NARROWING DATA PROTECTION'S ENFORCEMENT GAP

Filippo Lancieri[*]

Forthcoming, Maine Law Review Volume 74, Issue 1 (2022)

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. 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 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 increase governmental accountability, and antitrust provides examples on how to promote public transparency without sacrificing enforcement capacity.

---

[*]Research Fellow, The George J. Stigler Center for the study of the Economy and the State, UChicago Booth; Post-Doctoral Fellow, ETH Zurich Center for Law and Economics (as of August 2021), JSD Candidate, the University of Chicago Law School.

I would like to thank Lior Strahilevitz, Omri Ben-Shahar, Lisa Bernstein, Adam Chilton, William Hubbard, Brian Leiter, Travis Crum, Ari Ezra Waldman, Spencer Smith, Nicolo Zingales, Julian Nowag, Emilie Aguirre, Erin Miller, Roger Ford, Oles Andriychuk, Angela Daly and participants of 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. All errors are my own.

Table of Contents

INTRODUCTION

The 2016 European General Data Protection Regulation (GDPR)[1] was hailed as ushering 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

[1] General Data Protection Regulation 2016/679, 2016 O.J. (L 119) (EU).

This paper uses interchangeably data privacy, online privacy, data protection and digital privacy to refer to limits on the collection and processing of personal data.

[2] PriceWaterhouseCoopers, *GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey*, PWC (2017), http://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html.

California Consumer Privacy Act of 2018 (CCPA).[3] Yet, years afterwards 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 also point to underwhelming results: since the entering into force of both laws, none of twenty-two independent empirical studies conducted to assess their impact on the ground found meaningful legal compliance. 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 violations of the GDPR;[7] a cookie sweep of 38 large data processors performed by the Irish Data protection authority found that more than 18 months after the GDPR had come into force, 92% did not comply with the law;[8] another report exposed how European data authorities are underfunded

---

[3] See Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N. Y. UNIV. LAW REV. (2019) at 107; Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. (2021), at 1764. By 2020, 142 countries passed some form of data protection legislation, 62 in the past 10 years. Graham Greenleaf & Cottier Bertil, *2020 ends a decade of 62 new data privacy laws*, 163 PRIV. LAWS BUS. INT. REP. 24 (2020).

[4] Adam SATARIANO, *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*, THE NEW YORK TIMES, April 27, 2020, https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html.

[5] See California Proposition 24: The California Privacy Rights Act of 2020, available at https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.

[6] See Part I.B and Annex I below.

[7] Iskander Sanchez-Rola et al., *Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control*, *in* PROCEEDINGS OF THE 2019 ACM ASIA CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 340–351 (2019) at 341; 344-345, (analyzing 2.000 high profile EU websites).

[8] See Irish Data Protection Commission, *Report by the Data Protection Commission on the use of cookies and other tracking technologies* (2020), https://www.dataprotection.ie/sites/default/files/uploads/2020-

and poorly staffed.[9] 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,[10] a survey of the US' 600 largest companies' websites conducted in February 2020 found that even among the richest, most sophisticated American companies, a majority of did not offer CCPA portals for users to access their information—in some important sectors such as Technology, Media and Telecom and Health Services, only 40% of companies did so[11]—and another survey of Business-to-Consumer companies found that these businesses are receiving on average 11 data-related requests per month for every million California consumer identities they hold, meaning that the CCPA was being used by 0.001% of Californian consumers.[12] 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 (i) are there important gaps in the enforcement mechanisms of data protection laws? and, if yes, (ii) what can be done to improve their performance?

This paper helps answer both puzzles. First, it suggests that modern data protection laws largely fail to anticipate how exceptionally large information asymmetries and market power 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 do so, this paper is divided in three parts. Part I briefly outlines the rise of data protection laws in the US and the EU, and reviews the empirical literature on their (so far limited) impact on the ground.

Part II, the core of the paper, explores how Americans and Europeans designed their legal regimes to harness (different) combinations of market

---

04/Report%20by%20the%20DPC%20on%20the%20use%20of%20cookies%20and%20other%20tracking%20technologies.pdf, at 6.

[9] BRAVE, *Europe's governments are failing the GDPR* (2020), https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf, at 3, 6.

[10] Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL STREET JOURNAL, December 12, 2019, https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345.

[11] See PriceWaterhouseCoopers, *CCPA in Financial Services: Early Operational Benchmarks* (2020), https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/california-consumer-privacy-act/ccpa-financial-services.html

[12] Data Grail, *The State of CCPA: Benchmarking CCPA Trends Across Consumer (B2C) Brands* (2021), https://www.datagrail.io/the-state-of-ccpa/. at 4.

forces, tort liability and regulatory enforcement as mechanisms to ensure that companies reflect consumers' privacy preferences. Yet, if consumers cannot understand price/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/services or link them to recognizable legal harm, 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 discover and successfully prosecute 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 unsurmountable. Part III explores how policymakers can learn from the experience with the enforcement of antitrust and anti-corporate fraud laws to design changes that can help narrow this enforcement gap. Focusing on the institutional alternatives to diminish information asymmetries in the enforcement of data protection laws,[13] the paper 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 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. That is because these organizations have the incentives and the capacity to develop the skills to understand the complexity of data collection and denounce violations. In

[13] Antitrust scholars are increasingly focused on tackling the market power of digital platforms. See Filippo Lancieri & Patricia Sakowski, *Competition in digital markets: A review of expert reports*, 26 STANF. J. LAW BUS. FINANCE (2021) for a review of expert reports proposing antitrust and regulatory interventions to diminish the market power of companies such as Google, Facebook, Apple and Amazon.

doing so, they 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 data protection laws can use the resources raised by public fines, grants and *cy pres* awards to properly fund these sophisticated intermediaries, ensuring that they have the necessary means to perform their institutional role while ensuring their independence from industry interests (and deep pockets).

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 countervail that, 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 as a way to encourage insiders to reveal wrongdoing. Data protection laws should learn from their example 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. Data is a key input to national security and to companies competing in a digital world—so governments have legitimate interests to enable the widespread collection of personal data. A combination of governmental interests, the market power of large digital platforms and the complexity/opacity that characterizes many data markets increases the risks that regulators promote industry rather than consumers' interests. An aggravating factor is that 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 absolutely opaque. Antitrust regimes can provide an example on how to design a regulatory framework that increases transparency without sacrificing enforcement capacity.

A brief conclusion follows.

I. THE RISE OF DATA PROTECTION LAWS

A. Data protection on the books

Privacy rights were first developed in the United States and in Europe to safeguard individual dignity, autonomy and preserve some form of information self-determination.[14] A right to privacy naturally includes the protection of personal information that citizens do not want disclosed[15] and

[14] For a summary, see Filippo Lancieri, *Digital protectionism? Antitrust, data protection, and the EU/US transatlantic rift*, 7 J. ANTITRUST ENFORC. 27–53 (2019), at 30.

[15] Lior Strahilevitz, *Reunifying Privacy Law*, CALIF. LAW REV. 2007–2048 (2010), at 2016.

the increasingly important role databases containing personal data started playing in citizens' lives during the second half of the 20th century motivated the expansion of this "right to informational privacy" to incorporate some form of "right to data protection".[16]

The EU was among the first jurisdictions to enact, in 1995, an economy-wide Directive specifically focused on imposing limits on the collection and processing of personal data.[17] Widespread concerns around its lack of effectiveness, however, motivated the passage of the GDPR in 2016.[18] The GDPR grants EU citizens strong rights with regards to their data and also imposes a series of obligations on governments and companies that handle such data.[19] Noteworthy provisions include requirements that data are processed in lawful, fair and transparent manner, that users grant "explicit consent" to enable the collection and processing of data;[20] data minimization and purpose limitation; a right to be forgotten and to data portability; data protection by design and by default; minimum requirements around data security; an obligation that companies perform impact assessments for new technologies or new uses of data and notify users about data breaches; the strengthening of data protection authorities; and a right for citizens to go to Court to directly obtain full compensation for damages associated with violations of data protection laws.[21]

The US lacks a similar economy-wide data protection regime, historically relying on the Federal Trade Commission (FTC) as a de-facto online privacy

---

[16] Fred H. Cate, *The failure of fair information privacy principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 343–379 (2006), at 345. Riley v. California, 134 Ct 2473, 2489 (2014) (concluding that modern day smartphones hold so much personal data that law enforcement needs a warrant to search them). The US led this recognition of a right to data protection by passing the 1970 American Fair Credit Reporting Act and the 1974 Privacy Act, as well as a series of statutes that oversee the collection of specific data such as health or children. At the EU level, 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.

[17] 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.

[18] Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. LAW REV. 1966 (2013), at 1969-1971.

[19] For a summary, see Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union general data protection regulation: what it is and what it means*, 28 INF. COMMUN. TECHNOL. LAW 65–98 (2019).

[20] GDPR art. 7. Consent is one out of six legitimate reasons for the collection and processing of personal data (see art. 6)

[21] GDPR arts. 5, 16, 17, 20, 25, 32-35, 51, 52, 57, 58, 77-83. EU Data Protection authorities can fine companies up to 4% of their worldwide turnover for violations.

regulator.[22] The FTC enforces a regime of *informed consent*, where it mostly ensures that companies disclose to consumers how they collect and process data so that consumers can make an informed decision on whether to accept these terms in a take-it-or-leave-it fashion.[23] The FTC does not impose general limits on how personal data is collected or processed. Except in specific contexts, the agency lacks power to impose fines or other non-voluntary punishments, and the Supreme Court recently greatly curtailed its power to mandate the disgorgement of illegal profits.[24] 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, passed in 2018, is the leading US consumer data privacy regulation.[25] The CCPA is both narrower in scope than the GDPR and reflects fundamental differences in the role privacy plays in society.[26] Nonetheless, it represents a significant expansion over the simple informed consent doctrine. Noteworthy provisions include: stronger notification requirements for the collection and processing of personal data; a right of access and of erasure; a right to object against the selling of personal information; an obligation that companies create "data portals"; a right to data portability; and a direct right of action for damages in cases of data breaches (up to USD 750 per incident or actual damages, whichever is greater). The Office of the California Attorney General holds exclusive powers to enforce most CCPA provisions (with the exception of data breaches) and is also responsible for updating the terms of the regulation.[27]

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 are creation of a subgroup of sensitive personal data, expanded disclosure requirements, 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; a right to limit the use and disclosure of sensitive

---

[22] Lancieri, *supra* note 14, at 32.

[23] Daniel Solove & Woodrow Hartzog, *The FTC and the new common law of privacy*, COLUMBIA LAW REV. 583–676 (2014), at 592.

[24] *Id.* at 604-605 and AMG CAPITAL MANAGEMENT, LLC v. Federal Trade Commission, 593 U.S. (2021).

[25] Chander, Kaminski, and McGeveran, *supra* note 3, at 1769.

[26] Lancieri, *supra* note 14, at 31 (explaining how Europeans treat data as a fundamental right, while Americans treat data as an asset).

[27] CCPA Secs. 1798.100, 1798.105, 1798.110, 1798.125, 1798.130, 1798.150, 1798.155 and 1798.185. Penalties vary between USD 2500 per normal violation and USD 7500 per intentional violation.

personal data; the creation of the California Privacy Protection Agency—a regulatory agency with powers to enact regulations and impose administrative fines—and the determination that 9% of a fund that collects data protection fines should be annually distributed to civil society as grants.[28]

The GDPR and the CCPA, even after amended, are distinct bodies of law that differ in many important manners.[29] Yet, at their core they reflect a general belief that companies were not responsive to (at least some) citizens' preferences for increased control over how their personal data is collected and processed.[30]

The GDPR, for example, was passed partially in response to widespread concerns by European citizens regarding the collection and processing of personal data—67% of Europeans were concerned about not having complete control over their personal data, 70% were concerned about mismatches between information collection and processing and 90% believed it was important to have similar data protection rights across the EU.[31] The Regulation states that a central tenet of data protection is that Europeans know what type of personal data is being collected about them, and how it is processed.[32] It is also expressively 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.[33]

Somewhat similarly, a majority of Americans is concerned about data harvesting by corporations—81% of respondents to a 2019 survey indicate that they lack control over their personal data and that the risks of data collection outweigh the benefits, 79% are concerned that data is being misused.[34] By passing the CCPA, California's legislature explicitly intended

---

[28] CPRA, Secs. 8, 9, 10, 12, 13, 14, 17, 18 and 24. The California privacy protection agency can impose administrative fines of up to USD 2500 per each non-intentional violation of the law and USD 7500 per each intentional violation (CCPA Sec. 1798.155, as amended by the CPRA Sec. 17).

[29] See Chander, Kaminski, and McGeveran, *supra* note 3, at 1746 (comparing the GDPR and the CCPA and concluding that they offer "a fundamentally different regime for data privacy").

[30] GDPR recitals 7 and 11 expressively states that "Natural persons should have control of their own personal data" and that this requires the development of a strong regime to ensure compliance. The CPRA Section (2)(h) states that "People 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."

[31] GDPR recitals 7, 9 and 11; European Commission, *Special Eurobarometer 431 - Data Protection* (2015), at 6-7.

[32] GDPR Recital 39. Chander, Kaminski, and McGeveran, *supra* note 3, at 1750.

[33] GDPR recitals 9 and 11.

[34] See Pew Research Center, *Americans and privacy: Concerned, confused and feeling*

to give California consumers "an effective way to control their personal information" by giving them the right to: (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" and (iv) "to receive equal service and price, even if they exercise their privacy rights".[35] The CCPA was initially slated to be subject to a public vote and the wide expectation over its passage forced the industry to cut a legislative deal.[36] The CPRA—proposed to strengthen these enforcement mechanisms—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 protect their fundamental privacy rights, and that the Government of California must strengthen the enforcement of these rights over time.[37]

Some discount this clear preference for increased data control, asserting that while citizens submit they want increased protection, they trade their personal data for small incentives—an apparent contradiction known as the *privacy paradox*.[38] Yet, the existence of a strong "paradox" has been largely dismissed by more recent literature. While some disconnect between stated privacy preferences and actual personal behavior exists there is "ample and enduring" evidence that consumers recurrently act to protect their privacy in both online and offline scenarios.[39] Indeed, most 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.[40]

That is not to say that every citizen has strong preferences for increased

---

lack of control over their personal information (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf, at 4; and also Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The economics of privacy*, 54 J. ECON. LIT. 442–92 (2016), at 476 (stressing how survey and other evidence indicates that the protection of personal privacy is a leading concern in the US).

[35] CCPA Sec. 2(i).

[36] CPRA, Sec. 2(c) and Chander, Kaminski, and McGeveran, supra note 3, at 1781-82 (describing the disputes surrounding the passage of the CCPA).

[37] CPRA, Sections 2(e)(f)(g) and (h).

[38] Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age*, J. CONSUM. PSYCHOL. (2020), at 737; 749.

[39] *Id.*, at 737. Acquisti, Taylor, and Wagman, *supra* note 34, at 477-478. These range from simple analysis of consumer behavior to surveys, field studies, experiments and other pieces of data.

[40] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 740-744; 750. Numerous processes negatively impact privacy-related rational decision-making in specific circumstances, from extreme information asymmetries to bounded rationality, hyperbolic discounting, resignation, herding or cognitive and behavioral biases.

data protection, nor that these laws are perfect—the GDPR and the CCPA have been praised by many,[41] but criticized by some who believe they harm innovation, replace consumers' preferences by regulators' preferences and stifle free expression.[42] Rather, they reinforce that consumers' persistent call for better data protection should be accounted for.[43] A key reason behind democratically elected governments in California and the EU passing the largely popular CCPA, CPRA and GDPR is exactly because they found a disconnect 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.[44] Societies must ensure that these expenditures actually change market practices.

B. An underwhelming track-record (so far)

Yet, despite these bold ambition, the historical track-record of data protection laws in the EU and the US 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.[45] By one account, almost 75% of EU websites constantly violated the rules without suffering any form of punishment.[46] Across the Atlantic, even governmental authorities have deemed the FTC's lack of powers to fine firms for data-related violations as incapable of ensuring meaningful regulatory deterrence, and this was before the Supreme Court largely gutted its capacity to disgorge illegal profits, leaving the agency almost powerless.[47] A general diagnosis is

---

[41] Schwartz, *supra* note 3, at 102.

[42] see Roselin Layton, *The 10 Problems of the GDPR - Statement before the Senate Judiciary Committee* (2019), https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf

[43] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 750.

[44] See PriceWaterhouseCoopers, *supra* note 2; Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH UL REV 773 (2019), at 777, 803-07 (describing the large "paper trails" created by privacy compliance programs, but that do not materially improve data protection).

[45] See Ronald Leenes & Eleni Kosta, *Taming the cookie monster with dutch law–a tale of regulatory failure*, 31 COMPUT. LAW SECUR. REV. 317–335 (2015), at 329.

[46] Martino Trevisan et al., *4 years of EU cookie law: Results and lessons learned*, 2019 PROC. PRIV. ENHANCING TECHNOL. 126–145 (2019), at 127, 133, 140 (surveying 35.000 popular EU websites and finding that 49-74% placed tracking cookies before receiving consent, a violation of the directive).

[47] A wide review of FTC enforcement actions by the Government Accountability Office concluded that all but a handful of FTC cases ended up in settlements and recommended the development of a strong regulator with the capacity to regulate the market and impose broad civil penalties. United States Government Accountability Office, *Internet Privacy: Report to the Chairman, Committee on Energy and Commerce, House of Representatives* (2019), https://www.gao.gov/assets/700/696437.pdf, at 37. See also AMG

that the Fair Information Privacy Principles (the foundation of legacy data protection regimes in both sides of the Atlantic) have largely failed to achieve their stated goals of aligning consumers' and companies' privacy preferences and increasing data protection.[48] Private self-regulation has not fared any better.[49] That is mainly because these older laws were "*toothless"* or *"paper tigers*".[50]

The GDPR and the CCPA were partially designed to address these shortcomings.[51] Changes in the GDPR, for example, were specifically aimed at bringing data protection closer to antitrust in terms of enforcement, fining capacity and others.[52] Issuing a definitive judgement on the performance of these laws is complicated for at least two reasons: first because these are new and complex regulatory regimes, so it is perfectly possible that enforcement is suboptimal in the first years but improves as regulations mature; second, because many data protection markets are so opaque that reliable evidence for empirical studies is hard to obtain.

Still, these limitations notwithstanding, Annex I contains a comprehensive survey of studies that have independently assessed compliance with the commands of the GDPR and, to a lesser extent, CCPA. The available evidence consistently indicates an underwhelming impact of these new regimes—out of twenty-two independent evaluations, *none* found that these laws led to meaningful increases in data protection. For example, a survey of privacy protection policies of almost 200 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 2000 most-accessed websites found that 92% of them tracked users before providing any notice, 85% maintained or increased tracking even after the users opted-out, violating the Regulation;[53] these findings are backed by another study analyzing the 500 most visited websites in each EU country, finding that the amount of user tracking pre and post-GDPR stayed the same—the study warned against a false sense of

---

CAPITAL MANAGEMENT, LLC v. Federal Trade Commission, 593 U.S. (2021).

[48] Cate, *supra* note 16, at 344.

[49] See, generally, Robert Gellman & Pam Dixon, *Failures of privacy self-regulation in the united States*, *in* ENFORCING PRIVACY 53–77 (2016).

[50] 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 ELEC COM L 70 (2017) at 70, Hoofnagle, van der Sloot, and Borgesius, *supra* note 19, at 93, (also stressing how "the 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).

[51] Schwartz, *supra* note 18, at 1969-1971.

[52] Hoofnagle, van der Sloot, and Borgesius, *supra* note 19, at 67, 92.

[53] Sanchez-Rola et al., *supra* note 7, at 341, 344-345, (analyzing 2.000 high profile EU websites).

GDPR compliance.[54] Even EU authorities are finding widespread violations, as shown by a survey of 38 large data processors performed by the Irish Data protection authority that found that more than 18 months after the GDPR had come into force, 92% did not comply with the law.[55] There is less such independent data on CCPA compliance, but the trend is similar. A February 2020 PwC survey of the websites of the US' 600 largest companies reported that even among these large, very sophisticated companies, a majority did not offer portals for users to access their information.[56] An April 2021 report survey of Business-to-Consumer companies found that these businesses are receiving on average 11 data-related requests per month for every million California consumer identities they hold, meaning that the CCPA was being used by 0.001% of Californian consumers.[57] While not specifically targeted at the CCPA, a September 2020 scan of more than 80.000 of the world's most popular websites by US-based investigative journalism website The Markup found that tracking remains ubiquitous around the world and in the US, even in highly sensitive websites such as those of abortion providers or for victims of sexual violence.[58] Its general conclusions are that third-party tracking is as pervasive now as it was 10 years ago, but it has only "become creepier and more difficult to stop".[59]

These conclusions are backed by other pieces of evidence. After a detailed analysis of companies' internal data protection compliance practices, Professor Ari Waldman described the GDPR and the CCPA as a "house of cards" that is failing to deliver on its promised protections because companies privilege hollow, formal compliance over actual substance.[60] European data protection agencies received more than 275.000 complaints in the first eighteen months since the GDPR came into force, but by then they had issued only 785 fines.[61] Data protection agencies are generally underfunded and poorly staffed: "nearly every European government underfunds its DPA" and regulators in all jurisdictions (but Germany) lack tech specialists.[62] The head

---

[54] Martin Degeling et al., *We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy*, ARXI ARXIV180805096 (2018), at 7-8, 10, 14.

[55] See Irish Data Protection Commission, *supra* note 8, at 6.

[56] PriceWaterhouseCoopers, *supra* note 12.

[57] Data Grail, *supra* note 13. at 4.

[58] See The Markup, *The High Privacy Cost of a "Free" Website* (2020), https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites.

[59] The Markup, *What They Know … Now* (2020), https://themarkup.org/blacklight/2020/09/22/what-they-know-now.

[60] Waldman, *supra* note 44, at 776, 786, 803.

[61] European Commission, *Staff Working Document Accompanying the 2-year GDPR Review* (2020), https://ec.europa.eu/info/sites/info/files/1_en_swd_part1_v6.pdf, at 20;

[62] Brave, *supra* note 9, at 3, 6.

of the Irish data protection agency[63] 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".[64] The head of the German Data Protection authority summarized the situation as: "we have a problem of enforcement";[65] and the head of the Hamburg data protection authority is "completely critical of the enforcement structure of the GDPR (…) the whole system doesn't work".[66] 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 [with the law]".[67] Californians passed the CPRA to fill-in what they identified as clear 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 ground [initially described as very large] is almost certainly growing".[68] 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 enables 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.

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 that is present in many data markets undermine all three mechanisms as drivers of legal compliance.

---

[63] The data protection authority responsible for overseeing Google, Facebook, Apple, Twitter and other large tech platforms.

[64] Satariano, *supra* note 4.

[65] *Id.*

[66] Vincent Manacour & Mark Scott, *Two years into new EU privacy regime, questions hang over enforcement*, POLITICO, 2020, https://www.politico.eu/article/europe-data-protection-privacy-gdpr-anniversary/.

[67] Nandita Bose, *California AG says privacy law enforcement to be guided by willingness to comply*, REUTERS, 2019, https://www.reuters.com/article/us-usa-privacy-california-idUSKBN1YE2C4.

[68] David Erdos, *Feedback on Report on the Application of the General Data Protection Regulation* (2020), https://inforrm.org/2020/05/05/acontextual-and-ineffective-reviewing-the-gdpr-two-years-on-david-erdos/, at 2.

A. Market forces

1. Markets can force companies to reflect consumers' privacy preferences

Markets are the most cost-effective mechanism to ensure that companies reflect consumers' preferences. 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.[69] Exit is a binary choice that reflects the invisible hand working at its best—whenever the quality of a good/service goes down, consumers shift to another supplier. Voice is protest—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, as 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.[70] 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 consumer 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/stop collection of personal data at any point in time.[71] Both laws also establish (different) minimum levels of information

---

[69] 25 ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970), at 4, 21, 30.

[70] 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 (2015), at 2; Adrian Kuenzler, *Direct Consumer Influence—The Missing Strategy to Integrate Data Privacy Preferences into the Market*, YEARB. EUR. LAW (2020), at 6-8 (providing examples for some segments of the digital economy).

[71] Chander, Kaminski, and McGeveran, *supra* note 3, at 1750 (explaining how both the GDPR and the CCPA contain different provisions to increase transparency over data collection and processing); Wolfgang Kerber & Karsten K. Zolna, *The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law* (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3719098., at 18-19 (explaining how the GDPR focuses on addressing information and consumer

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.[72] 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.[73] 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 many times subject to collective action problems.[74] This is particularly true for complex, opaque goods where it is hard to perceive relative quality.

This failure is also true for many markets where data is a key input, where deep information asymmetries, opacity and economic concentration problems prevent meaningful consumer exit and voice.

2. The heightened information asymmetries in data protection

Information asymmetries abound in data protection and negatively impact consumers' capacity to effectively manage online privacy.[75] Privacy policies run for thousands of words and are usually not designed to optimize consumer understanding[76]—a typical user would spend several weeks a year

---

behavior market failures in data markets, but ignoring concentration aspects, what they call a dual market failure).

[72] For example, the GDPR requires that consent should be specific and unambiguous, that whenever the data processing has multiple purposes a specific consent must be given to each purpose and that clear imbalances between the data subject and the controller may imply that consent was not freely given. Heightened consent requirements apply to specific types of sensitive personal data, such as that about sexual orientation, religion and others. The CCPA just requires general notices.

[73] Dowding, *supra* note 70, at 2-3, 10, 25; HIRSCHMAN, *supra* note 69, at 82, 97.

[74] Dowding, *supra* note 70, at 10.

[75] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 742. Acquisti, Taylor, and Wagman, *supra* note 34, at 448.

[76] 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.

just reading them.[77] As a result, these policies—the main technique to inform consumers about the collection and processing of their personal data—are all but ignored.[78]

Even in a distant, 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.[79] Companies use different and obscure means to collect user data, including sign-in/subscription tracking, cookies, web tags, ad tags, pixels, fingerprinting, mobile apps or cellphone tracking.[80] A traditional user is tracked by an average of at least 20 different companies in its regular web browsing alone,[81] and most mobile apps and devices also collect and share a large amount of personal data.[82] For example, Google collects by default a significant amount of personal data from all Android users, some surveys have found that a median app in the Google Play Store hosts trackers by five different companies and 88% of Google Play Apps apparently share back data with Google (43% with Facebook).[83]

Even if users could comprehend the complexity of this data collection

---

COMPETITION AND MARKETS AUTH., ONLINE PLATFORMS AND DIGITAL ADVERTISING MARKET: FINAL REPORT (2020), https://perma.cc/AJ3F-C44Z, at 149.

[77] Alecia M. McDonald & Lorrie Faith Cranor, *The cost of reading privacy policies*, 4 ISJLP 543 (2008), at 563 (estimating that the average American would spend 244h per year (40 min/day) to read all privacy policies it encounters).

[78] The CMA found that that between [0-5%] of Google UK users accessed the company's privacy policies, and 85% of those who did spent less than 10 seconds on the page—probably a misclick. Facebook's had similar numbers of [0-5%] of users accessing its privacy control features over a 28-day period. See Competition and Markets Authority, *supra* note 76, at 173-174.

[79] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 745. Acquisti, Taylor, and Wagman, *supra* note 34, at 463.

[80] For a detailed analysis see AUSTRALIAN COMPETITION AND CONSUMER COMM'N, DIGITAL PLATFORMS INQUIRY - FINAL REPORT (2019), https://perma.cc/3CCL-M3GU, at 130.

[81] Steven Englehardt & Arvind Narayanan, *Online tracking: A 1-million-site measurement and analysis*, *in* PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 1388–1401 (2016), at 10, (surveying 100 random out of the 500 most accessed websites in 16 categories and finding an average of 20 different third-parties tracking users per site).

[82] See Elias P. Papadopoulos et al., *The long-standing privacy debate: Mobile websites vs mobile apps*, *in* PROCEEDINGS OF THE 26TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB 153–162 (2017), at 154, 158; Competition and Markets Authority, *supra* note 76, app. G at 37.

[83] See Reuben Binns et al., *Third party tracking in the mobile ecosystem*, *in* PROCEEDINGS OF THE 10TH ACM CONFERENCE ON WEB SCIENCE 23–31 (2018), at 26; Competition and Markets Authority, *supra* note 76, app. G at 10, app. F at F16.

network, some forms of surveillance can hardly be prevented by consumers alone: data collection mechanisms such as pixels, web bugs and fingerprinting are effectively invisible to the user;[84] Google does not allow Android users to become fully anonymized to advertisers and all major mobile carriers in the US were fined for selling real-time user location data without consent.[85] Many 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-party applications, something that users cannot block.[86] In theory, "*privacy labels*" or other similar alternatives can help consumers by conveying simple information that users can easily process and incorporate in their decision-making. However, these have failed in other markets in general[87] and in data markets in particular,[88] and they cannot address the many externalities involved in data processing.[89] Dark patterns employed in design interfaces can also greatly influence consumer decision-making, sometimes without significant awareness or pushback.[90]

Once this personal information is collected, it can behave as a public good—a non-rival, hardly excludable good that can be easily and cheaply copied and that quickly spreads through a complex web of companies and data brokers.[91] This means that once data has been shared, it is hard to purge

---

[84] Acquisti, Taylor, and Wagman, *supra* note 34, at 463-464.

[85] See *The FCC Fines Wireless Companies for Selling Users' Location Data*, WIRED, (2020), https://www.wired.com/story/fcc-fines-wireless-companies-selling-users-location-data/. Given the cellphones are designed to connect to the network, the only way to not be tracked would be avoid using your 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*, 3 SCI. REP. 1376 (2013).

[86] See Competition and Markets Authority, *supra* note 76, app. G, at 107-8 (explaining the shift and how it enables continued tracking despite decreases in third-party cookies).

[87] See Omri Ben-Shahar & Carl E. Schneider, *The failure of mandated disclosure*, UNIV. PA. LAW REV. 647–749 (2011), at 650-651 (describing how "mandated disclosure is ubiquitous (…) [but] not only does the empirical evidence show that mandated disclosure regularly fails in practice, but its failure is inevitable").

[88] Omri Ben-Shahar & Adam Chilton, *Simplification of privacy disclosures: an experimental test*, 45 J. LEG. STUD. S41–S67 (2016), at 4-5; See also Christine Utz et al., *(Un) informed Consent: Studying GDPR Consent Notices in the Field*, *in* PROCEEDINGS OF THE 2019 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 973–990 (2019), at 974, (showing how consent can be easily manipulated by dark patterns such as the position on the browser and the colors used).

[89] Omri Ben-Shahar, *Data Pollution*, 11 J. LEG. ANAL. 104–159 (2019), at 120, (describing how externalities in data collection prevent private contracting over data from being socially efficient).

[90] Jamie Liguri and Lior Strahilevitz, *Shinning a Light on Dark Patterns*, 13 J. LEG. ANAL. 43-109 (2021).

[91] Acquisti, Taylor, and Wagman, *supra* note 34, 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

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 companies themselves did not anticipate at the time of collection.[92]

In such a context, the CCPA's and the GDPR's sophisticated disclosure and consent obligations cannot wash away the fact that mandated disclosure and other provisions aimed at increasing consumer data awareness have failed. 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 simple simplification attempts have not changed that.[93] Only 29% of Americans know that Facebook owns Instagram and WhatsApp,[94] and only 26% understand that Facebook creates user profiles to target ads.[95] 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 is being sold to a complex network that enables, among others, the US Federal Government to enforce immigration laws or track potential terrorist threats.[96] Uninformed consumers cannot exercise exit nor 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 align consumer privacy preferences. Another problem is that the economic structure of many data markets pushes them to *winner-takes-all* or *winner-takes-most* scenarios where only one or two leading companies thrive. Indeed, a range of reports from expert panels and antitrust authorities from around the world highlighted the role of network effects, large economies of scale and scope

---

to exclude access to certain types of data); Englehardt and Narayanan, *supra* note 81, at 8 (finding more than 81.000 third-party tracking companies, 123 being normally found in navigation).

[92] Acquisti, Taylor, and Wagman, *supra* note 34, at 447.

[93] *Id.* at 479 ("numerous empirical studies have highlighted the limitations of transparency mechanisms [to increase data protection]).

[94] Pew Research Center, *Americans and Digital Knowledge* (2019), https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/.

[95] Pew Research Center, *Facebook Algorithms and Personal Data* (2019), https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/.

[96] See Byron Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL STREET JOURNAL, February 7, 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600; Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, MOTHERBOARD, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

(in part due to network effects), low marginal costs and low distribution costs in inducing concentration in different data markets.[97] Many of these dynamics are connected to the crucial role data itself plays as an input to products and services of the digital economy.[98] More importantly, these conclusions are supported by detailed analysis of particular competitive conditions in different relevant markets, including: (i) search;[99] (ii) social media;[100] (iii) search advertising;[101] (iv) display advertising;[102] (v) mobile app stores and mobile operating systems;[103] (vi) online marketplaces;[104] and (vii) mobile mapping services.[105]

In addition, concentration is growing in the infrastructure/backbone of the internet. Amazon Web Services' commands the internet cloud industry;[106] by some estimates, the Google maps API has a 90% global market share;[107] Google fonts also has a 90% market share;[108] Google tags, including Google Analytics, cover more than 80% of popular websites, while Facebook covers around 40% of the same websites.[109] These are all avenues for companies to collect consumer data. Many companies also obtain sensitive data directly from providers: Google, for example, has direct access to credit card data;[110] research indicates that 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,[111] and 88% of Google Play Store apps transfer data back to Google.[112] For consumers to avoid the collection of personal data due to

---

[97] Lancieri and Sakowski, *supra* note 13, at 10.

[98] Michal S. Gal & Oshrit Aviv, *The competitive effects of the GDPR*, 16 J. COMPET. LAW ECON. 349–391 (2020), at 352.

[99] Lancieri and Sakowski, *supra* note 13, at 56; Adrian Kuenzler, *Advancing Quality Competition in Big Data Markets*, 15 J. COMPET. LAW ECON. 500–537 (2020), at 515 (discussing limits on the exercise of exit and voice in search markets).

[100] Lancieri and Sakowski, *supra* note 13, at 61.

[101] *Id.* at 47

[102] *Id.* at 50.

[103] *Id.* at 37.

[104] *Id.* at 50.

[105] *Id*. at 75.

[106] *Id*. at 56.

[107] Datanyze, *Google Maps API Market Share and Competitor Report*, /market-share/mapping-and-gis--121/google-maps-api-market-share.

[108] Datanyze, *Web Fonts Market Share Report*, /market-share/web-fonts. Google Fonts is a free, open source web fonts websites use to format their websites. 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.

[109] Competition and Markets Authority, *supra* note 76, app. G, at 99-100.

[110] Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales, BLOOMBERG.COM, August 30, 2018, https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales.

[111] Australian Competition and Consumer Commission, *supra* note 80, at 391.

[112] Binns et al., *supra* note 83, at 26

backbone concentration or Business-to-Business deals they would have to all but stop using the internet.[113]

Both the CCPA's and the GDPR's provisions 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 effectively enable consumer exit. While 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 mass migration; and consumers' face a collective action problem to independently organize such migration. In addition, these rights to data portability usually do not include constant portability of update and accurate data, a problem for markets where data half-life is short. As such, simple data portability is unlikely to enhance consumers' exit strategies.

An alternative may be to establish a broader obligation of data interoperability—that is, the automated, constant transfer of data.[114] This solution, however, has its own important shortcomings. First, in the absence of a clear legal mandate, interoperability faces important legal hurdles. For example, US anti-hacking laws allows companies to prevent third-parties from accessing computerized systems and databases.[115] Second, while a legally mandated interoperability may enable consumer exit in some markets, such mandated sharing of personal data can harm personal privacy. Interoperability is complex, costly and research has shown that large bodies of anonymized personal data can be (sometimes easily) reidentified.[116] At the same time, the value of databases is in their volume and complexity and is

---

[113] Gunes Acar et al., *The web never forgets: Persistent tracking mechanisms in the wild*, *in* PROCEEDINGS OF THE 2014 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 674–689 (2014)at 675, (surveying the 100.000 most popular websites in Alexa in 2014 for techniques for online tracking that cannot be stopped by users, like fingerprinting, and finding that even very sophisticated users cannot protect themselves without significant trade-offs in terms of website functionality).

[114] Lancieri and Sakowski, *supra* note 13, at 94.

[115] Facebook, for example, has previously leveraged Federal criminal law to prevent the development of a potential competitor in social networks markets called Power Ventures, whose goal was exactly to create an interoperable meta-social network.[115] See Thomas Kadri, *Digital Gatekeepers*, 99 TEX. LAW REV. (2021) at 17-20

[116] Paul Ohm, *Broken promises of privacy: Responding to the surprising failure of anonymization*, 57 UCLA LAW REV. 1701 (2010), at 1716 (describing how new methods made reidentifying databases much easier); Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, *Estimating the success of re-identifications in incomplete datasets using generative models*, 10 NAT. COMMUN. 3069 (2019), at 2-3, (stating that "numerous supposedly anonymous datasets have recently been released and re-identified" and estimating that their model can leverage on an incomplete database of 1% of the US population to reidentify almost 90% of the population).

time-sensitive. On the one hand, an interoperability system based on consent faces the same collective action challenges of data portability. On the other, a system that relies on differential privacy or other similar protocols to mandatorily share data while protecting privacy will probably be so restricted that it will not effectively promote exit.[117]

Exit and voice only function 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.[118] Facebook, for one, has been condemned in both Germany and Italy for such practices.[119]

Data collection and processing is complex, but a simple example can help convey how information asymmetries and market concentration might prevent consumers from fully exercising exit and voice in data markets. To help contact and tracing programs during the Coronavirus pandemic, the UK government asked pubs to keep a record of consumers' names and cellphones. Restaurant staff then used this information to harass customers by sending messages asking them out on dates[120]—a violation of GDPR requirements such as specific consent for data processing and purpose limitation or of obligations to fully inform consumers under the CCPA. In theory, consumers can rely on markets to punish violating pubs—they can demand that management fires the harasser (voice), or they can change pubs,

---

[117] Daniel Kifer et al., *Guidelines for Implementing and Auditing Differentially Private Systems*, ARXIV PREPR. ARXIV200204049 (2020), at 7, (describing the restricted "privacy budget" that is essential to ensure that personal data remains anonymized in Facebook's Social Sciences One project, probably the world's most advanced employment of differential privacy protocols). Effective anonymization requires restricting access to data, but this restricted access would not help promote competition.

[118] Acquisti, Brandimarte, and Loewenstein, *supra* note 38, at 745-746. Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. LAW J. 39 (2019), at 55 and following (for a detailed report on how Facebook reflected at least some consumer privacy concerns while social media markets were competitive, but stopped doing so once Facebook dominated the market).

[119] Filippo Lancieri & Caio Mario Pereira Neto, *Designing remedies for digital markets: the interplay between antitrust and regulation*, *Forthcoming* JOURNAL OF COMP. LAW AND ECONOMICS (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3704763, at 17; Kerber and Zolna, *supra* note 72; Nicolo Zingales, *Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law*, 33 COMPUT. LAW SECUR. REV. 553–558 (2017).

[120] Donia Waseem & Joseph Chen, *Contact tracing: why some people are giving false contact details to bars and restaurants*, THE CONVERSATION (2020), http://theconversation.com/contact-tracing-why-some-people-are-giving-false-contact-details-to-bars-and-restaurants-143390

forcing the violating bar to go out of business (exit). However, data can be easily shared without the consumer knowledge—any restaurant staff can copy the consumer's name and telephone number and even send it to a friend for almost no cost and without awareness. If consumers provided their information to different pubs, they would not know which establishment to punish unless if revealed by the wrongdoer. Similarly, if only one pub exists in their city, consumers' have no exit options. Owners can ignore complaints and force consumers to choose between discounting the violation or stop going to pubs altogether.

As depicted in detail above, the complexity of data protection markets aggravates these information asymmetries and market concentration concerns—consumers share similar data with multiple providers without even knowing that their data is being collected, and may need to decide between sharing personal data or giving-up the use of smartphones, online search or digital mapping altogether. Under such circumstances, markets will not work as a mechanism to ensure that companies reflect consumers' privacy preferences.

B. Torts

1. Tort liability as a complement to market forces

Tort-based statutory causes of action can complement markets in ensuring that companies account for consumers' preferences without many of the downsides of top-down, command-and-control, public regulation.

Tort liability has many virtues. It continues to directly empower consumers, allowing for decentralized, often low-cost enforcement as damages encourage users to monitor companies and bring violators to court.[121] Moreover, when coupled with fee-sharing arrangements, collective redress mechanisms such as class actions or punitive damages, tort liability can sometimes overcome problems of information asymmetries or the low value of claims. Injunctions and damages awards may force powerful companies—including monopolies—to internalize consumer preferences by compelling or making it unprofitable for corporations to violate the law.[122]

Data protection laws acknowledge this power, establishing/outlining statutory data-related torts that complement markets in promoting consumers' preferences. The CCPA and the GDPR, for example, grant consumers a different combination of individual rights, such as the ones to require data rectification and erasure, a right to opt-out of data sales (in California), the right to be forgotten (in the EU), a right to be notified about

[121] Peter Cane, *Tort law as regulation*, 31 COMM WORLD REV 305 (2002), at 316.

[122] Ben-Shahar, *supra* note 89, at 124 (stressing how tort law can complement private contracting in implementing legal commands).

data breaches, the right to object to the processing of some forms of data, a right to withdraw consent, etc.[123] These are paired with general commands that consumers should be entitled to receive "full compensation" for harms suffered (GDPR) or can obtain injunctions and claim statutory damages against (at least some) violations of the law (CCPA). Because of the GDPR, citizens harassed by pub staff can complement exit and voice by going to Courts to obtain injunctions or collect damages for violations of their data protection rights.

A reliance on statutory torts as a mechanism to enforce consumer preferences, however, faces important shortcomings. First, and importantly, torts suffer from many of the problems around information asymmetries that plague markets: if goods are so complex and opaque that consumers or their attorneys cannot identify violations or cannot prove that it took place, then torts will not work as intended.[124] In addition, torts are also plagued by agency problems in the definition of the tort[125] and Courts sometimes struggle to establish causation, calculate damages or are incapable of addressing negative externalities that go beyond the harm to a single individual.[126]

---

[123] Chander, Kaminski, and McGeveran, *supra* note 3, at 1752 (stressing how the GDPR and the CCPA "share, too, the core elements of a number of additional individual rights (thought they differ in the details)" and listing those rights). For the many differences, see *Id.* at 1755-62. A clarifying note is important here. 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 (Section 1798.150(c)). For the purposes of this article, which is focused on how abstract legal rights are enforced on the ground, this separation can be understood as the law outlining a type of concrete harm that could qualify as a statutory tort (e.g. the ability to sue when a company does not grant a consumer the ability to access and correct information in databases) but removing from the consumer its independent enforcement power through the direct filing of complaints—something that greatly weakens the tort system as an effective enforcement mechanism. This separation is well explained, for example, by Justice Alito majority ruling in Spokeo: "Congress' role in identifying and elevating intangible harm does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants ta person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation." Spokeo, Inc. v. Robins, , 136 S.Ct. 1540 1549 (2016). Indeed, the potential weakness of this dynamic is exactly what this Section explores.

[124] Steven Shavell, *Liability for harm versus regulation of safety*, 13 J. LEG. STUD. 357–374 (1984). at 363 (listing dispersed harms/lack of economic incentives to sue, the discovery of the harm, establishing causality and market power as barriers to effective compensation through tort liability).

[125] Torts may reflect the preferences of only a subset of consumers or even of other parties than consumers. For example, mandatory rules may lead to higher quality/higher price combinations that exclude poorer consumers. See Oren Bar-Gill & Ben Ben-Shahar, *Regulatory techniques in consumer protection: a critique of European consumer contract law*, 50 COMMON MARK. REV 109 (2013), at 113; Waldman, *supra* note 44, at 793 (describing how legal endogeneity is a problem in data protection).

[126] Ben-Shahar, *supra* note 89, at 125.

Market power may also undermine torts as firms design opaquer products and leverage on their deep pockets to hire the best lawyers, conflict key economic consultants, drag-on discovery and generally raise the costs of litigation.

These shortcomings are not inevitable, they depend both on the design of the judicial system and of the statutory tort. Yet, an analysis of the GDPR and the CCPA reveals important obstacles that can prevent statutory torts from becoming an effective data protection enforcement mechanism. That is because lawmakers failed to account for how information asymmetries, market power and other general hurdles undermine data-related statutory torts when designing these laws.

2. Information asymmetries and market power undermine the CCPA

Start with the CCPA. Tort liability has historically been a weak mechanism to safeguard consumers' data protection preferences in the US. Many US Courts refuse Article III standing or actual recovery in privacy violation/data breach lawsuits for lack of a cognizable harm.[127] Privacy class action lawsuits are normally targeted at a couple of statutes that have statutory damages, and even those face many problems around conflicts of interest between lawyers and consumers.[128] While the CCPA (and the CPRA) could have addressed these shortcomings, some of the same information asymmetries that plague exit and voice also negatively impact tort enforcement under the Act.

An effective private litigation system requires consumers to be aware that violations took place. While this may be easier in data security given that new mandatory notifications of data breaches provide consumers with a clear warning, this is not the case for rights that limit the collection and processing of personal data. If information asymmetries, opacity, and externalities prevent consumers from understanding what is being done with their data and triggering exit and voice, they also prevent them from litigating these matters.

The American class action system is structured to circumvent this problem. By grouping claims, it allows for the pooling of resources and increases the sophistication of plaintiffs, enabling the more extensive civil discovery typical of US law. However, the complexity and opacity of data markets and the market power of digital platforms also undermine data protection class actions by enabling companies to impose terms of use that minimize their liability, to design more complex interfaces that hinder characterization of harm and to generally increase the cost of litigation—not only plaintiffs must hire experts and conduct lengthy investigations to discover violations but they do so aware that their counterparty has almost

[127] Solove and Citron, *supra* note 27, at 739, 741; Ben-Shahar, *supra* note 89, at 125.

[128] Marc Rotenberg & David Jacobs, *Enforcing Privacy Rights: Class Action Litigation and the Challenge of cy pres*, *in* ENFORCING PRIVACY 307–333 (2016), at 315.

endless resources to fight the claims.

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, allowing them to draft these terms in a way that hinders or blocks tort lawsuits (for example, by allowing for widespread data collection and processing or by requiring class waivers or mandatory arbitration).[129] The designed complexity and opacity of data collection and processing mean that data harms are neither immediate nor visible[130]—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 can provide courts with guidelines for harm calculation and can 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 no panacea as: (i) they only apply to data breach litigation and not to core data protection rights like the "do not sell my data" feature; (ii) even those data breach claims are overseen by the Attorney General of California, who may take over the case or even simply block consumers from moving forward;[131] and (iii) they still require plaintiffs to prove some actual harm before they can claim the minimum damages.[132] Importantly, the CPRA continues to prevent consumers from directly litigating core data protection rights—in a contradiction, both laws grants users a series of data protection rights, but then do not grant them powers to directly enforcement many of these rights in Courts.

Returning to the simple pub example from above, if consumers do not know that their name and telephone is being illegally shared nor which pub shared their data, they will not file a lawsuit. Even if consumers are aware that it was pub X that shared their information, the small value of potential

---

[129] A practice that is widespread among large US companies. See Imre Stephen Szalai, *The Prevalence of Consumer Arbitration Agreements by America's Top Companies*, 52 UC DAVIS REV ONLINE 233 (2018), at 234 (finding that 81 of Fortune 100 companies used arbitration agreements with connection to consumer contracts by 2018, and 78 included class action waivers); Rotenberg and Jacobs, *supra* note 128 at 313 (discussing how limitations to class actions by class action waivers/mandated arbitration clauses have undermined data protection enforcement); Waldman, supra note 44, at 796, 812 (describing how companies can evade legal liability by modifying terms of use and relying on other forms of hollow compliance).

[130] Ben-Shahar, *supra* note 89, at 125.

[131] CCPA 1798.150(b)(3).

[132] As decided in DOE V. CHAO, 540 US 614 (2004). See Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 NYUL REV 662 (2019), at 682-683, (discussing how expectation damages and other techniques to discourage inefficient breaches in data privacy do not accomplish their goals if breaches of data contracts are difficult to detect, prove or ascertain); Solove and Citron, *supra* note 27 (discussing important legal changes that would be necessary to increase private litigation of data breach harms).

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 pub may also prevent the lawsuit by requiring that before consumers receive drinks they tick an "I agree" box stating, on page thirty, that the consumer consents that its name and telephone may be used for any purposes the pub sees fit; that the consumer waives rights to a class action and agrees to private arbitration to solve disputes. A (very) wealthy pub can hire the best lawyers and economic experts, drag on discovery and appeal decisions all the way to the Supreme Court as a way to further discourage lawsuits. Finally, consumers in a one-pub town may not file claims because they are fearful that the aggravated pub owner will refuse to accept them in the future.

That is a stylized example: most data collection and processing takes place in a more complex and opaquer world that is filled with intermediaries—the consumer would not receive a text message by the pub, but by a call center that bought the information from a marketing agency that bought it from the pub. Nonetheless, even this simple example showcases many important limitations of data protection torts.

Indeed, and reflecting these limitations, even after the CCPA entered into force, new, high-profile data protection class actions lawsuits filed in California did not rely on the Act, but rather on other legislation aimed at protecting the safety of private communications such as Federal Wiretap Act or the California Invasion of Privacy Act.[133]

3. And the GDPR

The GDPR faces different but equally important challenges. Data related tort lawsuits have historically faced larger problems in the EU than in the US—for example, while Directive 95/46 (the pre-GDPR data protection legislation) created a range of specific data protection rights, problems around standing, causality and the calculation of damages have historically prevented consumers from properly enforcing these rights.[134]

While the GDPR brings about significant improvements over the old status-quo, it also missed opportunities to spur a robust personal data-related tort litigation system in the EU.

First, concerns around information asymmetries and limited consumer awareness that plague data-related torts in general may be even more relevant under the GDPR, as European jurisdictions host fewer sophisticated

---

[133] See, for example, two class-action lawsuits filed against Google in July 2020, Case No. 20-3664: Brown et al v. Google LLC et al, , https://www.insurancejournal.com/app/uploads/2020/06/brown-v-google.pdf. and Case No. 3:20-cv-4688: Rodriguez et al v Google LLC et al, , https://www.classaction.org/media/rodriguez-et-al-v-google-llc-et-al.pdf.

[134] Hoofnagle, van der Sloot, and Borgesius, *supra* note 19, at 93.

intermediaries like US data privacy NGOs and class-action plaintiffs and normally lack the extensive civil discovery available in the US.[135] The GDPR enables not-for-profit bodies, organizations or associations that have been constituted specifically for this purpose to represent consumers—it is up to Member States to determine specific rules on who will have standing to file such lawsuits.[136] The Regulation also leaves some margin for discretion in terms of court selection.[137]

Details around who has the power to sue, what are the resources of these organizations, which Courts have jurisdiction and which laws are applicable are key for an effective private litigation system: there is a vast scholarship in the US about strategic litigation and preclusion in class action lawsuits[138] and these strategies are known to preclude effective enforcement of data protection rights in the country.[139] EU consumers have stronger protections against the strategic use of jurisdiction, arbitration and class action waivers.[140] 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 damages" arising from privacy violations.[141] The problem is that the case-law of the European Court of Justice in this area is sparse.[142] Here, again,

---

[135] There are some potential exceptions, like the NYOB organization founded by privacy activist Max Schrems or the La Quadrature du Net, founded by French activists. Even these, however, have limited funding. See discussion below.

[136] GDPR, Art. 80 and recital 142.

[137] GDPR Art. 79 establishes that the lawsuit may be filed before the Courts of the Member State where the company is established or where the consumer resides. Art. 81 and recital 144 establish that when Courts identify multiple proceedings based on a similar fact pattern, parties may request that cases are consolidated by the Court where the first complaint was filed.

[138] Tobias Barrington Wolff, *Preclusion in Class Action Litigation*, 105 COLUM REV 717 (2005) at 746 (discussing conflicts of interest in plaintiff counsels in rapidly securing settlements that preclude the class in exchange for generous fees).

[139] Rotenberg and Jacobs, *supra* note 128, at 316 (providing examples of this problem).

[140] Julian Nowag & Liisa Tarkkila, *How much effectiveness for the EU Damages Directive? On the EU Damages Directive and Contractual Clauses Hindering Antitrust Damages*, 57 COMMON MARK. LAW REV. (2020), at 466, (exploring how the Brussels Regulation and the Unfair Contract Terms Directive protect consumers against contractual clauses establishing mandatory jurisdiction, arbitration and/or denying participation in class actions when these impact the effectiveness of EU laws).

[141] GDPR, Art. 82. Recital 146 complements it by establishing that "the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation".

[142] Johanna Chamberlain & Jane Reichel, *The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation*, 89 MISS LJ (2020), at 8, (stressing how the ECJ has not decided any case on Article 82 and that it will be up to

information asymmetries associated with the complexity and opacity of data protection make it harder for consumers to prove standing, demonstrate causation or calculate damages, 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, in particular (iii) demonstrating causality between the processing of the personal data and damages to the individual involved.[143]

Company's economic power and their associated deep pockets is also another barrier. For example, a previous study on the lack of private litigation under the preceding Directive 95/46 indicated not only that consumers were unaware of most violations, but also that they feared punishment by the large companies that they relied on if they filed complaints.[144] If consumers cannot credibly threaten to file complaints, tort liability will not force companies to comply with their preferences. Data privacy litigation is also bound to be expensive, as lawsuits might involve significant market monitoring, technical preparation and discovery to ascertain when companies' opaque data practices 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.[145] 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/or file lawsuits—it will be up for 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 takes place only *after* the government had found undertakings to be in violation of antitrust laws.[146] Moreover, the EU Damages Directive for competition law violations has so far failed to spur consumer-driven private litigation, which remains largely nonexistent. 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

---

specific Member State law to ensure that the broad principle is indeed effective).

[143] Brendan Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, 7 J INTELL PROP INFO TECH ELEC COM L 271 (2016), at 275; 283 (describing the problems in assessing civil liability in Directive 95/46 and stressing how the GDPR might help by shifting the burden of proof after a demonstration of prima facie harm).

[144] Golla, *supra* note 42 at 72.

[145] Nowag and Tarkkila, *supra* note 140, at 472 (stressing how the small value of awards is an impediment to EU consumer antitrust lawsuits).

[146] *Id.* at 457 (stressing how follow-on antitrust claims are likely the most common in the EU).

nature of data protection laws limits company-driven litigation. Indeed, whenever European online privacy NGOs discover violations, they usually file complaints before EU regulators rather than suing companies in Courts—showcasing the weakness of the tort system.[147]

Tort liability as a mechanism to promote legal compliance will certainly be weaker in a system where private parties are subordinated to regulators than in one relying on mixed public/private litigation. That is because on this subsidiary system the enforcement of legal rights is no longer decentralized and directly in the hands of consumers, but rather in the hands of government regulators. As a result, tort liability risks becoming merely a way to increase the deterrence value of public fines, not 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—the topic of the next section.

C. Regulatory enforcement

1. Command-and-control regulation as a third enforcement mechanism

The use of the government's coercive or fining powers to enforce command-and-control regulations is a third, important mechanism to ensure that markets reflect consumer preferences.[148] Regulatory enforcement represents a decision by governments to remove consumers from the direct determination of quality/prices in markets, replacing them by commands that impose specific obligations, minimum levels of quality, maximum prices, etc. 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 non-compliers.[149] All three are non-trivial, so 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 the legal/regulatory commands.[150]

Online privacy laws have long relied on regulators as complementors to markets and torts to ensure that companies reflect consumer preferences.[151]

---

[147] Nicholas Vinocur, *'We have a huge problem': European regulator despairs over lack of enforcement*, POLITICO, December 27, 2019, https://www.politico.eu/article/we-have-a-huge-problem-european-regulator-despairs-over-lack-of-enforcement/ (describing how EU privacy advocates have been filing complaints before regulators, not courts).

[148] Shavell, *supra* note 124, at 373; Kuenzler, supra note 70, at 18-19.

[149] Cane, *supra* note 121, at 312.

[150] *Id.* at 317.

[151] Directive 95/46 required EU Member State to establish independent data protection authorities and the FTC has concluded hundreds of settlements with companies for legal violations. See Solove and Hartzog, *supra* note 23, at 628 (analyzing 154 FTC privacy

Newer laws further strengthened public enforcement: both the GDPR and the CCPA require public authorities to define the content of many data protection rights and effectively enforce those rights.[152] 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 as of January 2023. All of these agencies are granted powers to order companies to change their behavior and impose billions of dollars in fines for non-compliance.

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 consumers lose their power to establish the content of regulations (as in torts) but they also lose control over when to enforce violations (a governmental employee has discretion to decide when to take action). 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 risks that the system is under-resourced, as governments may refuse to fund the costly and complex bureaucracies necessary to properly enforce the regulations.

These two problems are common to 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 them. Indeed, the regulatory systems created through the GDPR and the CCPA lack different but important institutional solutions that could help alleviate concerns.

2. The risks of regulatory capture in data protection

George Stigler's Nobel Prize winning insight was that regulators' and consumers' preferences may misalign, so that governmental action could protect companies and make consumers worse off. For Stigler, one of the main drivers of regulation is the demand by private, politically powerful interest groups trying to appropriate economic rents.[153] Effective governmental capture, however, is not easy, not least because it requires coordination among industry members who have private incentives to defect or to free ride.[154] The scholarship on regulatory capture has evolved

complaints, a number that has only increased since the article was published in 2013).

[152] Chander, Kaminski, and McGeveran, *supra* note 3, at 1759-61 (comparing the role of regulators in both laws).

[153] Richard A. Posner, *Theories of Economic Regulation*, 5 BELL J. ECON. MANAG. SCI. 335–358 (1974), at 335, 343; George J. Stigler, *The theory of economic regulation*, BELL J. ECON. MANAG. SCI. 3–21 (1971), at 5-7.

[154] Posner, *supra* note 153, at 346; Stigler, *supra* note 153, at 7, 12.

significantly since Stigler wrote his groundbreaking piece.[155] While main important gaps still remain, we now better understand how agents must expend significant 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 over academia, the ability to mobilize stakeholders and control over the human capital required by regulators.[156] 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.

Scholars identified key market characteristics that encourage private capture: (i) the concentration within the industry and the alignment of interests between players (that helps overcome collective action problems); (ii) opacity and information asymmetries between the industry and regulators; (iii) how dispersed the group paying the rent is; (iv) how opaque the rent payment is; and (v) the salience of the topic for the general public.[157] Importantly, this literature indicates that capture is *possible*, not that it *always happens*—the risk increases as the specific industry aligns with the characteristics described above.[158] Political influence is always a matter of degree, and different regulations may well reflect different combinations of public and private interests.

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 increase risks of private capture of these new public enforcement

---

[155] See, generally, Christopher Carrigan & Cary Coglianese, George J. Stigler,'The Theory of Economic Regulation', in THE OXFORD HANDBOOK OF CLASSICS IN PUBLIC POLICY AND ADMINISTRATION (2015); Sam Peltzman, *Stigler's Theory of Economic Regulation After Fifty Years*,https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3785342 (2021). Andrei Shleifer, George Stigler's Paper on Regulation and the Rise of Political Economy, PROMARKET (2021), https://promarket.org/2021/04/28/george-stiglers-regulation-political-economy-capture/

[156] Luigi Zingales, *Towards a political theory of the firm*, 31 J. ECON. PERSPECT. 113–30 (2017), at 122, 126; Luigi Zingales, *Preventing Economists Capture*, *in* PREVENTING REGULATORY CAPTURE: SPECIAL INTEREST INFLUENCE AND HOW TO LIMIT IT (2013).

[157] Zingales, *supra* note 156, at 116-119; Carrigan and Coglianese, *supra* note 155, at 3.

[158] Stigler, *supra* note 153, at 10. Carrigan and Coglianese, *supra* note 155, at 7. The cost of exercising political power against the community increases the more the capture damages the community through rent extraction or the easier it is for the community to organize to defend its interests through civil rights associations, universities, the media, etc.

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.[159] In addition, rent payments in online privacy are both obscure and distributed: data collection is complex, often occurs in the background of regular product/service use and replication and distribution costs are marginal, so 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 is in high demand. Governments, therefore, compete for talent with a profitable, high-paying industry, risking that revolving doors undermine enforcement and that regulatory agencies lack the technical personnel to design an effective data protection regime—the latter has already been documented in the EU.[160]

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. Intelligence agencies' surveillance apparatus rely on the processing of personal data (e.g. communications, location, bank transfers), so that limitations on data collection also mean limitations on how successful these agencies are in doing their work.[161] Both the CCPA and the GDPR, for example, explicitly exempt criminal enforcement and national security from their application[162] 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.[163] Three out of five Commissioners of

---

[159] See Part II.A.3 above. The potential exception is Apple. However, even Apple has been criticized for recurrently putting profits above privacy, such as when the company accepts billions of dollars from Google to secure the default search engine position on Safari—ignoring privacy-friendly alternatives such as DuckDuckGo—or its willingness to share private data as a condition to operate in countries such as China and Russia. It is also being sued for GDPR violations. See Ian Bogost, *Apple's Empty Grandstanding About Privacy*, THE ATLANTIC (2019), https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/; Natasha Lomas, *Apple's IDFA gets targeted in strategic EU privacy complaints*, TECHCRUNCH, November 16, 2020, https://social.techcrunch.com/2020/11/16/apples-idfa-gets-targeted-in-strategic-eu-privacy-complaints/.) Ultimately, Apple may not have incentives to advocate for strong, industry-wide data protection standards, as that would weaken its commercial strategy.

[160] Brave, *supra* note 9, at 3, 6 (finding that almost all EU data protection agencies lack data scientists).

[161] As Richard Posner summarized, "privacy is the terrorist's best friend", Richard A. Posner, *Privacy, surveillance, and law*, 75 UNIV. CHIC. LAW REV. 245–260 (2008), at 251.

[162] CCPA Section 1798.145; GDPR art. 23.

[163] Robert McMillan and Jeff Volz, *Barr Presses Facebook on Encryption, Setting Up Clash Over Privacy*, WALL STREET JOURNAL, October 4, 2019, https://www.wsj.com/articles/attorney-general-calls-on-facebook-to-limit-message-

the newly created Brazilian data protection agency are members of the Brazilian armed forces.[164]

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, help increase the secrecy of the operations—only one backdoor is needed—and are better for future Artificial Intelligence applications.[165] Governments also likely prefer to concentrate compliance in a single company established in their jurisdiction 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.[166] The more personal and non-personal data are key inputs for technological development in the digital era, the more governments concerned with the promotion of national champions will want to increase rather than restrict access to data.[167] This means that governments may have important economic

---

encryption-plans-11570130636.

[164] Angelica Mari, *Military takes over Brazil's National Data Protection Authority*, ZDNET (2020), https://www.zdnet.com/article/military-takes-over-brazils-national-data-protection-authority/

[165] Dakota Foster & Zachary Arnold, *Antitrust and Artificial Intelligence: How Breaking Up Big Tech Could Affect the Pentagon's Access to AI* (2020), at 13, 15, 20 (arguing that "data is a core ingredient in AI development" that bolsters national security, that data protection requirements like "siloed" data can hinder AI innovation and that the potential break-up of large tech companies can negatively impact national security by reducing network effects and deconcentrating data sources necessary for critical AI developments).

[166] China, for example, explicitly combines data and industrial policy to promote their national companies in general and in AI in particular (Hung Tran, *Industrial Policy War - Capitalism with Chinese Characteristics*, FINANCIAL TIMES, September 21, 2019, https://www.ft.com/content/79b242e2-3d21-3bcc-8880-59e6f34e96c4.); in the US, whenever companies like Facebook are faced with potential new regulation, they mention the risk that such protections may displace them in the race against China (Josh Constine, *Facebook's regulation dodge: Let us, or China will*, TECHCRUNCH (2019), https://social.techcrunch.com/2019/07/17/facebook-or-china/). The EU recently joined the fray, with its new "European Strategy for Data" data is predicated on data sharing and the promotion of national players. European Commission, *A European Strategy For Data* (2020), https://ec.europa.eu/digital-single-market/en/european-strategy-data

[167] Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY LAW REV. 639–694 (2013), at 666-667 (stressing how the absence of strong privacy laws was key for the development of internet innovation and the silicon valley). As Facebook's head of Global Affairs stated when pressed about data protection in an interview: "We don't hear so much about China, which combines astonishing ingenuity with the ability to process data on a

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 not only due to increased compliance costs, but also because legislation both restricts access to data and concentrates the remaining data in large providers.[168] 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—disproportionately impacting smaller companies with limited direct interaction with consumers.[169] It is too early to pass a definitive judgment, but different studies have found that some side effects of the enactment of the GDPR has been increased data and market concentration.[170] What is particular about this data protection/concentration dynamic is that industry players may leverage data protection regulations to protect their dominant position by complying with the law.[171] For example, both

vast scale without the legal and regulatory constraints on privacy and data protection that we require on both sides of the Atlantic". Constine, *supra* note 166.

[168] Gal and Aviv, *supra* note 98, at 4 ("identifying seven main parallel and cumulative market dynamics [following the GDPR] that may limit competition and increase market concentration").

[169] *Id.* at 28.

[170] Christian Peukert et al., *European Privacy Law and Global Markets for Data*, 1 CENT. LAW ECON. WORK. PAP. SER. (2020), at 11; 19; Konstantinos Solomos et al., *Clash of the trackers: measuring the evolution of the online tracking ecosystem*, ARXIV PREPR. ARXIV190712860 (2019), at 3, 6, 8 (generally find that Google gained or maintained very high-levels of market share after coming into force of the GDPR); Garrett Johnson, Scott Shriver & Samuel Goldberg, *Privacy & market concentration: Intended & unintended consequences of the GDPR* (2020), at 21-22 (finding that that the GDPR led to an average increase of 17% in market concentration). There is also suggestive evidence that the GDPR led to an almost 31% decrease in the funding of data-intensive startups in Europe vis-à-vis the US (Jian Jia, Ginger Zhe Jin & Liad Wangman, *The short-run effects of GDPR on technology venture investment* (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912, at 6).

[171] Inge Graef, Damian Clifford & Peggy Valcke, *Fairness and enforcement: bridging competition, data protection and consumer law*, 8 INT. DATA PRIV. LAW 200–223 (2018). at 220-22.

Google,[172] Facebook[173] and Apple[174] announced a series of changes to promote or to 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.[175] 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 always hard to identify, but there is growing anecdotal evidence suggesting it has already taken place in online privacy. Professor Waldman has aptly described how privacy laws in the US and the EU are undergoing a process of legal endogeneity that is highly deferential to industry practice, so that regulated agents define what the law means rather than the law constraining what private entities can do.[176] This prevents privacy laws from actually achieving their substantive goals. In the US, there have been multiple reports about how the FTC has been incapable or unwilling to stand up to large tech companies, including by FTC commissioners themselves.[177] In the EU, the European Court of Justice (ECJ)

---

[172] By dropping third-party cookies support in the Chrome browser; limiting the use of double-click IDs that advertisers use for independent monitoring of online ads and restricting third-party access to contextual data. James Hercher, *How We Got Here: A Look Back At The Privacy Changes That Reshaped Google*, ADEXCHANGER (2019), https://www.adexchanger.com/online-advertising/how-we-got-here-a-look-back-at-the-privacy-changes-that-reshaped-google/.

[173] This took place both in 2015 when Facebook restricted third-party access to users' data, and more recently when the company announced a pivot to a "privacy-centered platform"—not one that collects less data, but one that shares as little data as possible with third-parties. Josh Constine, *Facebook Is Shutting Down Its API For Giving Your Friends' Data To Apps*, TECHCRUNCH (2015), https://social.techcrunch.com/2015/04/28/facebook-api-shut-down/. and Ben Thompson, *Facebook's Privacy Cake*, STRATECHERY BY BEN THOMPSON (2019), https://stratechery.com/2019/facebooks-privacy-cake/.

[174] Why Apple's anti-tracking move hurts everyone … but Apple, VENTUREBEAT (2020), https://venturebeat.com/2020/09/12/why-apples-anti-tracking-move-hurts-everyone-but-apple/

[175] Liza Lovdahl Gormsen & Jose Tomas Llanos, *Facebook's Anticompetitive Lean in Strategies* (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3400204, at 68.

[176] Waldman, *supra* note 44, at 776-77, 792, 816-19.

[177] William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ REV 959 (2016), at 1011 (describing criticism of an early Facebook settlement with the FTC). Facebook's stock went up after its 2019 settlement with the FTC, hardly a sign of strong enforcement. Nilay Patel, *Facebook's $5 billion FTC fine is an embarrassing joke*, THE VERGE, 2019, https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke. A review of the FTC's enforcement actions by the Government Accountability Office concluded that all but a handful cases ended up in settlements and recommended more forceful action by a stronger regulator. United States Government

has been a leading EU institution in helping promote citizens' data protection rights by striking down what it saw as faulty public regulations that did not adequately promoted data protection.[178] The ECJ has also previously ruled that EU countries have not safeguarded the independence of their data protection authorities.[179] Other studies have shown that data authorities are reluctant to impose sanctions for violations, preferring to rely on cooperation[180] and, more recently European governments have been accused of using COVID to suspend GDPR rights[181] and of using the GDPR itself as a way to diminish public accountability.[182] There are many complaints from European activists and even other EU regulators that the Irish data protection authority—the leading GDPR enforcer—is dragging its feet on the enforcement of the Regulation because of the importance digital markets to the Irish economy.[183] Facebook famously settled in Ireland partially because

---

Accountability Office, *supra* note 72, at 37. Two FTC commissioners dissented from a 2019 settlement with Google, one claiming that the settlement was below Google's profits with the illegal practice. Rohit Chopra, *DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA In the Matter of Google LLC and YouTube LLC* (2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf.

[178] The decision invalidating the EU-US Safe Harbor was grounded on 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, and the subsequent invalidation of Privacy Shield also affirmed that the European Commission failed to assess whether the data of European citizens would receive adequate protection if transferred to the US. Case C-362/14 - Maximilian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (2015). paras. 88-90; Case C-311/18 - Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2020:559 (2020). paras 184-185, 191.

[179] C-288/12 - Commission v Hungary, ECLI:EU:C:2014:237 (2014); C-614/10 - Commission v Austria, ECLI:EU:C:2012:631 (2012) .

[180] Golla, *supra* note 42, at 73.

[181] Many European governments set-aside data protection concerns in the fight against COVID-19, with Hungary going as far as suspending the applicability of GDPR rights. See Samuel Stolton, *EU data watchdog "very worried" by Hungary's GDPR suspension*, (2020), https://www.euractiv.com/section/data-protection/news/eu-data-watchdog-very-worried-by-hungarys-gdpr-suspension/.

[182] European countries such as Hungary, Poland, Romania and Slovakia have apparently attempted to use the GDPR to harass journalists and NGOs revealing government wrong-doing. See AccessNow, *Two years under the GDPR: an implementation progress report* (2020), https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf, at 17-18.

[183] Nicholas Vinocur, *One Country Blocks the World on Data Privacy*, POLITICO (2019), https://www.politico.eu/interactive/ireland-blocks-the-world-on-data-privacy/.; Vinocur, *supra* note 147; Nicole Kobie, *Germany says GDPR could collapse as Ireland dallies on big fines*, WIRED UK, 2020, https://www.wired.co.uk/article/gdpr-fines-google-facebook.

of its "favorable regulatory reputation"[184] and NYOB, a leading European privacy NGO, has published a scathing letter accusing the Irish regulator of being "structurally biased", cooperating with Facebook to purposefully delay the enforcement of the GDPR as a way to help attract foreign investment.[185] Indeed, the lack of appropriate resources and initiative by Irish regulators has been denounced even by other European data privacy regulators,[186] leading commentators to claim that Ireland is a "safe haven for tech giants".[187]

b. The systems lacks appropriate counterweights

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

Start with civil oversight. As Louis Brandeis rightly stated, "sunshine is the best of disinfectants" when it comes to fighting powerful, vested interests.[188] Data protection is certainly on the spotlight in Europe and, to a lesser extent, in the US. It is possible, then, to design regulatory systems that leverage on this public awareness to offset capture risks. However, data protection agencies in the EU and the US tend to be extremely opaque. The FTC and the California Office of the Attorney General have almost no public information about ongoing investigations. They also hardly supply information on the reasons behind the opening or closing of cases. Similarly, many important EU authorities rely on annual reports, press releases or brief statements to announce the opening or closing of investigations. In particular, many have complained about the obscurity of the Irish and Luxembourg data authorities, probably the EU's most powerful.[189] The Irish Data Protection Commission, for example, does not host even basic transparency mechanisms

---

[184] Karlin Lillington, *Ireland's regulatory reputation encouraged Facebook HQ*, THE IRISH TIMES, September 9, 2015, https://www.irishtimes.com/business/technology/ireland-s-regulatory-reputation-encouraged-facebook-hq-1.2279283.

[185] NYOB, *Open Letter on the Irish Data Protection Commission* (2020), https://noyb.eu/sites/default/files/2020-05/Open%20Letter_noyb_GDPR.pdf., at 3; NYOB is also suing the Irish Data Protection Authority for the same reasons (NYOB, *Irish High Court allows Judicial Review to stop Facebook EU-US transfers*, NOYB.EU (2020), https://noyb.eu/en/irish-high-court-allows-judicial-review-stop-facebook-eu-us-transfers)

[186] Kobie, *supra* note 183.

[187] AccessNow, *supra* note 182, at 14.

[188] LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT - CHAPTER V: WHAT PUBLICITY CAN DO (1914), https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/other-peoples-money-chapter-v

[189] Vinocur, *supra* note 147.

such as a page summarizing the status of ongoing cases or a public agenda for officials.[190] As seen above, European privacy NGOs accused the agency of holding numerous confidential meetings with defendants to advise them on how to comply with the law, withholding most of the information from complainants and from other European regulators.[191] Without transparency there cannot be an effective civil oversight of the Government.

Lawsuits for failure to act are another important mechanism in the fight against private capture.[192] In this area, the GDPR is more advanced than the CCPA, requiring 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[193]—the CCPA (even after CPRA amendments) has no similar provisions. Even the GDPR, however, has important flaws connected with the lack of agency transparency and the fact that regulators retain wide discretion in deciding how to handle complaints—there is minimum judicial oversight[194]—allowing agencies to potentially game provisions and delay cases indefinitely.[195]

Finally, regulatory systems must always thread a fine balance between relying on a single, powerful regulator with the appropriate powers and resources to challenge dominant businesses and creating overlapping enforcement powers, multiplying the number of agents a party has to influence to determine the final outcome of a policy. The GDPR and the CCPA/CPRA adopt different strategies: while the Californian law concentrates all enforcement of non-data breach violations in the California State Attorney General (or, later, the California Privacy Protection Agency), the GDPR foresees enforcement by multiple national data protection authorities and enables "joint investigations" between these agencies as a way to solve potential disputes. While this European dispersion of enforcement power may be welcome as a mechanism to increase accountability, the creation by the GDPR of a one-stop shop system reliant on a "lead

---

[190] As of May 9, 2021.

[191] NYOB, *supra* note 185, at 8-9.

[192] The best example being the SCHREMS I, *supra* note 178, and SCHREMS II, *supra* note 178, cases referenced above.

[193] GDPR Arts. 57(1)(f) and 78(2).

[194] David Erdos, *Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?* (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521372, at 6.

[195] Authorities can simply provide an update that the cases are ongoing, delaying them indefinitely. This seems to have happened in the UK, where 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 outcome of cases. See *Id.* at 8 (quoting Platts v Information Commissioner [2019] UKFTT 2018/0211 (GRC) and Shiel v Information Commissioner [2019] UKFTT 2019/0018 (GRC)).

supervisory authority"[196] combined with a convoluted system of joint-investigations[197] effectively concentrates key EU data protection enforcement in two regulators located in Ireland and Luxembourg[198]—countries that are particularly prone to regulatory capture as they disproportionately benefit from the growth of the digital economy.[199] This is a serious institutional design flaw that all but nullifies the benefits of the multiple enforcer system, as shown by early data indicating that this cooperation mechanism has been ineffective in allowing for effective multi-party investigations[200] and by the widespread denouncing of the 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 a system over-reliant on public enforcement is the potential lack of resources.[201] While this risk is pervasive 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 others.[202] Antitrust and data protection policies share significant concerns around information asymmetries—both competition and online privacy violations are mostly hidden from the public view.[203] Unlike antitrust, however, data

---

[196] GDPR Art. 56(1)

[197] In GDPR joint investigations, a lead authority can either invite others to a joint investigation or non-lead authorities may request the European Data Protection Board ("EDPB") to include them in an investigation. If a conflict between the authorities takes place, the decision by the lead authority prevails unless 2/3 of the 29 members of the EDPB vote otherwise. Even then, the initial lead authority is in charge of adopting the final decision based on the vote (GDPR Arts. 62 and 65).

[198] Erdos, *supra* note 68, at 3. AccessNow, *supra* note 182, at 13.

[199] For example, the Irish fast growing digital sector responds for 13% of national GDP, 26% of exports and 10% of all employment. Irish Business and Employers Confederation, *Brexit and the Irish Technology Sector* (2019), https://www.technology-ireland.ie/Sectors/TI/TI.nsf/vPages/Influence~Working_Groups~data-working-group/$file/TI+Brexit+Impact+Report+WEB.pdf, at 13, 15. As mentioned above, Facebook's Deputy Chief Privacy Officer famously stated that Ireland's "regulatory reputation" is a key reason why the company is based there. Lillington, *supra* note 184.

[200] Erdos, *supra* note 68, at 4. Most authorities have no budget or staff for joint-investigations.

[201] Shavell, *supra* note 124, at 364 (identifying high administrative costs as a key hurdle to the effectiveness of public regulation).

[202] Hoofnagle, van der Sloot, and Borgesius, *supra* note 19, at 67, 92.

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

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 economy-wide: to small and large businesses, non-profit organizations and even individuals.[204] Small, unknown companies can collect and process a significant amount of sensitive personal data—Cambridge Analytica being just one example—and, as the digital economy grows, the jurisdiction of data protection authorities will expand, risking that these agents become regulators of a "law of everything".[205] The FTC, for example, 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.[206]

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/encourage private parties to supply regulators with hard-to-access information.[207] 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 illegal behavior. The CCPA (even after amended by the CPRA) and the GDPR do not incorporate any similar mandatory

---

[204] GDPR Art. 4(2); 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*, EUR. J. RISK REGUL. 1–25 (2020), at 18-19 (stressing how this risks underenforcement in data protection and proposing that regulators privilege actions against large firms).

[205] Nadezhda Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, 10 LAW INNOV. TECHNOL. 40–81 (2018).

[206] Federal Trade Commission, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers* (2013), https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived; Muzayen Al-Youssef, *Bislang vier Strafen wegen DSGVO-Verstößen seit Mai*, DER STANDARD, November 23, 2018, https://www.derstandard.de/story/2000092017999/erst-vier-strafen-wegen-dsgvo-seit-mai.; AEPD case PS/00408/2020, published on 04/30/2021, https://gdprhub.eu/index.php?title=AEPD_-_PS/00408/2020&mtc=today

[207] See, for example, OECD, *Recommendation of the Council concerning Effective Action against Hard Core Cartels* (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0452, at 6, (recommending the establishment of leniency programs that encourage self-reporting of violations as a backbone of an effective cartel detection system).

"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 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 35 to 140 personnel between 2016 and 2020; the 700 staff of the UK's Information Commissioner is now larger than the antitrust division of the FTC.[208] Yet, their workload is all but endless: it took European data protection agencies only 18 months to issue the same amount of EU-wide potential cooperation requests that their antitrust counterparts issued in more than fourteen years (around 2500 investigations);[209] in the first nine months of GDPR enforcement, European data protection authorities received 206.326 notifications of potential violations, closing 37.900 investigations.[210] by November 2019, the number of complaints rose to 275.000—a potential backlog of hundreds of thousands of cases—leading to only 785 fines, most still subject to judicial review.[211] Authorities themselves acknowledged they are overwhelmed with the workload.[212]

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 USD 5 million, enough only to support an

---

[208] Irish Data Protection Commission, *Annual Report - 2019* (2020), https://www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf, at 8; UK ICO, *Information Commissioner's Annual Report and Financial Statements 2018-19* (2019), https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf, at 46.

[209] Between May 2004 and December 2018, European competition authorities notified the European Competition Network about the opening of 2525 antitrust investigations, while European data authorities issued 2542 cooperation requests in just eighteen months. See Commission, *ECN - Statistics*, https://ec.europa.eu/competition/ecn/statistics.html and European Data Protection Board, *2019 Annual Report* (2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_annual_report_2019_en.pdf. at 5, 30.

[210] European Data Protection Board, *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities* (2019), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf, at 12.

[211] European Commission, *supra* note 61, at 20;

[212] Satariano, *supra* note 4.

enforcement staff of 23 lawyers who are also responsible for broader consumer protection.[213] The FTC has acknowledged that lack of resources is undermining its enforcement capacity[214] and prevents the expansion of the agency's 46-person strong data protection team (4% of the agency's total staffing), which had been criticized as insufficient to effectively monitor and enforce data protection laws.[215] Yet, the FTC's annual budget is around USD 330 million, while the guaranteed funding of the California Privacy Protection Agency is only USD 10 million;[216] in the EU, the Irish Data Protection Commission's 2019 budget was EUR 15 million and the Luxembourg's authority EUR 5.5 million.[217] 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]."[218]

Finalizing the stylized pub example, as a third alternative to remedy the violation the aggrieved consumer could complain to a dedicated regulator that its name and phone data had been illegally collected and processed. In this case, however, the consumer cannot enforce the law directly—first it will have to convince a public agent to open an investigation into the matter. The consumer, however, is not aware of which pub shared the data, so the agent has to require the pubs in the areas 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 it can do to accelerate the process. The same public agent, however, oversees data processing in the entire city, so it has to simultaneously handle thousands of other complaints. Pubs also generally refuse to share the information the agent needs to finalize the case, as they profit from it. In addition, the pub industry is responsible for 26% of the country' exports and 10% of its employment, and many pubs settled in that specific jurisdiction because it has somewhat permissive data use laws.[219] The agent, therefore, knows that the government does not want to antagonize that industry—in fact, the agents' boss had meetings with pub

---

[213] Yuri Nagano, *California Attorney General Plans Few Privacy Law Enforcement Actions, Telling Consumers to Take Violators to Court*, SAN FRANCISCO PUBLIC PRESS, May 15, 2019, https://sfpublicpress.org/news/2019-05/california-attorney-general-plans-few-privacy-law-enforcements-telling-consumers-to-tak.

[214] Leah Nylen, *FTC suffering a cash crunch as it prepares to battle Facebook*, POLITICO (2020), https://www.politico.com/news/2020/12/10/ftc-cash-facebook-lawsuit-444468.

[215] Stigler Center, *supra* note 116, at 220.

[216] CPRA Sec. 24.18.

[217] AccessNow, *supra* note 182, at 11.

[218] European Data Protection Board, *supra* note 210, at 5.

[219] The same data for the importance of the digital economy to Ireland. See footnote 194 above.

owners to help understand their data needs. After years, the regulatory agency issues a fine that amounts to 0.1% of what the pub in question earned in profits in the preceding year.[220] The pub 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. Mandates are broad and large information asymmetries and market power significantly increase the public resources needed to enforce the laws and the risks of both private and public capture.

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 (even after the CPRA amendments) and the GDPR have been failing to fully account for how exceptionally large information asymmetries and market power usually found in many data markets undermine markets, torts and regulatory enforcement as mechanisms to ensure that companies reflect consumers' data privacy preferences. As mentioned in Part I above, it is possible that some form of compliance improves as these regimes mature. Yet, past experience shows that this improved compliance is in no way guaranteed.[221] Societies are now spending billions of scarce private and public resources in 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 that they do so in quicker and more cost-effective way.

It is beyond this paper to provide definitive solutions to the multiple and complex issues identified above. First because most of these will be jurisdiction specific, requiring changes to the different laws that regulate public transparency, standing, discovery, causation, the filing of lawsuits for

[220] The first fine issued by the Irish DPA against a leading tech company, Twitter, took almost two years of investigation (despite being a simple, objective case of the company not complying with a 72-hour data breach notification deadline) and amounted to approximately USD 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 , https://social.techcrunch.com/2020/12/15/twitter-fined-550k-over-a-data-breach-in-irelands-first-major-gdpr-decision/.

[221] As seen above, compliance with the Directive 95/46 or the European E-privacy directive has been extremely low, despite their enactment decades ago.

failure to act, etc. (each likely demanding a paper of its own); and second because one cannot rule out that these systems may require a significant rethinking of their fundamental goals.[222] Rather, the objective here is to learn from the way in which more mature regulatory regimes such as antitrust and anti-corporate fraud have tackled the common challenge of large *information asymmetries* undermining legal compliance: if they are not addressed, it is unlikely that any privacy laws will fully deliver on their goals. This focus on information asymmetries is justified because the antitrust community is already actively discussing how to diminish the market power of large digital platforms,[223] but 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/enforcers; and (iii) forcing governmental accountability as a way to diminish risks of regulatory capture.

A. Multiplying monitoring and enforcement resources

Not only the collection and processing of personal data is usually taking place in complex, non-transparent environments, but the widespread collection and easy replicability of these data expands the jurisdiction of online privacy laws. As 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, however, these regimes have been designed to encourage that sophisticated private organizations understand the complexity of corporate practices and denounce violations: for example, a large survey on corporate fraud lawsuits in the US 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;[224] and the majority of US antitrust litigation is private, not public.[225] Data protection laws should be equally designed to

---

[222] See Waldman, *supra* note 44, at 825, discussing other structural changes to privacy laws that would also be important to help promote compliance.

[223] See Lancieri and Sakowski, *supra* note 13, for a general review of diagnosed concerns and potential remedies.

[224] Alexander Dyck, Adair Morse & Luigi Zingales, *Who blows the whistle on corporate fraud?*, 65 J. FINANCE 2213–2253 (2010), at 2225.

[225] United States, *Submission of the United States to the OECD on the Relationship Between Public and Private Antitrust Enforcement* (2015),

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 costs of capturing regulators.

An expansion of these sophisticated private intermediaries, however, requires the availability of appropriate and independent funding. This is currently not the case, as most privacy NGOs and other similar organizations are supported by grants and donations, an unreliable and insufficient source of funding for mass oversight.[226] An effective online privacy regulatory system should ensure a consistent, independent source of funding for these intermediaries, enabling them to invest time and resources in hiring technical personnel, starting complex and potentially unfruitful investigations and/or litigation and better equipping them to resist the temptation of being co-opted by large corporate donations.[227]

There are different mechanisms to help ensure that private parties have incentives to specialize in this field. For example, the US legal system foresees treble damages for antitrust violations as a way to encourage private litigation, something that the Supreme Court has said works as "a chief tool in the antitrust enforcement scheme"[228] that encourages litigants to serve as "private attorneys general".[229] This is certainly an important mechanism to be considered, even if it has limitations and is of difficult acceptance abroad.[230]

A likely more acceptable institutional design alternative that jurisdictions

---

https://www.justice.gov/atr/file/823166/download, at 3.

[226] For example, even the most well-known European NGOs like NYOB and La Quadrature du Net have trouble raising resources. NYOB has so far raised only 66% of its EUR 500.000 funding goal for 2020, La Quadrature's raised only 70% of its 2020 EUR 400.000 goal. See https://support.noyb.eu/funding; https://www.laquadrature.net/en/about/. In the US, the Electronic Privacy Information Center, another large NGO, had a budget of roughly USD 2 million in 2018. See https://www.epic.org/epic/EPIC-2018-Audit.pdf, at 6.

[227] A problem that exists in antitrust. See, Tony Romm, *Amazon, Facebook and Google turn to deep network of political allies to battle back antitrust probes*, WASHINGTON POST (2020), https://www.washingtonpost.com/technology/2020/06/10/amazon-facebook-google-political-allies-antitrust/; Daisuke Wakabayashi, *Big Tech Funds a Think Tank Pushing for Fewer Rules. For Big Tech.*, THE NEW YORK TIMES, July 24, 2020, https://www.nytimes.com/2020/07/24/technology/global-antitrust-institute-google-amazon-qualcomm.html.

[228] Hawaii v. Standard Oil Co., 405 U.S. 251, 262 (1972).

[229] Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc., 473 U.S. 614, 635 (1985).

[230] See, generally, Daniel A. Crane, *Optimizing private antitrust enforcement*, 63 VAND REV 673 (2010). (discussing limitations in American private antitrust enforcement).

should consider is to create a system of recurrent grants that is linked to how well these intermediaries perform their role. These grants would be funded by the resources raised from fines and damages 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[231] or other intermediaries are entitled to a small percentage: (i) of the fines that result from an investigation that started from a private complaint; or (ii) of 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: it can ensure long-term funding for these organizations, rather than large lump-sum awards followed by periods without any resources; it can be implemented without changes that impact the perceived justice of tort law and it directly connects funding to effective monitoring, minimizing administrative costs.

Again, antitrust policies can provide an example on how the indirect method would work. Brazilian antitrust laws establish that fines imposed by the Brazilian competition authority are allocated to a public fund aimed at protecting citizens' diffuse interests—in 2019, the fund raised approximately USD 120 million.[232] This fund is managed by a council composed of seven career civil servants and three civil societies representatives, appointed for a renewable mandate of two-years.[233] 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. In 2019 alone the fund awarded 46, long-term grants. Here, it is also worth mentioning the changes brought about by the CPRA, which are an important step in this direction. Section 18 of the new law foresees that nine percent of the Consumer Privacy Fund that collects CCPA damage awards (and that currently goes mostly to the Californian treasury) will be distributed by the California Privacy Protection Agency as grants to civil society and law enforcers.[234] The three percent that would go to NGOs, however, seems

[231] Such as https://themarkup.org, a non-profit, investigative journalism newsroom focused on investigating large tech platforms.

[232] Article 28, §3 of Law 12.529/11 and the public information on the resources of the fund, available at https://www.justica.gov.br/seus-direitos/consumidor/direitos-difusos/arrecadacao-1

[233] Article 3 of Brazilian Presidential Decree 1.306/94.

[234] Section 18 of the CPRA. The distribution 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

insufficient to bring monitoring resources to levels that can actually diminish the high levels of information asymmetries in data protection.[235] Such levels should be enlarged, and European countries should also adopt similar initiatives.

The direct funding system, on the other hand, could be an expansion of the already common US practice of directing *cy pres* awards in class action lawsuits to privacy NGOs.[236] A problem with these *cy pres* settlements in data protection is the occasional distribution of awards to organizations that are not directly connected to online privacy.[237] To address this, the law could encourage that awards are funneled to the public fund, which would then ensure that *cy pres* resources are distributed more broadly and fairly.

Both proposals have limitations of their own. First, they focus on deterrence rather than victim compensation—a choice justified at a moment when enforcement levels are low, but this could change in the future. Privacy class actions settlements could also continue to be unduly funneled to plaintiffs' lawyers and/or to organizations that do not protect consumer privacy[238] and/or that a public grant system can be diverted to accomplish interests other than what it was initially envisioned.[239] To prevent this, it would be 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 foresee 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 management council. Finally, different jurisdictions should set different 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 on donations, grants and/or awards from tort litigation—would be much more capable of detecting wrongdoing than one overtly reliant on public regulators.

---

and local law enforcement agencies to fund cooperative programs with international law enforcement organizations.

[235] Even if CCPA fines reach unprecedented USD 100 million, this would lead to an annual distribution of USD 3 million dollars, not enough to support many large-scale organizations with lawyers, tech specialists, etc.

[236] COMMITTEE ON DIGITAL PLATFORMS FINAL REPORT, STIGLER CTR. FOR THE STUDY OF THE ECON. AND THE STATE AT CHICAGO BOOTH 23 (2019), https://perma.cc/RWV9-KRL5, at 220.

[237] Rotenberg and Jacobs, *supra* note 128, at 309, 321, quoting Marek v. Lane, 134 S. Ct. 8, 8–9 (2013).

[238] *Id.* at 309.

[239] The Brazilian fund did not award grants for many years as the government earmarked the funds to help diminish the public budget deficit.

B. Bringing data protection violations to light

The information asymmetries between how companies collect and process personal data and what civil society and regulators know about it increase the importance of mechanisms designed to bring violations to the attention of these overseers. A stronger, better-funded civil society will increase monitoring resources. Yet, another comparison with antitrust, anti-corruption/anti-corporate fraud regimes showcases the importance of the regulatory system also encouraging insiders to report illegal behavior through the establishment of a solid whistleblowing program.

Whistleblowers (in particular employees) are key to the discovery of corporate fraud.[240] Antitrust regulators have also long relied on leniency programs—through which companies denounce cartels in exchange for a more lenient prosecution—as a key mechanisms to bring otherwise secret and illegal private deals to light. Indeed, past studies have found that having access to privileged, internal information greatly increases the probability of successfully exposing hidden fraud.[241] Financial incentives associated with the revealing of the fraud also significantly improve the probability of employees exposing wrongdoing and diminish wrong denunciations.[242]

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 solid whistleblowing programs specifically aimed at encouraging the reporting of data protection violations.[243] In particular, it is

---

[240] Dyck, Morse and Zingales, *supra* note 224, at 2225 (surveying 216 high-profile corporate fraud cases in the US and finding employees, non-financial markets regulators, business analysts and the media (sophisticated third parties) responded 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. ACCOUNT. RES. 123–171 (2018) at 128 (reviewing 658 SEC enforcement actions for fraud and finding that "employee whistleblowing plays an integral role in monitoring firm behavior"); OECD, *Detection of Foreign Bribery: The role of Whistleblowers and Whistleblower protection* (2017), http://www.oecd.org/corruption/anti-bribery/OECD-The-Role-of-Whistleblowers-in-the-Detection-of-Foreign-Bribery.pdf. at 3, 11 (stressing the key role whistleblowers play in revealing wrongdoing).

[241] Dyck, Morse, and Zingales, *supra* note 224, at 2215, 2230-31. (Finding that a potential detector without access to internal company data is 15% less likely to blow the whistle). Call et al., *supra* note 240, at 126 (finding that whistleblowers are associated with larger monetary penalties for targeted firms and larger prison sentences for employees).

[242] Dyck, Morse, and Zingales, *supra* note 224, at 2246-47, (finding that whistleblower employees with financial rewards responded for 41% of frauds exposed in the healthcare industry, where there are financial incentives to report cases, versus 14% in other industries without such incentives. Also finding that frivolous corporate fraud lawsuits are lower in the healthcare than in other industries. A potential detector with financial incentives is 27% more likely to reveal significant fraud). OECD, *supra* note 240, at 11.

[243] Both the California and the EU have general whistleblowing protections: in

key that this program:

i. Defines a "whistleblower" broadly to include not only formal employees but also contractors, consultants, former employees, temporary employees, etc.[244] 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;[245]

iii. Allows for potential whistleblowers to obtain confidential advice from the public authority before filing a report. This has been done, for example, both in The Netherlands and in the US, where the SEC created a dedicated, specialized whistleblower hotline to provide guidance to potential corporate-fraud whistleblowers.[246] 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;[247]

iv. Protects the anonymity of whistleblowers.[248] For example, in Austria, corporate-fraud whistleblowers are allowed to create a unique, secure and official mailbox with pseudonym and password to protect their confidentiality while exchanging information.[249] This also allows the

---

California, the California Whistleblower Protection Act, the False Claims Act and California Labor Code Section 1102.5 provide general protections against retaliation for revealing wrongdoing; in the EU, Directive 2019/1937 from October 2019 establishes minimum levels of whistleblowing protection around the Union and states that these laws should include, among many others areas, violations of data protection laws (Article 1(a)(x)). Yet, the translation of these commands to a dedicated data protection program is lagging, to say the least. At the moment of this writing, California has no dedicated data protection whistleblowing program, nor have important EU jurisdictions such as Ireland or Luxembourg. These general provisions also fall short of many recommendations made herein. For example, the EU Directive does not encourage financial rewards that are key for an effective program. See 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 NORD. J. EUR. LAW 38–49 (2019).

[244] OECD, *supra* note 240, at 15.

[245] *Id.* at 4.

[246] *Id.* at 7-8.

[247] *Id.* at 9.

[248] Dyck, Morse, and Zingales, *supra* note 224, 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).

[249] OECD, *supra* note 240, at 10.

authority to provide feedback to the whistleblower and keep it updated about the status of the claim;

v. Provides financial rewards for successful reports. Financial rewards are key to encourage whistleblowing, as employees risk ending their careers for revealing the wrongdoing.[250] These rewards should be large enough to encourage whistleblowing and also should have minimum thresholds, to help prevent frivolous claims. For example, In the US, SEC awards range between 10-30% of the money collected as a result of the whistleblower denunciation, as long as the sanctions are above USD 1 million;[251]

vi. Protects good-faith whistleblowers from retaliation, including broad civil remedies or even punitive damages for whistleblowers that have been retaliated against.[252] Most whistleblowers first report wrongdoing internally to the company, only resorting to regulators whenever companies refuse to take action.[253] The law should make clear that these employees are equally protected and can require that companies have an obligation to forward any serious whistleblower complaints to regulators within a given period. It should also shield good faith whistleblowers when they report wrongdoing to journalists and other private intermediaries that can raise awareness to potential problems; and

vii. Protects whistleblowers from legal/criminal charges regarding slander, violation of trade secrets, corporate espionage and even civil defamation lawsuits that can be used by well-resourced organizations to silence reporting parties.[254]

All of these principles must be adapted to the laws of specific jurisdictions. Nonetheless, a dedicated data protection whistleblower program that incorporates most of these principles would help 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, data policy's heightened risk of capture by private or public interests also reinforces the need for institutional safeguards to protect the public interest.

---

[250] Dyck, Morse, and Zingales, *supra* note 224, at 2251 ("a natural implication of our findings is that the role of monetary incentives should be expanded").

[251] OECD, *supra* note 240, at 11.

[252] *Id.* at 19.

[253] *Id.* at 14.

[254] *Id.* at 11.

Many important data protection agencies such as the those of Ireland, Luxembourg and even the FTC are unjustifiably opaque. 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—sunshine is the best of disinfectants when fighting entrenched private interests.

Again, a comparison with antitrust laws can help showcase a way to improve the design of data protection laws. For example, extensive public disclosure rules have been instrumental in helping understand the role of corporate donations in influencing policy advice in competition policy[255] and multiple reports have suggested enhancing transparency obligations for US antitrust authorities as a way to increase public confidence in regulators and hinder attempts of regulatory capture.[256] Extensive discovery rights have also helped expose many cases of corporate malpractice.[257]

Some antitrust systems have been expressively designed to maximize transparency as a way 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 are confidential.[258] To comply with this legal requirement, 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 version of both private and public documents are freely available on CADE's website, while 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

---

[255] See Wakabayashi, *supra* note 227.

[256] THE FED. TRADE COMM'N AT 100 REPORT—INTO OUR 2ND CENTURY: THE CONTINUING PURSUIT OF BETTER PRACTICES (Jan. 2009) at 119–20; THE NEXT ANTITRUST AGENDA: THE AMERICAN ANTITRUST INSTITUTE'S TRANSITION REPORT ON COMPETITION POLICY TO THE 44TH PRESIDENT OF THE US (2008) at 187; ANTITRUST MODERNIZATION COMMISSION, REPORT AND RECOMMENDATIONS (2007) at 64-65.

[257] Roy Shapira & Luigi Zingales, *Is pollution value-maximizing? The DuPont case*, NBER WORK. PAP. 23866 (2017), at 8 (showcasing how internal DuPont documents exposed at trial where key to discovery of illegal practices by the company).

[258] Article 49 of Brazilian Law 12.529/11.

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 in some key central 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, this structure that 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.[259]

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 to this webpage public versions of new case developments such as statements of scope and indictments (e.g. Statements of Objection) as well as company's responses; and (iii) upload to this webpage public version of opinions/settlements 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, the CCPA, the CPRA and their dozens of international counterparts 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 indicates 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

[259] 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. OECD, *Peer Reviews of Competition Law and Policy: Brazil* (2019), http://www.oecd.org/daf/competition/oecd-peer-reviews-of-competition-law-and-policy-brazil-ENG-web.pdf, at 9-11. 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, beating international peers such as the FTC and the DoJ. CADE, *Cade is awarded the Agency of the Year in the Americas* (2018), http://www.cade.gov.br/cade_english/cade-is-awarded-the-agency-of-the-year-in-the-americas.

protection regulatory regimes are here to stay. Societies must now ensure that these laws lead to meaningful improvements on the ground. This article indicates that narrowing data protection's enforcement gap is not impossible, but it will require better institutional design. Multiplying monitoring and enforcement resources, encouraging that insiders bring violations to light and promoting regulatory accountability are important but initial solutions to help tackle a multi-faceted, 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.

ANNEX I: SURVEY OF THE EMPIRICAL EVIDENCE ON THE GDPR'S AND THE CCPA'S IMPACT ON THE GROUND

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-two independent studies, found meaningful compliance on the ground. In particular, fourteen studies found widespread violations.[260]

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". 92% 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;[261]

ii. A review of the privacy policies of 194 firms before and after the passage of the GDPR finds 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";[262]

---

[260] It is worth noting that many European studies focus on the collection and processing of data through cookies, something that has limitations (as indicated below). Cookies are mostly regulated by the ePrivacy directive. However, Article 7 of the GDPR has reframed what characterizes as effective consent for the collection of personal data, including through cookies. Therefore, these studies find violations of both the ePrivacy directive and of the GDPR. This is backed by European case law, such as the European Court of Justice landmark ruling in case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH, Judgement of the Grand Chamber, ECLI:EU:C:2019:801. See Cristiana Santos, Nataliia Bielova & Célestin Matte, *Are cookie banners indeed compliant with the law? deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners*, ARXIV PREPR. ARXIV191207144 (2019). at 1-2.

[261] Sanchez-Rola et al. *supra* note 7, at 341, 344-345. Importantly, this study included both first and third party tracking.

[262] Davis and Marotta-Wurgler, *supra* note 132, at 667, 699.

iii. A study tracking 1250 top-visited European and US websites before and after the GDPR (February to September 2018) finds only a small decrease in advertising third-party requests, which the authors say they cannot directly link to the GDPR;[263]

iv. a survey of the five most popular Consent Management Platforms (CMPs) used by the UK's 10.000 most accessed websites found that by September 2019 only 11.8% of the UK websites met minimum notice and consent requirements required by law;[264]

v. a study of 1000 randomly selected EU consent notices collected by 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;[265]

vi. another study of 1426 consent banners used by Europe's 22.949 most accessed websites 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. All in all, the study found that 54% of websites surveyed violated legal requirements;[266]

vii. a study of cookie placements in 35.000 popular EU websites after four years of the coming into force of the European e-privacy directive found that between 49% to 74% placed tracking cookies before receiving consent (depending on definition of tracking), a percentage that stayed constant after the entry into force of the GDPR—indicating that both policies were ineffective. It points to a lack of auditing by regulators as a reason behind its failure;[267]

viii. a study analyzing the 500 most visited websites for each EU country found that, even after the GDPR (October 2018), 15% of these websites had no privacy policy, 37% of websites did not comply with cookies consent notice and the amount of consumer tracking pre- and post-GDPR mostly remained the same. The study warned against a false sense of GDPR compliance;[268]

---

[263] Jannick Sørensen & Sokol Kosta, *Before and after GDPR: The changes in third party presence at public and private european websites*, *in* THE WORLD WIDE WEB CONFERENCE 1590–1600 (2019), at 1599.

[264] Midas Nouwens et al., *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*, ARXIV PREPR. ARXIV200102479 (2020), at 6.

[265] Utz et al., *supra* note 88, at 974.

[266] Célestin Matte, Nataliia Bielova & Cristiana Santos, *Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework*, ARXIV PREPR. ARXIV191109964 (2019), at 2.

[267] Trevisan et al., *supra* note 46 at 127, 133, 140.

[268] Degeling et al., *supra* note 54, at 7-8, 10, 14.

ix. Another study of the 27.000 most accessed websites in the EU, the US and Canada found that the coming into force of the GDPR led to a 14.9% drop in the use of third-party vendors, but that this number rebounded to pre-GDPR levels by the end of 2018, potentially because firms became less afraid of enforcement actions;[269]

x. A cookie sweep of 38 large data processors by the Irish Data protection authority found that more than 18 months after the GDPR had come into force, 92% did not comply with the law;[270]

xi. An in-depth study with data covering data from 1 January 2018 to 31 July 2018 from one of the largest online travel agencies and travel meta-search engines find that the GDPR resulted in a reduction of 12.5% in total cookies (not consumers, as 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 increases by 8%, something that should lead to increased ability to predict consumer behavior;[271]

xii. In interesting 2020 analysis of data interconnection agreements and interconnection points Internet Service Providers (a proxy for data transfers) pre and post GDPR. Contrary to expectations, they find a precise zero GDPR effect, meaning that the GDPR has not let to decreases in data traffic that could potentially impact investments in internet networks;[272]

xiii. 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. Their conclusion is that a "substantial proportion of the websites do not comply with the law [GDPR] even at the very basic level";[273]

---

[269] Johnson, Shriver and Goldberg, *supra* note 170, at 14-15.

[270] Irish Data Protection Commission, *supra* note 8, at 6.

[271] Guy Aridor, Yeon-Koo Che & Tobias Salz, *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR*, NBER WORK. PAP. (2020), https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-guy_aridor.pdf, at 3-4, 15-18.

[272] Ran Zhuo et al., *The Impact of the General Data Protection Regulation on Internet Interconnection*, NBER WORK. PAP. 26481 (2020), https://www.nber.org/system/files/working_papers/w26481/revisions/w26481.rev0.pdf at 4, 38.

[273] Georgios Kampanos & Siamak F. Shahandashti, *Accept All: The Landscape of Cookie Banners in Greece and the UK*, ARXIV PREPR. ARXIV210405750 (2021). at 1, 14.

xiv. A detailed survey of GDPR and the 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;[274]

xv. A following study conduct in January 202 analyzed the basis for the collection and processing of personal data by more than 600 European advertisers. The findings "demonstrate the persistence of the advertising industry in non- compliant (with GDPR and ePrivacy Directive) methods for tracking and pro- filing, bundled in often complex and vague presentation of purposes";[275]

xvi. A PwC surveyed the websites of the US' 600 largest companies done in February 2020 found that a majority of these websites did not offer portals for users to access their information;[276]

xvii. A survey by Data Grail, a US 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 11 requests per month. This means that only 0.001% of consumers are exercising their rights. That is despite average cost of almost USD 200,000 per request;[277]

xviii. While not specifically targeted at the CCPA or the GDPR, a September 2020 scan of more than 80.000 of the world's most popular websites by US-based investigative journalism website The Markup found that tracking remains ubiquitous around the world and in the US, even in highly sensitive websites such as those of abortion providers or for victims of sexual violence.[278] Its general conclusions are that third-party tracking is as pervasive now as it was 10 years ago, but it has only "become creepier and more difficult to stop".[279]

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

xix. One study analyzed web tracking by 5100 of the most visited EU websites

---

[274] Santos, Bielova, and Matte, *supra* note 265. at 3, 74.

[275] Célestin Matte, Cristiana Santos & Nataliia Bielova, *Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?*, *in* ANNUAL PRIVACY FORUM 163–185 (2020). at 2.

[276] PricewaterhouseCoopers, *supra* note 12.

[277] Data Grail, *supra* note 14. at 4.

[278] The Markup, *supra* note 58.

[279] The Markup, *supra* note 59.

between September 2017 to April 2019 and finds that the GDPR was correlated with a reduction of 9% in the number of 3rd party tracking cookies for the median website and a 17% reduction in 3rd party HTTP requests. However, it also finds 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 even expanded to more websites;[280]

xx. One study of 110.000 websites between May 2017 and November 2018 estimated that GDPR has led to a 12% decrease in third-party tracking cookies and a (smaller) increase in first-party cookies—what the authors see as evidence that the GDPR may have achieved some data minimization goals. The authors, however, find that 3rd party requests, which can also be seen as a proxy for tracking, rebounded to pre-GDPR levels as companies learnt how to navigate compliance. All in all, the study finds that the GDPR's impacts are potentially more pronounced in antitrust/market concentration than in privacy;[281]

xxi. A rare study comparing permissions for data access in the 50 most downloaded apps of the Android Play Story between March 2017 to December 2018 found a general decrease in the number of permission requests for apps, in particular to access contacts, location and microphone. 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;[282] and

xxii. Finally, one study using Adobe Analytics data for 1084 dashboards finds that the GDPR led to a decrease of 11.7% in page views for European websites and a 13.3% revenue fall for e-commerce websites. This would be partially motivated (6.9-29%) by users do 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 nor impacts on web-tracking, it states both 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 find "modest progress" towards

[280] Solomos et al., *supra* note 170, at 3, 6, 8.

[281] Peukert et al., *supra* note 170, at 21, 24.

[282] Nurul Momen, Majid Hatamian & Lothar Fritsch, *Did App privacy improve after the GDPR?*, 17 IEEE SECUR. PRIV. 10–20 (2019), at 16-17, 19.

GDPR compliance.[283]

Importantly, although 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. This methodology, however, 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 rather by embedding their third-party code in first-party applications.[284] There are even fewer studies addressing legal compliance with regards to equally intrusive but less "transparent" tracking mechanisms such as pixels, tags, fingerprinting, localStorage, 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.[285]

Third, many cookie sweeps also restrict their analysis to homepages, but studies found more pervasive online tracking beyond the homepage.[286]

Fourth, there are few studies looking on how these laws have impacted tracking outside of the browser world, in particular in mobile/mobile apps and smart devices. That is despite the fact that 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.[287]

When considering those, it is likely that online privacy violations are much more widespread than what has been diagnosed.

---

[283] Samuel Goldberg, Garrett Johnson & Scott Shriver, *Regulating Privacy Online: An Economic Evaluation of the GDPR*, (2020), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421731, at 2-3, 18, 26, 34, 38.

[284] Competition and Markets Authority, *supra* note 76, app. G, at 107-8 (explaining the shift and how it enables continued tracking despite decreases in third-party cookies).

[285] Pierre Laperdrix et al., *Browser fingerprinting: A survey*, 14 ACM TRANS. WEB TWEB 1–33 (2020). at 26.

[286] For example, Englehardt and Narayanan, *supra* note 81, at 18, reported an average of 20 trackers per website homepage. When they visited 4 pages within websites for a small subsample, the average number of trackers increased to 34 per page.

[287] Papadopoulos et al., *supra* note 82, at 154, 158; Competition and Markets Authority, *supra* note 76, app. G, at 37.