymmetries and the cost of detecting violations. For example, antitrust regimes acknowledged that obscurity and complexity hindered enforcement, leading jurisdictions around the world to reform their competition laws to incorporate leniency regimes and mandatory merger notifications as a way to force or encourage private parties to supply regulators with hard-to-access information. Extensive discovery rights and treble damages further encourage private parties to oversee markets and bring violators to court, increasing the overall resources dedicated to the discovery of illegal behavior. The CCPA, CPRA and GDPR do not incorporate any similar mandatory “information revealing” solutions in their regimes.

This somewhat unique combination of a broad mandate, a system not designed to generate the type of information required for regulatory oversight, and a lack of a complementary civil society puts significant pressure on the resources that data authorities need to properly perform their role. Another comparison with antitrust can help showcase the size of the challenge. European data protection agencies have grown significantly since the enactment of the GDPR. The Irish Data Protection Commission grew from 70 to 145 personnel between 2016 and 2021 and the seven hundred staff of the UK’s Information Commissioner is now larger than the antitrust

---

246. See, e.g., ORG. FOR ECON. COOP. & DEV., RECOMMENDATION OF THE COUNCIL CONCERNING EFFECTIVE ACTION AGAINST HARD CORE CARTELS 6 (2021) [hereinafter RECOMMENDATION OF THE COUNCIL] (recommending the establishment of leniency programs that encourage self-reporting of violations as a backbone of an effective cartel detection system); ORG. FOR ECON. COOP. & DEV., REVIEW OF THE RECOMMENDATION OF THE COUNCIL CONCERNING EFFECTIVE ACTION AGAINST HARD CORE CARTELS 15-17 (2019) [hereinafter REVIEW OF THE RECOMMENDATION] (describing the rise in antitrust leniency programs around the world in the past twenty years).
division of the FTC, which had 528 full-time staff at the end of 2020.248 Yet, their workload is all but endless—it took European data protection agencies only eighteen months to trigger the same amount of EU-wide potential cooperation requests that their antitrust counterparts issued in more than fourteen years (around 2,500 investigations).249 In the first nine months of GDPR enforcement, European data protection authorities received 206,326 notifications of potential violations, closing a total of 37,900 investigations.250 By November 2019, the number of complaints rose to 275,000, but it only led to 785 fines, most of which are still subject to judicial review.251 Authorities themselves acknowledged they are overwhelmed with the workload.252

As a result, governments must continue to devote a growing share of scarce public funds to an area they might rather not, as enforcing data protection laws can conflict with some other important priorities such as national security or industrial policy. Lack of political will means that agencies may be chronically underfunded. For example, the 2019 budget of the California office of the Attorney General, which is responsible for overseeing the CCPA, was around $5,000,000, which was only enough to support an enforcement staff of twenty-three lawyers who are also responsible for broader consumer protection.253 The FTC has acknowledged that its lack of resources is undermining its enforcement capacity254 and is preventing the expansion of its already constrained data protection team (composed of sixty-one employees in 2020, or 5% of the agency’s total staffing),255 which has been criticized as insufficient to effectively monitor and enforce data protection laws.256 The FTC’s annual budget is around $330,000,000, while the guaranteed funding of the California Privacy Protection Agency is only $10,000,000.257 In the EU, the Irish


252. Satariano, supra note 4.


Data Protection Commission’s 2019 budget was €15,000,000, and the budget of the Luxembourg authority was €5,500,000. Although most European data protection authorities stressed the need for a significantly larger budget and personnel to appropriately enforce their new, expanded legal responsibilities, “almost none of them received the requested amount” of funding.

Finalizing the stylized restaurant example, as a third alternative to remedy potential violations of its data rights, the aggrieved consumer could complain to a dedicated regulator that their name and phone data had been illegally collected and processed by a third-party. In this case, however, the consumer cannot enforce the law directly. First, they would need to convince a public agent to open an investigation into the matter. The consumer, however, does not know which restaurant shared their data, so the agent must require all of the restaurants the consumer visited to disclose whether they were responsible. This means that the public enforcer must depend on the restaurants to produce the information needed to enforce the law. The consumer is then only updated every three months that investigations are ongoing, but there is hardly anything they can do to accelerate the process. The same public agent, however, oversees data processing in the entire locality, so it must simultaneously handle thousands of other complaints. Restaurants also generally refuse to share the information the agent needs to finalize the case, as they profit from it. In addition, the restaurant industry is key for the economic development of this specific country, and many restaurants settled in that country because it has somewhat permissive data use laws. The agent, therefore, knows that the government does not want to antagonize that industry. After many years, the regulatory agency issues a fine that amounts to 0.1% of what the restaurant in question earned in profits in the preceding year. The restaurant still has the option to appeal the fine before the judiciary, further delaying the enforcement of the law.

Again, this is a stylized example. Yet, it touches in only some of the challenges of developing an effective regulatory system for complex data collection and processing practices. Broad mandates, large information asymmetries, and market power significantly increase the public resources needed to enforce the laws and increase the risks of both private and public capture.

---

258. MASSÉ, supra note 213, at 11.
259. EUR. DATA PROT. BD., supra note 250, at 7.
260. As previously discussed, Ireland’s digital sector is responsible for 26% of the country’s exports and 10% of its employment. See IRISH BUS. & EMPS. CONFEDERATION, supra note 234, at 13-17; see also Lillington, supra note 215, at 4.
261. The first fine issued by the Irish data protection authority against Twitter took almost two years of investigation, despite being a simple case of the company not complying with a seventy-two-hour data breach notification deadline, which amounted to approximately $550,000, or 0.1%, of Twitter’s 2019 profits. Natasha Lomas, Twitter Fined ~$550K Over a Data Breach in Ireland’s First Major GDPR Decision, TECHCRUNCH, (Dec. 15, 2020), https://social.techcrunch.com/2020/12/15/twitter-fined-550k-over-a-data-breach-in-irelands-first-major-gdpr-decision/ [https://perma.cc/K3W4-V3D6].
III. NARROWING DATA PROTECTION’S ENFORCEMENT GAP THROUGH INSTITUTIONAL DESIGN

Regulatory systems must be designed to anticipate implementation challenges and facilitate monitoring and enforcement. Yet, online privacy laws like the CCPA, CPRA, and GDPR fail to account for the role of exceptionally large information asymmetries and market power in undermining markets, torts, and regulatory enforcement as mechanisms to ensure that companies reflect the data privacy preferences of consumers. As mentioned in Part I above, it is possible that compliance will improve as these regimes mature. However, experience shows that this is not guaranteed. Societies are now spending billions of scarce private and public resources on systems with important flaws. Narrowing data protection’s enforcement gap will require improving the institutional design of these laws. By paying more attention to what happens in the shadows of the law, scholars and policymakers can help ensure not only that these regimes better deliver on their promises, but also that they do so in a quicker and more cost-effective manner.

It is beyond the scope of this Article to provide definitive solutions to the multiple and complex issues identified above. First, most of the solutions would be jurisdiction specific, requiring changes to different national laws that regulate public transparency, standing, discovery, causation, trade secret laws, the filing of lawsuits for failure to act, etc. Second, it is possible that these systems may require a significant rethinking of their fundamental goals. Rather, the objective of this Article is to learn from the ways more mature regulatory regimes, such as antitrust and anti-corporate fraud, have tackled the common challenges of large information asymmetries that undermine legal compliance. If these challenges are not addressed, it is unlikely that any privacy law will fully deliver on its goals. This focus on information asymmetries is justified because the antitrust community is already discussing how to diminish the market power of large digital platforms. However, the equally important role of these asymmetries in undermining data protection compliance has been largely neglected.

In particular, an improved data protection regulatory system should incorporate at least three key principles: (i) multiplying available monitoring and enforcement resources, (ii) bringing violations to the attention of monitors and enforcers, and (iii) forcing governmental accountability to diminish risks of regulatory capture.

A. Multiplying Monitoring and Enforcement Resources

Not only is the collection and processing of personal data usually taking place in complex, non-transparent environments, but also the widespread collection and easy replicability of these data expands the jurisdiction of online privacy laws. As

262. Compliance with Directive 95/46 or the European E-privacy directive has been extremely low, despite their enactment decades ago. See supra Section I.B.
263. See Waldman, supra note 55, at 825 (discussing other structural changes to privacy laws that would also be important to help promote compliance).
264. See generally Lancieri & Sakowski, supra note 14 (reviewing diagnosed concerns and potential remedies).
seen above, this combination undermines monitoring and enforcement in systems that rely primarily on regulatory enforcement, like the GDPR and the CCPA.

Important information asymmetries, however, are not exclusive to data protection, even if they are exacerbated in it. Anti-corporate fraud and antitrust policies also face challenges in discovering intra-corporate wrongdoing in complex environments. To help tackle this problem, these regimes have been designed to encourage sophisticated private organizations that understand the complexity of corporate practices and denounce violations. For example, a large survey on corporate fraud lawsuits in the U.S. found that regulators exposed only 20% of wrongdoing, with the remaining 80% being exposed by employees, the media, academia, industry analysts, and other sophisticated third-parties.265 The majority of U.S. antitrust litigation is private, not public.266 Data protection laws should be equally designed to expand the number of sophisticated private intermediaries—such as privacy NGOs, independent think-tanks, and class-action plaintiffs—that have the expertise and resources to comprehend the complexity of data processing and act alongside public regulators in detecting violations. These sophisticated civil society intermediaries are also better equipped to constantly monitor regulatory action, increasing the cost of capturing regulators.

An expansion of these sophisticated private intermediaries requires the availability of appropriate and independent funding. However, most privacy NGOs and other similar organizations are supported by grants and donations—an unreliable and insufficient source of funding for mass oversight.267 An effective online privacy regulatory system should ensure a consistent, independent source of funding for these intermediaries, enabling them to invest time and resources into hiring technical personnel, starting complex and potentially unfruitful investigations, potential litigation, and better equipping them to resist the temptation of being co-opted by large corporate donations.268

267. For example, even the most well-known European NGOs, like NOYB and La Quadrature du Net, have trouble raising resources. NOYB has so far raised only 78% of its €500,000 funding goal for 2020. NOYB, Our Funding Goal: 2/3 by Supporting Members, https://support.noyb.eu/funding [https://perma.cc/7UVJ-5P3E] (last visited Dec. 23, 2021). La Quadrature du Net relies on donations for 70% of its annual budget of around €400,000, but in 2020 they only raised €217,000, and for 2021 they raised even less—around €140,000. See About Us, LA QUADRATURE DU NET, https://www.laquadrature.net/en/about/ [https://perma.cc/TS5JE-UMTE] (last visited Dec. 23, 2021); Rallumez les ombres, faites un don à la Quadrature du Net, LA QUADRATURE DU NET, https://www.laquadrature.net/donner/ [https://perma.cc/6MFX-85ZE] (last visited Dec. 23, 2021). In the U.S., the Electronic Privacy Information Center, another large NGO, had a budget of roughly two million dollars in 2018. See ELEC. PRIV. INFO. CTR., FINANCIAL STATEMENTS 6 (2018).
There are different mechanisms to help ensure that private parties have incentives to specialize in this field. For example, the U.S. legal system awards treble damages for antitrust violations to encourage private litigation—a mechanism that the Supreme Court has said works as “a chief tool in the antitrust enforcement scheme”\textsuperscript{269} that encourages litigants to serve as “private attorneys general.”\textsuperscript{270} This is certainly an important mechanism to consider, even if it has limitations and is of difficult acceptance abroad.\textsuperscript{271}

Jurisdictions should consider creating a system of recurrent grants that is linked to how well intermediaries perform their role as an institutional design alternative. These grants would be funded by the resources raised from fines and damage awards associated with data protection violations and would be distributed according to both a direct and an indirect method. Under the direct method, the laws could establish that private parties such as NGOs, data-focused investigative news agencies (such as The Markup), or other intermediaries, are entitled to a small percentage of: (i) the fines that result from an investigation that started from a private complaint, or (ii) the damages awarded in tort litigation where these organizations represent consumers.

Under the indirect method, a panel of public authorities and civil society representatives could annually distribute grants to NGOs, universities, think tanks, dedicated investigative news agencies, and other private organizations that are engaged in projects aimed at improving data protection. This mechanism has several advantages. For example, it (i) can ensure long-term funding for these organizations, rather than large lump-sum awards followed by periods without any resources; (ii) can be implemented without changes that impact the perceived justice of tort law; and (iii) can directly connect funding to effective monitoring, minimizing administrative costs.

Again, antitrust policies provide an example as to how the indirect method would work. Brazilian antitrust laws require that fines imposed by the Brazilian competition authority are allocated to a public fund aimed at protecting the diffuse interests of citizens. Between 2016-2020, the fund raised approximately BRL 3,000,000,000 (approximately USD 575,000,000).\textsuperscript{272} This fund is managed by a council composed of seven career civil servants and three civil entity representatives who are selected for a renewable appointment of two years.\textsuperscript{273} The fund annually publishes public calls for applications through which universities, NGOs, and even other entities can request resources to support their activities in defense of the public

interest. For example, in 2019 the fund awarded forty-six long-term grants. The changes made to the CPRA also serve as an important step in this direction. Section 1798.160(b)(2)(B) of the CPRA ensures that 9% of the Consumer Privacy Fund that collects CCPA damage awards—a majority of which goes to the Californian treasury—will be distributed by the California Privacy Protection Agency as grants to civil society and law enforcement. The 3% that would go to NGOs, however, seems insufficient to bring monitoring resources to a point where they can actually diminish the high levels of information asymmetries in data protection. Monitoring resources should be increased, and European countries should also adopt similar initiatives.

The direct funding system, on the other hand, could be an expansion of the already common U.S. practice of directing cy pres awards in class action lawsuits to privacy NGOs. A problem with cy pres settlements in data protection suits is the occasional distribution of awards to organizations that are not directly connected to online privacy. To address this, the law could encourage awards to be funneled to the public fund and distributed according to the aforementioned rules, potentially ensuring that cy pres resources are not unduly targeted.

Both proposals have limitations. First, they focus on deterrence rather than victim compensation—a choice which is justified at a time when enforcement levels are low, but that could change in the future. Privacy class action settlements could also continue to be unduly funneled to plaintiffs’ lawyers and organizations that do not protect consumer privacy, or to a public grant system that can be diverted to accomplish interests other than those that were initially envisioned. To prevent these limitations, it is important that judges closely monitor settlements and that laws create a centralized, public database that lists all damages awards and public grants to enable oversight. Laws may also ensure that the fund has an obligation to award at least a percentage of its annual budget, impose strict conflict of interest rules, and increase the number of independent civil society representatives that are part of the

---

274. Id.
276. Cal. Civ. Code § 1798.160(b)(2)(B) (effective Jan. 1, 2023). The distribution of the 9% would be: (i) 3% to nonprofit organizations to promote and protect consumer privacy, (ii) 3% to nonprofit organizations and public agencies to educate children in the area of online privacy, and (iii) 3% to state and local law enforcement agencies to fund cooperative programs with international law enforcement organizations. Id. § 1798.160(B) (i)-(iii).
277. Id. For instance, even if CCPA fines reach an unprecedented $100,000,000, this would lead to an annual distribution of $3,000,000, which is arguably not enough to support many large-scale organizations that employ lawyers, tech specialists, etc.
278. See Stigler Ctr., supra note 256, at 220.
280. See id. at 309.
management council. Finally, different jurisdictions should establish separate funds, ensuring some form of competition over governance.

Still, a data protection regulatory regime that expands the funding of independent and sophisticated data privacy intermediaries—allowing them to tap into donations, grants, and awards from tort litigation—would be much more capable of detecting wrongdoing than one that is overtly reliant on public regulators.

B. Bringing Data Protection Violations to Light

The information asymmetries between how companies collect and process personal data and what society and regulators know about this collection, increase the importance of mechanisms designed to bring violations to the attention of overseers. A stronger, better-funded civil society will increase monitoring resources. Antitrust, anti-corruption, and anti-corporate fraud regimes show that it is important that regulatory systems also encourage insiders to report illegal behavior through the establishment of a robust whistleblowing program.

Whistleblowers (in particular employees) are key to the discovery of corporate fraud.282 Antitrust regulators have also long relied on leniency programs—through which companies denounce cartels in exchange for a more lenient prosecution—as a key mechanism to bring otherwise secret and illegal private deals to light.283 Indeed, past studies have found that having access to privileged internal information greatly increases the probability of successfully exposing hidden fraud.284 Offering financial incentives to those who reveal fraud also significantly improves the probability that employees will expose wrongdoing and diminishes mistaken denunciations.285

Increasing compliance with online privacy laws will require redesigning regulatory systems to bring otherwise obscure violations to light. These comparative experiences showcase the importance of data protection authorities establishing

282. Dyck et al., supra note 265, at 2225-26 (surveying 216 high-profile corporate fraud cases in the U.S. and finding that employees, non-financial market regulators, business analysts, and the media were responsible for 54% of all corporate frauds exposed, with employees being the most important at 17% of cases); Andrew C. Call et al., Whistleblowers and Outcomes of Financial Misrepresentation Enforcement Actions, 56 J. ACCT. RSCH. 123, 126, 128 (2018) (reviewing 658 SEC enforcement actions for fraud and finding that “employee whistleblowers play an integral role in monitoring firm behavior”); ORG. FOR ECON. COOP. & DEV., THE DETECTION OF FOREIGN BRIBRY: THE ROLE OF WHISTLEBLOWERS AND WHISTLEBLOWER PROTECTION 3, 11 (2017) (stressing the key role whistleblowers play in revealing foreign bribery).

283. See generally RECOMMENDATION OF THE COUNCIL, supra note 246, at 6; REVIEW OF THE RECOMMENDATION, supra note 246.

284. See Dyck et al., supra note 265, at 2215, 2231 (finding that a potential detector’s access to internal company data increased that actor’s probability of detecting fraud by 15%); Call et al., supra note 265, at 126 (finding that whistleblower involvement in the enforcement process is associated with greater monetary penalties for targeted firms and longer prison sentences for targeted employees).

285. Dyck et al., supra note 265, at 2246 (finding that whistleblower employees in the healthcare industry, where there are financial incentives to report cases, were responsible for 41% of frauds exposed in the industry, versus 14% in other industries without financial incentives). The rate of frivolous corporate fraud lawsuits is lower in healthcare than in other industries. Id. In fact, among the fraud committing firms studied, those in the health care industry had a 27% higher probability of having an employee as the whistleblower. Id.
robust whistleblowing programs specifically aimed at encouraging the reporting of data protection violations.\textsuperscript{286} In particular, it is key that this program:

i. Defines a “whistleblower” broadly to include not only formal employees but also contractors, consultants, former employees, temporary employees, etc.\textsuperscript{287} The program should also protect public employees who may report potential capture of regulatory authorities.

ii. Raises awareness of the protections afforded by the program to potential reporting persons by hosting workshops, requiring corporate training, and publicizing the program broadly in specialized channels and in the media.\textsuperscript{288}

iii. Allows for potential whistleblowers to obtain confidential advice from the public authority before filing a report.\textsuperscript{289} This has been done, for example, both in the Netherlands and in the U.S. In the U.S., the Securities and Exchange Commission (SEC) created a specialized whistleblower hotline to provide guidance to potential corporate-fraud whistleblowers.\textsuperscript{290} As an alternative, the data protection fund discussed above could provide resources to independent, private third-parties like NGOs dedicated to protecting and guiding potential whistleblowers or even representing them before authorities.\textsuperscript{291}

\textsuperscript{286} Both California and the EU have general whistleblower protections. In California, whistleblower laws that provide general protections against retaliation for revealing wrongdoing include the California Whistleblower Protection Act, CAL. GOV’T CODE § 8547.8 (West 2021), the False Claims Actions Act, CAL. GOV’T CODE § 12651 (West 2021), and California Labor Code, CAL. LAB. CODE § 1102.5 (West 2021). In the EU, Directive 2019/1937 (October 2019) establishes minimum levels of whistleblowing protection around the EU and also requires member states to ensure that their whistleblower protection program encompass violations of data protection laws. See Directive 2019/1937, of the European Parliament and of the Council of 23 October 2019 on the Protection of Persons Who Report Breaches of Union Law, art. 1, 2019 O.J. (L 305). Yet, the translation of these commands to a dedicated data protection program is lagging. California, along with important EU jurisdictions such as Ireland and Luxembourg, do not yet have a dedicated data protection whistleblowing program. In general, these whistleblowing protection statutes fall short of the many recommendations for a robust protection program that are made herein. For example, the EU Directive does not encourage financial rewards that are key for an effective program. See, e.g., Dimitrios Kafteranis, Rethinking Financial Rewards for Whistle-Blowers Under the Proposal for a Directive on the Protection of Whistle-Blowers Reporting Breaches of EU Law, 2 NORDIC J. EUR. L. 38 (2019).

\textsuperscript{287} REVIEW OF THE RECOMMENDATION, supra note 246, at 15.

\textsuperscript{288} Id. at 4.

\textsuperscript{289} Id. at 7-8.

\textsuperscript{290} Id.

\textsuperscript{291} Id. at 9.
iv. Protects the anonymity of whistleblowers. For example, in Austria, authorities have created a portal through which corporate-fraud whistleblowers may report wrongdoings using a secure mailbox that encrypts the information, protects their anonymity, and enables authorities to provide feedback and updates about the status of the claim.

v. Provides financial rewards for successful reports. Financial rewards are key to encouraging whistleblowing because employees who report wrongdoing risk ending their careers. These rewards should be large enough to encourage whistleblowing and include minimum thresholds to help prevent frivolous claims. For example, whistleblowers who provide the U.S. SEC with information that leads to over one million U.S. dollars in sanctions are rewarded with ten to thirty percent of the money collected.

vi. Protects good-faith whistleblowers from retaliation—a common occurrence in tech markets—through tactics such as broad civil remedies or punitive damages. Most whistleblowers prefer to first report company wrongdoing internally and alert regulators only when the company then refuses to take action. The law should make clear that these employees are protected, and require that companies have an obligation to forward any serious whistleblower complaints to regulators within a given period. The law should also shield good-faith whistleblowers when they report wrongdoing to journalists and other private intermediaries that can call attention to potential problems.

vii. Finally, these programs should protect whistleblowers from civil and criminal charges—such as slander, violation of trade secrets, corporate espionage, and defamation—that well-resourced organizations may use to silence reporting parties.

292. Dyck et al., supra note 265, at 2240, 2245 (finding that in 37% of cases employee whistleblowers do not identify themselves, and that in 82% of cases where employees were named, the individuals were fired, quit under distress, or had significantly altered responsibilities as a result of revealing the wrongdoing).

293. O.R.G. FOR ECON. COOP. & DEV., supra note 282, at 10.

294. Dyck et al., supra note 265, at 2251 (“A natural implication of our findings is that the role of monetary incentives should be expanded.”).


296. Id. at 19-20.


These principles would certainly have to be adapted to jurisdictional laws, but a dedicated data protection whistleblower program that incorporates even most of these principles would diminish information asymmetries and increase the enforcement of online privacy.

C. Increasing Governmental Accountability

Finally, while some characteristics of data protection weaken exit and voice and reinforce the importance of a solid public enforcement system, heightened risk of capture by private or public interests in data policy also emphasizes the need for institutional safeguards to protect the public interest. Many important data protection regulators are unjustifiably opaque, such as those of Ireland, Luxembourg, and even the U.S. By requiring authorities to publicize a wide range of information about their enforcement actions, online data privacy regimes can diminish the costs of private oversight and help expose eventual problems. After all, sunshine is the best of disinfectants when fighting entrenched private interests.

Again, a comparison with antitrust law can help showcase how to improve the design of data protection laws. Extensive public disclosure rules have been instrumental in understanding how corporate donations influence advice in competition policy. Multiple reports have suggested enhancing the transparency obligations of U.S. antitrust, which would increase public confidence in regulators and hinder attempts of regulatory capture. Extensive discovery rights have also helped expose many cases of corporate malpractice.

Some antitrust systems have been expressly designed to maximize transparency to help fight regulatory capture without undermining enforcement capacity. The Brazilian experience is noteworthy. Brazil’s competition law establishes that antitrust proceedings should be public by default, but that the private parties may request, or the regulator may determine, that certain types of information be kept confidential. To comply with this legal requirement, the Conselho Administrativo de Defesa Econômica (CADE) (the Brazilian antitrust authority) created a system where private parties are required to prepare both a public and a confidential version of any document they file before CADE. CADE’s systems also host public and confidential versions of all of CADE’s opinions—including statements of objections or opinions to approve a merger or dismiss an investigation. All the public versions of both private and public documents are freely available on CADE’s website, while

299. See generally Wakabayashi, supra note 268.


301. Cf. Roy Shapira & Luigi Zingales, Is Pollution Value-maximizing? The DuPont Case, 2, 6-7 (Nat’l Bureau of Econ. Rsch., Working Paper No. 23866, 2017) (showcasing how internal DuPont documents exposed at trial were key to uncovering illegal practices by the company).

302. Article 49 of Brazilian Antitrust Law (Law N.º 12,529/11).
the private versions are protected by secrecy laws. Some investigations require absolute secrecy (e.g., cartel investigations before dawn raids). For those, CADE maintains a smaller public and a more extensive private record, but both are confidential until the authority rules that publicity will not harm the investigation, nor the parties involved. However, ultimately the public record is made available to civil society.

Requiring private parties to disclose in advance what specific pieces of information they understand as confidential is important because it: (i) expedites disclosure; (ii) allows CADE to focus potential disputes on key pieces of data over which there is disagreement; and (iii) allows interested private parties to better understand and challenge abusive confidentiality requests. While this system increases administrative costs, the structure, which requires private parties to cooperate in implementing regulatory transparency, helps minimize negative impacts on enforcement actions. Indeed, CADE hosts one of the most active anti-cartel programs in the world and—despite Brazil’s history of corruption—CADE’s work is well-recognized by Brazilians and international organizations alike. 303

Data protection laws should impose similar obligations on regulators. In particular, it would be important that regulators: (i) maintain a webpage that lists ongoing investigations, describing the scope of the investigation and the interested parties; (ii) upload public versions of new case developments such as statements of scope and indictments to this webpage (e.g., Statements of Objection) as well as the company’s responses; and (iii) upload public versions of opinions and settlements to this webpage, as well as at least a short but precise justification on the reasons why authorities decided to close investigations, settle cases, or impose fines.

CONCLUSION

The GDPR, CCPA, CPRA, and their dozens of international counterparts have, and will continue to, bring about profound changes. Data markets, usually left almost to their own devices, now face a new environment where the state mediates at least part of the interactions between companies and consumers. Yet, data protection laws have been failing to fully deliver on their promises. This Article suggests that this has been in part because legislators have not anticipated how the particularly pervasive information asymmetries and market power found in many data markets undermine the role of markets, torts, and regulatory enforcement as mechanisms to ensure legal compliance.

Democratic governments around the world have decided that these data protection regulatory regimes are here to stay. Societies must now ensure that these laws lead to meaningful improvements on the ground. This Article suggests that

303. The OECD affirmed that CADE is “well regarded domestically and internationally within the practitioner community, with peer agencies and within the Brazilian administration” and praised CADE’s work in prosecuting cartels. ORG. FOR ECON. COOP. & DEV., PEER REVIEWS OF COMPETITION LAW AND POLICY: BRAZIL 9-11 (2019). In addition, the prestigious British magazine Global Competition Review considered CADE the best antitrust agency in the Americas in three of the past five years. CADE is Awarded the Agency of the Year in the Americas, CADE (Nov. 4, 2018), http://antigo.cade.gov.br/cade_english/cade-is-awarded-the-agency-of-the-year-in-the-americas [https://perma.cc/6DEQ-P7JV].
narrowing data protection’s enforcement gap is not impossible, but it will require better institutional design. Multiplying monitoring and enforcement resources, encouraging insiders to bring violations to light, and promoting regulatory accountability are important but are only initial solutions to help tackle a multi-faceted and complex problem. This is a field that will welcome contributions from lawyers, data and political scientists, economists, psychologists, and many other scholars for years to come.

APPENDIX

*Impacts on the Ground: A Survey of the Empirical Evidence on How the GDPR and CCPA Impacted Data Protection*

A survey of empirical studies assessing the impacts of the GDPR and the CCPA on actual data collection and processing points to underwhelming results so far. None of the twenty-six independent studies surveyed found meaningful compliance on the ground. In particular, twenty studies, summarized below, found widespread violations.  

i. A review of 2,000 high profile websites found that while the GDPR did give users more privacy controls, “tracking is prevalent, happens mostly without user’s consent, and opt-out is difficult.” Ninety-two percent of websites start tracking users before providing them with any notice and 85% continue tracking them or add even more cookies after the users opt-out.  

ii. A review of the privacy policies of 194 firms before and after the passage of the GDPR found that while the vast majority amended their policies to become more information protective, “the overall level of compliance [with GDPR provisions] is not high in absolute terms.”  

iii. A study tracking 1,250 top-visited European and U.S. websites before and after the GDPR (February 2018 to September 2018)  

---  

304. It is worth noting that many European studies focus on the collection and processing of data through cookies, which have limitations. Cookies are mostly regulated by the ePrivacy directive. However, Article 7 of the GDPR has reframed what constitutes effective consent for the collection of personal data, including through cookies. Therefore, these studies found violations of both the ePrivacy directive and the GDPR. These findings are backed by European case law. See, e.g., C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, ECLI:EU:C:2019:801 (Oct. 1, 2019); see also Cristiana Santos et al., *Are Cookie Banners Indeed Compliant with the Law? Deciphering EU Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners*, 2020 TECH. & REGUL. 91, 91-92 (2020).

305. Sanchez-Rola et al., *supra* note 8, at 5, 9-10 (including both first-party and third-party tracking).

found only a small decrease in advertising third-party requests, which the authors could not directly link to the GDPR.  

iv. A survey of the five most popular Consent Management Platforms (CMPs) used by the UK’s ten thousand most accessed websites found that by September 2019 only 11.8% of the UK websites met minimum notice and consent requirements.

v. A study of one thousand randomly selected EU consent notices collected through October 2018 found that 57% of these notices nudge users towards privacy-unfriendly options and 96% of them provide either no consent choice or confirmation only, violating the GDPR.

vi. Another study of 1,426 consent banners used by the 22,949 most accessed websites in Europe found that, by September 2019, 10% of websites placed cookies before giving the user any choice and 5% still placed the cookies after the user refused to give consent. Overall, the study found that 54% of websites surveyed violated legal requirements.

vii. A study of cookie placements in 35,000 popular EU websites after four years of coming into compliance with the European e-privacy directive found that between 49% and 74% placed tracking cookies before receiving consent (depending on the definition of tracking), a percentage that stayed constant after the GDPR came into effect. This indicates that both policies were ineffective, and points to a lack of auditing by regulators.

viii. A study analyzing the five hundred most visited websites for each EU country found that, even after the GDPR, 15% of the websites studied had no privacy policy, 37% did not comply with cookies consent notices, and the amount of consumer tracking pre- and
post-GDPR mostly remained the same. The study warned against a false sense of GDPR compliance.

ix. Another study of the 27,000 most accessed websites in the EU, the U.S., and Canada found that the GDPR initially led to a 14.9% drop in the use of third-party vendors, but that number rebounded to pre-GDPR levels by the end of 2018, potentially because firms became less afraid of enforcement actions.

x. A cookie sweep of thirty-eight large data processors by the Irish Data Protection Commission found that more than eighteen months after the GDPR had come into force, 92% did not comply with the law.

xi. Another cookie sweep of 175 websites performed by the Dutch data protection authority in December 2019 found that almost no website was fully compliant with legal requirements.

xii. An in-depth study covering data from January 1, 2018 to July 31, 2018 from one of the largest online travel agencies and travel meta-search engines found that the GDPR resulted in a reduction of 12.5% in total cookies (not total consumers because one consumer can have many cookies), which is a proxy for decreased online tracking. However, the remaining consumers are more persistently trackable after the GDPR, so the overall level of online tracking increased by 8%—something that should lead to increased ability to predict consumer behavior.

xiii. An interesting analysis of data interconnection agreements and interconnection points to Internet Service Providers (a proxy for data transfers) pre- and post- GDPR was conducted in 2020. Contrary to expectations, the study found that the GDPR had a statistically significant net zero effect, meaning that the GDPR

313. Degeling et al., supra note 65, at 7-8, 10, 14.
314. Id.
316. DATA PROT. COMM’N, supra note 9, at 6.
319. Id.
has not led to decreases in data traffic that could potentially impact investments in internet networks.\textsuperscript{320}

xiv. A 2020 large-scale survey of 17,000 websites and more than 7,500 cookie banners in the UK and Greece (14,000 in the UK and 3,000 in Greece) found that only 50\% of websites display a cookie notice, and that the majority of websites employed dark patterns to nudge users towards acceptance. The study concluded that a “substantial proportion of the websites do not comply with the [GDPR] even at the very basic level.”\textsuperscript{321}

xv. A detailed survey of GDPR and ePrivacy Directive requirements for consent involving the collection of information through cookies concluded that fully automatic consent verification by technical means is not compliant with both laws. Yet, this is the widespread method of adoption in the EU.\textsuperscript{322}

xvi. A study conducted in January 2020 analyzed the basis for the collection and processing of personal data by more than six hundred European advertisers. The findings “demonstrate[] the persistence of the advertising industry in non-compliant (with GDPR and ePrivacy Directive) methods for tracking and profiling, bundled in often complex and vague presentation of purposes.”\textsuperscript{323}

xvii. An automated and manual visit of the top five hundred UK websites before and after the GDPR, combined with 8,416 websites from the browsing of fifteen users in the UK and China, found that websites that gave users more choice in terms of cookie compliance stored more cookies after the enactment of the GDPR. It also found that many websites appear to disregard user choice, storing cookies despite denials in consent, and that the number of tracking cookies remained stable before and after the enactment of the GDPR.\textsuperscript{324}


\textsuperscript{321} Georgios Kampanos & Siamak F. Shahandashti, Accept All: The Landscape of Cookie Banners in Greece and the UK 1, 14 (Apr. 12, 2021) (on file with arXiv.org).

\textsuperscript{322} Santos et al., \textit{supra} note 304, at 92, 135.

\textsuperscript{323} Célestin Matte et al., Purposes in IAB Europe’s TCF: Which Legal Basis and How are They Used by Advertisers? 2 (May 7, 2020) (on file with hal.inria.fr).

A fascinating survey of more than 900 news and media websites in the U.S. and the EU between April 2018 and November 2019 found that while the introduction of the GDPR led to an initial decrease in the number of third-party cookies and tracking responses in EU websites, this number quickly rebounded to pre-GDPR levels. In addition, the study found that the GDPR had a small but significant impact on the amount of page views, but no significant impact on the quantity of content published or the quality of content and social media engagement, even for websites that relied heavily on advertisement. Given the study set-up, this may be interpreted to mean that the GDPR did not meaningfully impact the tracking capacity of these websites.

A February 2020 PwC survey of the websites of the six hundred largest companies in the U.S. found that a majority of these websites did not offer portals for users to access their information.

A survey by DataGrail, a U.S. privacy management tool, found that throughout 2020 business-to-consumer companies received, on average, 137 data subject requests per million identities they hold per year, with the average stabilizing at around eleven requests per month. This means that only 0.001% of consumers are exercising their rights despite the average cost of almost $200,000 per request.

While not specifically targeted at the CCPA or the GDPR, a September 2020 scan of more than eighty thousand of the world’s most popular websites found that tracking remains ubiquitous around the world and in the U.S., even for highly sensitive websites, such as those of abortion providers or for victims of sexual violence. The general conclusion is that third-party tracking is as pervasive now as it was ten years ago, but it has only “become creepier and more difficult to stop.”

Other studies present a more favorable picture of the on the ground impact of the GDPR. Even those, however, also show only a limited impact and introduce important caveats about the state of GDPR enforcement.

---

326. Id. at 47-48, 55.
327. PwC, supra note 2.
328. DATAGRAIL, supra note 13, at 4-6.
329. Id.
330. Sankin & Mattu, supra note 70.
331. Angwin, supra note 71.
i. One study analyzed web tracking by 5,100 of the most visited EU websites between September 2017 and April 2019, and found that the adoption of the GDPR was correlated with a 9% reduction of third-party tracking cookies for the median website, and a 17% reduction in third-party HTTP requests for the median website. However, it also found that the GDPR led to no change in tracking by the most pervasive companies, such as Google, Facebook, Amazon and others. These companies would have expanded to more even websites.

ii. One study of 110,000 websites between May 2017 and November 2018 estimated that the GDPR has led to a 10% decrease in third-party tracking cookies, a smaller increase in first-party cookies, and a 6% decrease in requests to third-party websites that disclose their collection of personal data. The authors of the study see this as evidence that the GDPR achieved at least some data minimization goals. However, they also found that third-party requests in general, which can be seen as a proxy for tracking, rebounded to pre-GDPR levels as companies learned how to navigate compliance. In any event, the absolute impact levels are low for such an all-encompassing regulation.

iii. A rare study comparing permissions for data access in the fifty most downloaded apps from Android’s Google Play store between March 2017 and December 2018 found a general decrease in the number of permission requests for apps—particularly to access contacts, location, calendar, SMS, and phone. It also found less use of these permissions in idle mode. However, it noted that apps are more frequently using permissions for camera, microphone, and body sensors. The overall conclusion is that app privacy has only moderately improved since the GDPR’s entry into force.

iv. An automated analysis of the privacy policies of 695 websites (that appear in the Top 500 ranking in Alexa’s Top Sites service) between November 2017 and October 2019 found that enacting the GDPR led to changes in privacy policies in the U.S. and EU.

332. Solomos et al., supra note 201, at 3, 6, 8.
333. See id.
334. See generally Peukert et al., supra note 201.
335. Id. at 1, 13-14, 16.
337. Id. at 6
338. Id. at 1, 6, 9.
Further, a manual coding of 246 policies found that EU-based websites became much more compliant with GDPR requirements.\textsuperscript{339} Still, the average formal compliance with GDPR requirements was only 68%.\textsuperscript{340}

v. Finally, one study using Adobe Analytics data for 1,084 dashboards found that the GDPR led to a 11.7\% decrease in page views for European websites and a 13.3\% revenue fall for e-commerce websites. This was partially motivated (6.9-29\%) by users not providing consent to data collection and by decreases in paid marketing channels as drivers of traffic. While the study does not assess data collection or its impacts on web-tracking, it states that the vast majority of websites in their sample adopts an opt-out approach for consent, which is in violation of data protection laws and that changes in marketing budgets are consistent with some websites moving ads from channels that rely on personal data to others that do not. Overall, the study found “modest progress” towards GDPR compliance.\textsuperscript{341}

Importantly, although they are very valuable, these studies have a selection bias in reporting what they can count readily. They usually use third-party cookies as proxies for tracking because this is what can be measured by external sweeps. However, this methodology has important limitations.

First, these sweeps cannot measure how much data is actually collected through each cookie, so they are an imperfect proxy at best. Second, many companies (such as Google and Facebook) responded to data protection laws not by diminishing data collection, but by embedding their third-party code in first-party applications.\textsuperscript{342}

There are even fewer studies addressing legal compliance with regard to equally intrusive but less “transparent” tracking mechanisms such as pixels, tags, fingerprinting, local storage, browser extensions, single sign-on, or even direct matching and sharing of personal data. A large survey on browser fingerprinting, for example, argued that their increasing prevalence and stealth nature made it “particularly dangerous” to the privacy of users.\textsuperscript{343} Third, many cookie sweeps also restrict their analysis to homepages, but studies found more pervasive online tracking

\begin{thebibliography}{9}
\bibitem{340} \textit{Id.} at 49 (obtained by dividing the average compliance score of 6.13 by the full compliance score of 9).
\bibitem{342} \textit{COMPETITION & MKTS. AUTH.}, \textit{supra} note 90, at G8, G25-26 (explaining the shift and how it enables continued tracking despite decreases in third-party cookies).
\bibitem{343} Pierre Laperdrix et al., \textit{Browser Fingerprinting: A Survey} 26 (Nov. 4, 2019) (on file with arXiv.org).
\end{thebibliography}
Fourth, there are few studies looking on how these laws have impacted tracking outside of the browser world, in particular for mobile apps and smart devices. This limitation exists even though mobile apps have been found to be more invasive than browsers and other evidence points to widespread collection of personal data by mobile apps and devices. When these limitations are accounted for, it is likely that online privacy violations are much more widespread than what has been diagnosed.

344. See generally Englehardt & Narayanan, supra note 95, at 1394 (reporting an average of eighteen trackers per website homepage that increased to thirty-four per page when four pages were visited within the website).

345. See Papadopoulos et al., supra note 96, at 154, 158; COMPETITION & MKTS. AUTH., supra note 90, at G27.