Gaining or Losing Control? An Empirical Study on the Real Use of Data Control Rights and Policy Implications

Ella Corren[*]

ABSTRACT: Privacy concerns are on the rise, and lawmakers and regulators around the world are responding with widespread legislative action led by the United States and the European Union. The California Consumer Privacy Act ("CCPA") and many other state laws across the United States, together with congressional proposals, the European Union's General Data Protection Regulation, and similar laws in the rest of the world, all provide people with new data control rights. The formal objective of these rights is to provide control over people's personal information, and they include the right to access one's personal information, the right to delete it, and the right to opt-out of its sale to third parties. Data control rights are the centerpiece of all these new laws and the ultimate response we are seeing to concerns about surveillance capitalism. But do data control rights work in practice?

This Article empirically investigates whether consumers use their data control rights. It leverages a unique opportunity to answer this crucial and thus far open question, presented by the CCPA. This Article is based on an original dataset: It collects and analyzes, for the first time, usage metrics reported by firms under a CCPA Regulations requirement.

This Article adds a novel contribution to the discussion about data control rights and the regulation of the information economy more broadly—part theoretical, part empirical, and part normative. First, this Article explores the origins of data control rights and the goals that have shaped them. To study the effectiveness of a law, it is necessary to compare its intended goals and idealized theoretical outcomes with a measurement of the real-world outcomes that the law has generated.

[*] University of California, Berkeley, School of Law, Doctoral Candidate (J.S.D.). Lloyd M. Robbins Fellow; E. David Fischman Scholar. I would like to thank Kenneth Bamberger, Kiel Brennan-Marquez, Hanoch Dagan, Lesley Fair, Yan Fang, David Grewal, Chris Hoofnagle, Thomas Kadri, Christopher Kutz, Peter Menell, Manisha Padi, Daniel Solove, Rory Van Loo, and Lauren Willis for their invaluable feedback and insights. In addition, I am grateful for useful comments provided by the participants of the 2023 Consumer Law Scholars Conference, the 2023 Privacy Law Scholars Conference, and the 2023 Conference on Empirical Legal Studies.

Second, this Article's data analysis reveals that only a tiny fraction of consumers are exercising data control rights. The Article further analyzes different usage trends amongst the various rights and the gap between the results and the idealized theoretical expectations.

Third, this Article argues that normatively it is crucial to measure the real-life effects of the laws that govern the information economy. The Article further proposes ways to enhance current regulatory approaches in light of the California experience.

INTRODUCTION

Privacy concerns have been on the rise for decades, and they are rising still.[1] A torrent of scandals and revelations has exposed that crucial parts of the information economy are very much unknown or misunderstood by the public, to the detriment of individuals, consumers, and society at large.[2] In response, we now face a legislative tsunami across the world, with the United States and the European Union at the forefront. The California Consumer Privacy Act ("CCPA")[3] and many other laws in states across the United States,[4] the most recent bipartisan congressional proposal for comprehensive federal privacy regulation,[5] the European Union's General Data Protection Regulation

1. *See, e.g.*, Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [https://perma.cc/EYE4-PGCX] ("Data-driven products and services are often marketed with the potential to save users time and money or even lead to better health and well-being. Still, large shares of U.S. adults are not convinced they benefit from this system of widespread data gathering. Some 81 [percent] of the public say that the potential risks they face because of data collection by companies outweigh the benefits . . . ."); JOSEPH TUROW, YPHTACH LELKES, NORA A. DRAPER & ARI EZRA WALDMAN, UNIV. OF PA. ANNENBERG SCH. FOR COMMC'N, AMERICANS CAN'T CONSENT TO COMPANIES' USE OF THEIR DATA 2 (2023), https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf [https://perma.cc/9P3K-8ELW].

2. *See, e.g.*, Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 520 (2019) ("As a rule, it appears that Facebook users tend to be deeply ignorant of the ways the company serves (or disserves) them . . . . This is not just an unusually stark asymmetry of information. It is an elaborate system of social control whose terms are more imposed than chosen."); *Protecting Kids Online: Testimony from a Facebook Whistleblower: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, & Data Sec. of the S. Comm. on Com., Sci., & Transp.*, 117th Cong. 1–4 (2021) (statement of Frances Haugen), https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49 [https://perma.cc/336S-QUL9] (providing testimony by a Facebook whistleblower revealing practices that harmed consumers and the public); Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [https://perma.cc/L5C9-G7ZU] (revealing the Cambridge Analytica scandal); Vindu Goel, *Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry*, N.Y. TIMES (June 29, 2014), https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html (on file with the *Iowa Law Review*) (revealing that Facebook conducted a psychological experiment in which it manipulated the feed of over half a million users thereby impacting their emotions).

3. CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2022).

4. *See, e.g.*, Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575–85 (2024); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301–13 (2023); Connecticut Personal Data Privacy and Online Monitoring Act, 2022 CONN. ACTS 22-15 (Reg. Sess.); Utah Consumer Privacy Act, UTAH CODE ANN. §§ 13-61-101–701 (LexisNexis Supp. 2023); Iowa Consumer Data Protection Act, S.F. 262, 90th Gen. Assemb., Reg. Sess. (Iowa 2023); Indiana Consumer Data Protection Act, IND. CODE §§ 24-15-1-1 to 15-11-2 (2023); Montana Consumer Data Privacy Act, MONT. CODE ANN. §§ 30-14-2801 to 2817 (2023); Oregon Consumer Privacy Act, S. 619, 82d Leg. Assemb., Reg. Sess. (Or. 2023); Tennessee Information Protection Act, H.R. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023); Texas Data Privacy and Security Act, H.R. 4, 88th Leg., Reg. Sess. (Tex. 2023); Delaware Personal Data Privacy Act, H.R. 154, 152d Gen. Assemb., Reg. Sess. (Del. 2023).

5. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); Allison Grande, *House Leaders Vow to Push Data Privacy Bill over Finish Line*, LAW360 (Mar. 1, 2023, 10:26

("GDPR"),[6] and similar laws in the rest of the world,[7] all provide new rights for people with regard to their personal information.[8] These rights are called "data control rights" or "privacy rights" because their formal objective is to provide control over people's personal information. Broadly, data control rights include the right to access one's personal information, the right to correct it, the right to delete it, the right to opt-out of the sale of it to third parties, the right to port it to a competitor, the right to have a human in the loop when it comes to automated decision-making, and the right to limit the processing of "sensitive" personal information, among others.[9] Data control rights are the centerpiece of all these new laws, and the ultimate response we are seeing to concerns about surveillance capitalism. But do data control rights work? Until now, we lacked a clear answer.

PM), https://www.law360.com/articles/1580836/house-leaders-vow-to-push-data-privacy-bill-over-finish-line (on file with the *Iowa Law Review*). *See generally* JONATHAN M. GAFFNEY, ERIC N. HOLMES & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 (2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10776 (on file with the *Iowa Law Review*) (summarizing the American Data Privacy and Protection Act and examining the considerations of Congress in passing the Act). While legislative action on the ADPPA had not been completed in the 117th Congress, the ADPPA was reintroduced in the 118th Congress. *See* Grande, *supra*.

6. *See* Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU); *see also* Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 982–84 (2023) [hereinafter Solove, *Limitations of Privacy Rights*] (summarizing the rights conferred by the GDPR and more recently by American state consumer privacy laws); *see generally* Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'NS TECH. L. 65 (2019) (explaining the European Union's General Data Protection Regulation).

7. *See* Solove, *Limitations of Privacy Rights*, *supra* note 6, at 977 ("Individual privacy rights are enshrined at the heart of most information privacy and data protection laws. Countless privacy laws in the United States and worldwide provide individuals with rights in their personal data . . . . Rights are the centerpiece of many privacy laws. Many elements of privacy laws involve mechanisms to ensure that organizations effectively administer these rights." (footnote omitted)).

8. *See, e.g.*, Ari Ezra Waldman, *The New Privacy Law*, 55 UC DAVIS L. REV. ONLINE 19, 21–22 (2021) [hereinafter Waldman, *New Privacy Law*]; Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. 1221, 1223–24 (2022) [hereinafter Waldman, *Privacy, Practice, and Performance*]; Solove, *Limitations of Privacy Rights*, *supra* note 6, at 977; Margot E. Kaminski, *The Case for Data Privacy Rights (Or, Please, a Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385, 388 (2022); Ari Ezra Waldman, *Privacy's Rights Trap*, 117 NW. U. L. REV. ONLINE 88, 89–90 (2022) [hereinafter Waldman, *Privacy's Rights Trap*].

9. *See, e.g.*, CAL. CIV. CODE §§ 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 (West 2022) (creating a right to request information about what is being collected about consumers and whether any such information is being sold or disclosed to third parties; a right to opt-out of the sale or sharing of consumers' personal information; a right, subject to limitations, for consumers to request deletion of personal information collected; a right to correct inaccurate personal information; and a right to limit use and disclosure of sensitive personal information); Council Regulation 2016/679, arts. 12–22, 2016 O.J. (L 119) 1, 39–46 (EU) (providing the right to information, right to access, right to rectification, right to erasure, right to restriction, right to data portability, right to object, and the right to not be subject to automated decisions). Additionally, while consent is not regarded a formal data control right but a separate central principle, it is very close to a data control right in its nature and application. *See* Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551, 597–98 (2023).

The empirical question leading this Article is whether consumers *use* their data control rights. This is a crucial question because these rights have become the core of the legislative solution, crowding out other regulatory approaches,[10] although their effectiveness remains unclear. This is also an open question. The CCPA presents a unique opportunity to empirically study the extent to which consumers use their data control rights. The California regulator has built into the law itself a mechanism that provides evidence of the usage of data control rights by consumers. This Article is based on an original dataset[11]: I collect and analyze usage metrics reported by firms for the past two years under a CCPA Regulations requirement.[12]

The data reveal a disappointing reality: Very few consumers use their rights.[13] But it also raises a host of questions: How should we interpret the results? Is the law accomplishing its goals? Are data control rights working as lawmakers intended? Importantly, the data also invites us to a broader critical question: How can we measure the effectiveness of laws governing the information economy? Thus far, we did not have the proper tools to study the effects of these laws, and the metrics provided by the California regulation are only a first step.

The centrality of data control rights in regulation has been criticized on theoretical and analytical grounds.[14] While many seem to be in consensus on the desirability of these rights, a few scholars have warned against the fixation

---

10. *See* Waldman, *Privacy's Rights Trap*, *supra* note 8, at 98–103.

11. Ella Corren, Gaining or Losing Control? An Empirical Study on the Real Use of Data Control Rights and Policy Implications Dataset (Feb. 18, 2023) [hereinafter Gaining or Losing Control Dataset] (unpublished dataset) (on file with the *Iowa Law Review*).

12. The CCPA Regulations were adopted by the California Attorney General and went into effect on August 14, 2020. *CCPA Regulations*, STATE CAL. DEPT. JUST., https://oag.ca.gov/privacy/ccpa/regs [https://perma.cc/2VFR-Z48R]. A first set of amendments to the CCPA Regulations went into effect on March 15, 2021. *Id.* A second set of amendments to the CCPA Regulations went into effect on March 29, 2023. *California Consumer Privacy Act Regulations*, CA.GOV: CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/regulations/consumer_privacy_act.html [https://perma.cc/VD6Y-X2NC].

13. *See infra* Part II.

14. *See, e.g.*, JULIE E. COHEN, HOW (NOT) TO WRITE A PRIVACY LAW 5 (2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/2CHH-8QW9]; JULIE E. COHEN, BETWEEN TRUTH AND POWER 262–63 (2019); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 426–29 (2018); Waldman, *Privacy, Practice, and Performance*, *supra* note 8, at 1227–28; Waldman, *New Privacy Law*, *supra* note 8, at 38; Solove, *Limitations of Privacy Rights*, *supra* note 6, at 985; Waldman, *Privacy's Rights Trap*, *supra* note 8, at 94–96. For earlier critiques on data control rights focused on notice-and-consent and privacy-as-control, see, for example, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1660–64 (1999); Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1930 (2013) [hereinafter Cohen, *What Privacy Is for*]; Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013) [hereinafter Solove, *Privacy Self-Management*]; Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 818–34 (2000); Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 862 (2000); and Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–26 (2000); see also ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 69–71 (2018) (critiquing the approach to privacy law that is focused solely on the individual and emphasizing privacy's social and collective values); and NEIL RICHARDS, WHY PRIVACY MATTERS 39 (2021) (developing a theory of privacy as rules).

on data control rights and the tunnel vision effects they have on laws, policymakers, and the information economy as a whole.[15] This Article's contribution to the discussion on data control rights and the regulation of the information economy is part empirical, part theoretical, and part normative. The Article continues as follows.

Part I explores the origins of data control rights and the goals that have shaped them. To study the effectiveness of laws, it is necessary to compare their intended goals—what a respective law was set to achieve—with a measurement of the real-world outcomes that the law has generated.[16] If the law does not have clear goals, or if its goals are not easily measurable, it is challenging to study its effectiveness. In the case of laws granting new data control rights, their outcomes and overall success—and to some extent their goals—have thus far been ambiguous and vague. Part I proposes possible answers to the question of what the goal of data control rights is.

Part II then provides an empirical analysis of the CCPA data control rights usage metrics reported by firms. The CCPA instituted a first-of-its-kind reporting requirement, creating a unique opportunity to empirically study the impact of these rights. To the best of my knowledge, this Article presents the first empirical study of data control rights usage that is not based on consumer surveys or experiments but on real-world numbers provided by firms under a legal mandate.[17] I collect and analyze usage metrics reported across two years

15. *See* Solove, *Limitations of Privacy Rights*, *supra* note 6, at 978, 984–93 (arguing that, while data control rights are important, they "are at most capable of being a supporting actor": First, because "[r]ights put too much of the onus on individuals to fight a war they can't win"; second, because invoking data control rights requires an expertise to assess risks, costs, and benefits, that people generally lack; and third, because it is not enough to protect privacy at the level of the individual and neglect a societal solution); Waldman, *Privacy's Rights Trap*, *supra* note 8, at 93–103 (joining Solove's arguments and adding two more lines of critique: an expressive critique—rights-centered privacy laws send the wrong message that privacy is only an individualistic matter and the responsibility for protecting it lies with the individual alone—and a structural critique—sometimes rights are Pyrrhic victories, seemingly solving the problem but actually crowding out better solutions); *see also* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 954–56 (2017) [hereinafter: Hartzog, *FIPs*] (discussing the shortcomings and inadequacies of the Fair Information Practices).

16. Or with a theoretical analysis of its likely implications. For example, if the law prohibits plants from emitting certain discharges with the goal of reducing pollution, we could measure the emissions of plants to verify their compliance with the law, and we could also independently test the air and ground around such plants to verify if the goal of reducing pollution was indeed achieved. We could also analyze the likely implications of the law, and whether, if complied with, it is indeed likely to reduce pollution.

17. For surveys attempting to measure consumers' privacy-enhancing activities, see, for example, Oksana Kulyk, Nina Gerber, Annika Hilt & Melanie Volkamer, *Has the GDPR Hype Affected Users' Reaction to Cookie Disclaimers?*, J. CYBERSECURITY, 2020, at 1, 1–4; Wanda Presthus & Hanne Sørum, *A Three-Year Study of the GDPR and the Consumer*, 14TH IADIS INT'L CONF. INFO. SYS., 2021, at 153, 153–60; Kovila P.L. Coopamootoo, Maryam Mehrnezhad & Ehsan Toreini, *"I Feel Invaded, Annoyed, Anxious and I May Protect Myself": Individuals' Feelings About Online Tracking and Their Protective Behaviour Across Gender and Country*, 2022 PROCEEDINGS 31ST USENIX SEC. SYMP. 287, 287–88; CISCO SECURE, CISCO, BUILDING CONSUMER CONFIDENCE THROUGH TRANSPARENCY AND CONTROL 3 (2021), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf?CCID=cc000742&DTID=odicdc000016&OID=rptsc027438 [https://perma.cc/6DE4-E9WE] (drawing on 2,600 anonymous responses from

by about 130 firms.[18] These metrics pertain to the CCPA's right to know (access) one's personal information,[19] right to delete such personal information,[20] and the right to opt-out of the sale of personal information to third parties.[21]

The CCPA Regulations require businesses that process the personal information of more than 10,000,000 consumers in a given year to report on their website metrics on how many requests to exercise data control rights were made and how many of these requests were complied with or denied.[22] Data collection and analysis present several challenges that I explain and discuss. I analyze the reported metrics and reveal disappointing results for a regime centered around data control rights. By way of illustration, for an overwhelming majority of firms—roughly eighty percent—no more than 1 in 1,000 consumers a year (0.1 percent) have used their rights to know, to delete, or to opt-out.[23] While the results show that the right to opt-out is the most used right—an important insight to regulators—its usage is still very low compared to the entire consumer base, and I discuss why that may be so. I further analyze the main problems with the CCPA's regulatory approach that are revealed by the results—the unclear standard set by the CCPA and the fact that the regulator does not seem to be enforcing the reporting requirement or keeping track of firms' reports.

Part III leverages the empirical results to develop a broader theoretical analysis of data control rights and explores the ramifications of their low usage. I analyze the nature and logic of data control rights, and I argue that the low usage exposes a weak design that is prone to failure. I further argue that the trouble with data control rights is that they do not provide any benefit or protection unless they are actively invoked. Informed by the empirical results, I then explore a more granular account of the effects these rights are supposed to achieve, in theory, and how those expectations are debunked in a reality where their usage is very low.[24]

Part IV offers a normative perspective and future research avenues. The information economy presents a unique and unfortunate irony: It revolves

---

twelve countries); CISCO SECURE, CISCO, DATA TRANSPARENCY'S ESSENTIAL ROLE IN BUILDING CUSTOMER TRUST 3 (2022), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf [https://perma.cc/AUH5-9J7U] (similar).

18. Gaining or Losing Control Dataset, *supra* note 11.

19. CAL. CIV. CODE §§ 1798.100, 1798.110 1798.115 (West 2018). After January 1, 2023, see only CAL. CIV. CODE § 1798.110 and § 1798.115 (West 2022).

20. CAL. CIV. CODE § 1798.105 (West 2018).

21. *Id.* § 1798.120 (West 2018). Beginning on January 1, 2023, the CCPA additionally includes the right to correct inaccurate personal information and the right to limit use and disclosure of sensitive personal information. CAL. CIV. CODE § 1798.121 (West 2022). The usage of these new rights was not yet realized nor measured (metrics on these additional rights will only be available starting July 2024).

22. CAL. CODE REGS. tit. 11, § 7102(a) (2021) ("A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall . . . [c]ompile the following metrics for the previous calendar year . . . .").

23. Gaining or Losing Control Dataset, *supra* note 11.

24. *See infra* Section IV.B.

around information and the great advancements that can be achieved by harnessing information, but there is so little we know about how it really works, the risks it creates, and how people react to its multifaceted manifestations. We need to build a capacity to measure and understand how information extraction and exploitation are done "in the wild," how people react to data-extractive processes, and how firms implement and comply (or not) with various requirements. We need all that to better understand what lawmakers are actually achieving and what more can be done.[25] While the CCPA's reporting requirement yields some visibility into the impact of data control rights, there is still much that is unknown and difficult to measure. The metrics studied in this Article evoke curiosity for further data and demonstrate the potential of gaining visibility into the impact of privacy laws and other laws governing the information economy by requiring firms to report real-world data. I argue that, normatively, it is crucial to measure the actual effects of laws governing the information economy, and I propose ways to enhance current regulatory approaches in light of the CCPA experience.

I. THE ORIGINS AND GOALS OF DATA CONTROL RIGHTS

To study the efficacy of laws, it is necessary to determine the intended goals of the law in question and then juxtapose those goals against the law's real-world outcomes. This Section proposes possible answers to the question of what the goal of data control rights is.

A. POWER BALANCING

What is the goal of data control rights? One possible answer is that data control rights aim to provide consumers and individuals with means to protect themselves in the waging war over the capitalization of information by transferring some power from firms to consumers. Until recently, all consumers had were timid "privacy policies" providing a veneer of protection and the dormant power to either consent to or decline a transaction.[26] But now the

25. *See also* SABA CHINIAN, PRIVACY LEGISLATION ON THE GROUND: EFFECTS OF AND RESPONSES TO THE GDPR AND CCPA 1 (2023) ("The GDPR and CCPA are the most consequential data information regulations since the development of intellectual property law. But from a long-term perspective, the GDPR and CCPA are ultimately 'first drafts' in privacy protection.").

26. *See also* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019) ("Consent is the foundation of the relationships we have with search engines, social networks, commercial web sites, and any one of the dozens of other digitally mediated businesses we interact with regularly."); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016) ("[A] second hallmark of modern American privacy law, [is] its reliance on a control-based regime of 'notice and choice.' Under this arrangement, terms are hidden in the fine print of legal notices virtually no one reads, and there is as little meaningful choice as in old-fashioned consumer adhesion contracts."); Solove, *Privacy Self-Management*, *supra* note 14, at 1880 ("Consent legitimizes nearly any form of collection, use, or disclosure of personal data"); Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 596 (2024) ("Consent plays a profound role in nearly all privacy laws. . . . Most privacy consent is a fiction. When the law allows dubious or nonexistent consent to masquerade as valid consent, it grants unwarranted legitimacy to data collection, use, and disclosure."); Joseph Turow & Chris Jay Hoofnagle, Opinion, *Mark*

regulation over the information economy is booming, and it is arming consumers with weaponry—data control rights—against data-intensive firms.[27] The power-balancing answer fits history. The origins of data control rights go back several decades: The idea to empower individuals vis-à-vis data-intensive organizations—be it the government or firms in the market—through the regulatory provision of data control rights dates back to the 1970s.[28] The earliest example in the United States is the Fair Credit Reporting Act ("FCRA"), which was passed in 1970.[29] The FCRA provided individuals with several rights, including the right to access personal data maintained by credit reporting firms, and the right to correct it.[30]

In 1973, the U.S. Department of Health, Education, and Welfare ("HEW") published a thoughtful report[31] which proved highly influential over the years and paved the way for data control rights' centrality. The report responded to a "public concern about the issues posed by automation of personal-data record-keeping operations."[32] In response, the report proposes "[a] [r]edefinition of the [c]oncept of [p]ersonal [p]rivacy,"[33] based on the principle of "mutuality."[34] Essentially, what mutuality means is balancing the relationship between the powerful data processor and the weaker individual: The data processor should not be the only decision-maker in the matter of the individual's data and privacy.[35] Based on notions of fairness and due process,[36] mutuality suggests that the individual should also have a role, and a measure of control, over their own privacy and personal data.[37]

Zuckerberg's Delusion of Consumer Consent, N.Y. TIMES (Jan. 29, 2019), https://www.nytimes.com/2019/01/29/opinion/zuckerberg-facebook-ads.html (on file with the *Iowa Law Review*) ("Use of personal information is a serious issue to the American public. People consent because they have no choice."); Chris Jay Hoofnagle, Aniket Kesari & Aaron Perzanowski, *The Tethered Economy*, 87 GEO. WASH. L. REV. 783, 795 (2019) (criticizing how "courts bind consumers to license provisions, terms of use, and privacy policies on the basis of constructive notice."). *See generally* Corren, *supra* note 9; Waldman, *New Privacy Law, supra* note 8; Waldman, *Privacy, Practice, and Performance, supra* note 8; Solove, *Limitations of Privacy Rights, supra* note 6; Waldman, *Privacy's Rights Trap, supra* note 8.

27. *See* sources cited *supra* note 8; Solove, *Limitations of Privacy Rights, supra* note 6, at 977 ("Privacy laws have always relied heavily on rights, and the trend is increasing.").

28. *See, e.g.*, Waldman, *Privacy, Practice, and Performance, supra* note 8, at 1225.

29. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681b (2018).

30. *See id.* §§ 1681j, 1681i; *see also* Solove, *Limitations of Privacy Rights, supra* note 6, at 979–80 (discussing the FCRA's inclusion of several individual privacy rights).

31. *See generally* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973) [hereinafter HEW REPORT].

32. *Id.* at iii. (displaying Willis H. Ware's letter dated June 25, 1973).

33. *Id.* at 38.

34. *Id.* at 39–41.

35. *Id.* at 40.

36. *Id.* at 40–41; *see also* Kaminski, *supra* note 8, at 386 ("These rights aim to establish a kind of data due process for individuals whose information is gathered, held, processed, and used by often powerful entities").

37. HEW REPORT, *supra* note 31, at 40–41; Solove, *Limitations of Privacy Rights, supra* note 6, at 977. Prior to the HEW Report, Alan Westin is considered to have pioneered the privacy-as-control theory. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). Warren and Brandeis

This type of control was translated into individual rights.[38] The idea was to empower individuals by granting them rights, such as the right to know that data is being collected and used and the right to access such data. Indeed, the purpose of the "mutuality" principle was to empower the individual from zero to something but not from zero to everything. The individual is not provided with full control or even half control. The individual is, at best, reactive; they do not decide what data is collected or how it is used or transferred, or to whom.[39] That is because the mutuality principle relies on a crucial default assumption: Personal data will be, and should be, collected, used, and disseminated.[40] This train will not be stopped in its tracks. That was evidently true in the 1970s, and it is even more so now.

Therefore, the HEW Report's motivation and rationale for data control rights were not that they would solve, decide, or prevent the privacy struggle between the individual and the data processor—i.e., shield the individual from privacy harms to begin with—but rather to provide the individual with empowering tools so they can *participate* in the struggle, but on a fair basis—i.e., provide the individual with a sword. The HEW Report proposed the following rights: the right to know,[41] the right to access,[42] the right to prevent repurposing of personal data without consent,[43] and the right to correct.[44] It also proposed some general requirements for organizations processing personal data based on internal compliance mechanisms.[45]

The HEW Report's original set of proposed data control rights has proven to be a beacon to subsequent legislators and regulators in the United States and around the world.[46] It set a model for best practices, known as the Fair

famously coined that privacy is the right of the individual to decide when "to be let alone" and to control the existence of one's public representations. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193, 198, 218 (1890).

38. But see sources cited *supra* note 14 for a critique on this notion of privacy-as-control.

39. HEW REPORT, *supra* note 31, at 40 ("[R]ecords of personal data usually reflect and mediate relationships in which both individuals and institutions have an interest and are usually made for purposes that are shared by institutions and individuals. In fact, it would be inconsistent with this essential characteristic of mutuality to assign the individual record subject a unilateral role in making decisions about the nature and use of his record. To the extent that people want or need to have dealings with record-keeping organizations, they must expect to share rather than monopolize control over the content and use of the records made about them.").

40. *Id.* at 39–40 ("Use of a record about someone requires that its contents be accessible to at least one other person—and usually many other persons. Once we recognize these characteristics of records, we must formulate a concept of privacy that is consistent with records. . . . An important recognition is that privacy, at least as applied to record-keeping practices, is not inconsistent with disclosure, and thus with use.").

41. *Id.* at 41, 57–59, 62–63.

42. *Id.* at 59.

43. *Id.* at 41, 61.

44. *Id.* at 41, 63.

45. *Id.* at 41, 53–57.

46. *See, e.g.*, Robert Gellman, *Willis Ware's Lasting Contribution to Privacy: Fair Information Practices*, 12 IEEE SEC. & PRIV. 51, 51 (2014) (noting that these notions have become "the most important single concept in privacy all around the world"); Hartzog, *FIPs*, *supra* note 15, at 957–58; *see also* Solove, *Limitations of Privacy Rights*, *supra* note 6, at 980 n.14 ("A year earlier, a similar

Information Practice Principles ("FIPPs"). During the 1970s and 1980s, the FIPPs were recognized and adopted across both sides of the Atlantic.[47] In 1980, the Organization for Economic Cooperation and Development ("OECD") adopted the FIPPs in an expanded version of eight principles,[48] which was embraced worldwide.[49] Subsequently, the 1995 European Union Data Protection Directive,[50] and its 2016 successor, the GDPR,[51] were both based on the FIPPs,[52] as was California's 2018 CCPA. Now, the FIPPs "are synonymous with data protection all over the world" and form the basis of most privacy laws worldwide, with the European Union's adequacy requirements for cross-border data exchanges contributing to that as well.[53]

At the time of the HEW Report's publication in 1973, it reflected perhaps the most advanced and comprehensive vision for privacy regulation.[54] It is, therefore, striking to see how little has changed and how much the HEW Report is still relevant and representative of the regulatory approach today. This is evident from recent laws like the CCPA. Part of the California Attorney General's website is dedicated to informing the public about the CCPA.[55] This information is exclusively focused on those data control rights that the CCPA

---

report by the Younger Committee in Great Britain, articulated a set of ten principles, many of which were similar to the HEW principles, although none of the Younger principles were cast in terms of providing rights to individuals." (citing Robert Gellman, Fair Information Practices: A Basic History 5–6 (Apr. 6, 2022) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020 [https://perma.cc/6NAC-QL8S])).

47. *See* Gellman, Fair Information Practices: A Basic History, *supra* note 46, at 8 n.11; COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 99 (1992). The FIPPs were also "the foundation for the U.S. Privacy Act of 1974." Hartzog, *FIPs*, *supra* note 15, at 957.

48. *See generally* ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (Sept. 22, 1980).

49. *See* Hartzog, *FIPs*, *supra* note 15, at 958 ("The OECD Privacy Guidelines are now the most commonly cited version of the FIPs. . . . There are now more than 100 countries with data privacy laws and most of them are built upon most or all of the minimum fair information practices specified by the OECD." (footnote omitted)).

50. *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

51. *See* Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

52. Hartzog, *FIPs*, *supra* note 15, at 955–56.

53. *Id.* at 954; *see also* GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES 5–10 (2014) (noting the importance of data protection principles, the OECD Guidelines, and the EU's Data Privacy Directive in the formation of data privacy laws); Christopher Wolf, *Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers*, 43 WASH. U. J.L. & POL'Y 227, 235–42 (2013); Daniel Susser, *From Procedural Rights to Political Economy: New Horizons for Regulating Online Privacy*, *in* THE ROUTLEDGE HANDBOOK OF PRIVACY AND SOCIAL MEDIA 281, 282–83 (Sabine Trepte & Philipp Masur eds., 2023).

54. *See* HEW REPORT, *supra* note 31, at 167–77 app. B (surveying and comparing contemporary privacy laws around the world); *supra* note 46 and accompanying text (discussing the earlier Younger report in Great Britain).

55. *See California Consumer Privacy Act (CCPA)*, STATE CAL. DEP'T JUST. (Mar. 13, 2024) [hereinafter California AG Website], https://oag.ca.gov/privacy/ccpa [https://perma.cc/LJ6B-8FRS].

has created and the "control" that they provide to individuals.[56] Even when other parts of the CCPA are mentioned they are tied to facilitating the provision of CCPA's data control rights and not much more.[57] The California Privacy Protection Agency has a similar webpage highlighting individual data control rights above all else.[58]

As its legislative history shows, the CCPA was always focused on rights and the control they purportedly provide to individuals.[59] The California ballot initiative that provided the original language of the CCPA discusses five goals for the law, four of them revolving around individual data control rights (as it were, the right to know what categories of personal information firms are collecting, the right to know whether and to whom firms are selling or disclosing personal information, the right to opt-out, and the right not to be discriminated if an individual has used any of their data control rights).[60] The California Privacy Rights Act—CCPA's major amendment—has similar goals and it creates additional individual rights, increasing their overall significance.[61]

B. SOLVING A DEFINITIONAL PROBLEM

Beyond the power-balancing goal and its successful legacy, there is another—perhaps lesser told, but fuller—answer to the question of what the goal of data control rights is. I will call it the "privacy ill-defined" answer. Under this view I argue that data control rights are tasked with solving the puzzle of *defining privacy*—but it is doubtful they can succeed at that.

---

56. *Id.* ("The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control . . . . This landmark law secures new privacy rights for California consumers . . . . In November of 2020, California voters approved Proposition 24, the CPRA, which amended the CCPA and added new additional privacy protections . . . . [now] consumers have [additional] new rights . . . .").

57. *Id.* ("Businesses that are subject to the CCPA have several responsibilities, including responding to consumer requests to exercise these rights and giving consumers certain notices explaining their privacy practices.").

58. *Id.*

59. While the CCPA includes other obligations and requirements, individual rights are at the center of the law, and they reflect its organizing principle. *See, e.g.*, Solove, *Limitations of Privacy Rights*, *supra* note 6, at 983 ("Although [American state privacy] laws have several other non–rights-based provisions, many of these requirements involve the administration of rights. The clear center of gravity in these laws is providing rights for consumers.").

60. *See* Letter from Mary Ross to Initiative Coordinator, Off. of the Att'y Gen. 3–4 (Nov. 17, 2017), https://www.oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf [https://perma.cc/6KCQ-ZVMK] (submitting amendments to the ballot initiative to create the California Consumer Privacy Act and outlining the purpose and intent of the proposed law). The fifth goal pertained to safeguarding consumers from security breaches. *Id.*; *see also* Letter from Alastair Mactaggart, Bd. Chair, Californians for Consumer Priv., to the Nat'l Telecomms. & Info. Admin. 1–2 (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/11_9_18_ntia_rfc_californians_for_consumer_privacy_final_.pdf [https://perma.cc/PXS7-93RF] (describing the principles and goals of the CCPA).

61. *See* CAL. SEC'Y OF STATE, TEXT OF PROPOSED LAWS: PROPOSITION 24, at 42, 43–44 (2020), https://cppa.ca.gov/regulations/pdf/prop24_text.pdf [https://perma.cc/23G8-SUMW] ("Unless California voters take action, the hard-fought rights consumers have won could be undermined by future legislation. . . . Rather than diluting privacy rights, California should strengthen them over time. . . . In enacting this act, it is the purpose and intent of the people of the State of California to further protect consumers' rights, including the constitutional right of privacy.").

It is no secret that privacy suffers from a bad public image[62] and an even worse definitional problem.[63] Since Warren and Brandeis's characterization of privacy as a "right to be let alone" in an article from 1890, scholars have endlessly debated privacy's meaning and purpose,[64] yet no single agreed-upon definition has emerged.[65]

Enter the HEW Report, with its FIPPs, rights-based approach. Indeed, the report develops its rights-based approach against a background of conceptual unclarity: The report's starting point is to admittedly grapple with the fundamental problem of how to define the right to privacy in order to delineate its boundaries and practical effect.[66] After rejecting the possibility that a clear definition of privacy would come from the Constitution, legislation, or the courts,[67] the report proposes to redefine personal privacy[68] based on the principle of mutuality,[69] which leads to the report's proposed data control rights later developed and popularized as the FIPPs.[70]

The idea of FIPPs/data control rights has certainly taken over the regulatory world[71] and has provided a "common language for privacy."[72] This common language might be confused as a substitute for a definition of what privacy is and what it is for. It might be seen as filling in the conceptual blanks and transforming a vague concept into concrete, operationalizable means of action,

62. *See* Cohen, *What Privacy Is for*, *supra* note 14, at 1904.

63. *See, e.g.*, *id.* ("No single meme or formulation of privacy's purpose has emerged around which privacy advocacy might coalesce."); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) ("Privacy, however, is a concept in disarray. Nobody can articulate what it means."); María P. Angel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, 124 COLUM. L. REV. 507, 509–11 (2024) ("This vibrant, interdisciplinary field with decades of history possesses no real sense of what constitutes a privacy problem and what does not."); Woodrow Hartzog, *What Is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677, 1677 (2021) ("Throughout history, privacy has evaded a precise meaning."); ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 45–46, 50–52 (2021) (discussing the complex landscape of privacy definitions and theory: From narrow and corporate-friendly definitions, to the privacy-as-control discourse, to the diversity of the privacy scholarship more broadly); David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 225 (2016) (noting that "setting out a crisp definition" of what the term privacy entails "turns out to be remarkably difficult to do").

64. Angel & Calo, *supra* note 63, at 3.

65. Hartzog, *supra* note 63, at 1678 ("[F]rom the early 1900s to the present day, lawmakers and judges have regularly been compelled to give the term 'privacy' a broad and consistent legal meaning. It hasn't gone well."); Ignacio N. Cofone, *Privacy*, *in* ENCYCLOPEDIA OF LAW AND ECONOMICS 1645 (Alain Marciano & Giovanni Battista Ramello eds., 2019) ("There is no universal agreement on what is privacy.").

66. HEW REPORT, *supra* note 31, at 33–42.

67. *See id.* at 33–38.

68. *Id.* at 38.

69. *Id.* at 40–41.

70. *See supra* Section I.A.

71. *Id.*

72. Hartzog, *supra* note 63, at 1682–83 (citing Paula Bruening, *Fair Information Practice Principles: A Common Language of Privacy in a Diverse Data Environment*, INTEL (Jan. 28, 2016), https://community.intel.com/t5/Blogs/Intel/Policy-Intel/Fair-Information-Practice-Principles-A-Common-Language-for/post/1332843 [https://perma.cc/4RYH-2JGX]).

precisely what the authors of the HEW Report meant to do—but is it? Mutuality is only a thin idea of a relation,[73] and it cannot put sufficient flesh on the bones of privacy. At best, mutuality transfers some powers from firms to individuals. But important questions remain wanting: Are those powers sufficient? How would those powers contribute to or supply individuals with more privacy? Could we really balance the power asymmetry that exists between firms and consumers through the means of individual rights? These questions proved quite complicated over the years, and throwing individual rights at a privacy problem did not seem to be enough.[74] Naturally, the inherent unclarity in the concept of privacy carries over to the legal manifestation of privacy as a set of individual rights. It is like a hereditary defect: Privacy lacks a healthy "definitional" chromosome, and therefore, its offspring—data control rights—suffers from the same core deficiency. It thus remains unclear what these rights are supposed to be or are capable of achieving.[75]

The two possible answers—the power-balancing answer and the privacy ill-defined answer—are not necessarily competing and are somewhat complementary. Data control rights could help shift more power to consumers while also offering a (limited) workaround for privacy's definitional problems.[76]

The power-balancing view is how the CCPA was advocated for and "advertised." Under this view, the goal of data control rights is to increase the power of consumers vis-à-vis firms. Under the privacy ill-defined view, data control rights are a substitute for a definition of privacy and are therefore taken to be valuable in and of themselves. Under both views, it seems that for data control rights to be considered successful, they must be used by consumers to some significant extent. Part II presents empirical results on how many consumers use their data control rights; Part III then builds on the views developed here and explores whether the empirical results suggest that data control rights achieve their goals.

II. EMPIRICAL FINDINGS: HOW MUCH ARE DATA CONTROL RIGHTS USED?

A. THE REPORTING REQUIREMENT

The privacy regime of the CCPA includes a first-of-its-kind reporting requirement, which enables measuring the actual usage by individuals of their data control rights. Businesses that process the personal information of at least 10,000,000 consumers in a given year are required to publish on their website the data ("metrics") on how many consumers have made requests to

73. *See, e.g.*, Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 592 (2021).

74. *See, e.g.*, Hartzog, *supra* note 63, at 1682–83; Hartzog, *FIPs*, *supra* note 15, at 964–77; Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1721–37 (2020); Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 343, 367 (Jane K. Winn ed., 2006).

75. *See infra* Part III.

76. *See infra* Part III.

exercise data control rights,[77] and how many of these requests were complied with or denied.[78] The CCPA Regulations leave it up to the firm to decide whether it will report on the *reasons* it has denied requests, and it also suggests how firms might do that, but in a limiting fashion.[79] Since this reporting requirement was put in place, firms reported data on the rights to know, to delete, and to opt-out,[80] for the years 2020 and 2021.[81]

Firms are supposed to report on data control rights usage by "consumers," and the reporting threshold requirement is based on the number of "consumers" as well.[82] Who are consumers? The CCPA defines consumers as natural persons who are California residents.[83] It is unknown if all reporting (and nonreporting) firms have followed this definition to a tee. First, the actual number of consumers each firm has, whether in or outside of California, is generally nonpublic information, so it is impossible to know exactly which firms fall under the reporting obligation.[84] Second, some larger firms have not reported anything while some smaller firms have provided a report.[85]

77. *See* CAL. CODE REGS. tit. 11, § 7102(a) (2021) ("A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall: (1) Compile the following metrics for the previous calendar year: (A) The number of requests to know that the business received, complied with in whole or in part, and denied; (B) The number of requests to delete that the business received, complied with in whole or in part, and denied; (C) The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and (D) The median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out."). After March 29, 2023, the language of section 7102(a) was amended to additionally include similar data on the rights to correct, opt-out of *sharing* of personal information, and limit use of personal sensitive information. CAL. CODE REGS. tit. 11, § 7102(a) (2023).

78. *See* CAL. CODE REGS. tit 11, § 7102(a)(1)–(2) (2021) ("Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.").

79. *See* CAL. CODE REGS. tit. 11, § 7102(a)(2)(A) (2021) ("In its disclosure pursuant to subsection (a)(2), a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds."). After March 29, 2023, see CAL. CODE REGS. tit. 11, § 7102(a)(2) (2023).

80. *See supra* note 21.

81. Data collection and analysis for this article were completed prior to July 2023, which is when firms were required to report their metrics for 2022. *See infra* note 87 and accompanying text.

82. *See* CAL. CODE REGS. tit. 11, § 7102(a)(1) (2021).

83. See CAL. CIV. CODE § 1798.140(g) (West 2018), and after January 1, 2023, see CAL. CIV. CODE § 1798.140(i) (West 2022), in both cases the full definition is: "'Consumer' means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier."

84. A narrow exception to this rule is a recent development in European Union law. The European Union's Digital Services Act requires firms to report whether they have over 45 million users in the EU. *See, e.g.*, *DSA: Very Large Online Platforms and Search Engines*, EUR. COMM'N (Feb. 21, 2024), https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops [https://perma.cc/JCC9-A2VS].

85. For example, consider the differences between two firms in the same industry catering for consumers in the same market, Netflix and Hulu. While Hulu provided metrics reports for 2020 and 2021, Netflix did not. *See Your California Privacy Rights*, HULU, https://web.archive.or

However, the CCPA Regulations also allow firms to report on "requests received from all individuals, rather than requests received from consumers."[86] Thus, firms may report on requests they received from *non-Californians* as well as Californians—U.S. consumers or global consumers, and anything in between—provided that they state they have done so, which is what some firms explicitly did. However, as I discuss below, it seems that some firms chose to report on a territory broader than California without stating that they have done so.

There are certain limitations to the data provided by firms, which I discuss as they arise in Sections II.B to II.D below.

B. DATA COLLECTION AND ANALYSIS

I manually collected metrics reports for the years 2020 and 2021 from the websites of firms.[87] As mentioned above, it is impossible to know which firms fall under the CCPA's reporting requirement threshold of 10,000,000 "consumers" (Californians) or more in a given year, and additionally, firms are allowed to report on all individuals, inside *and* outside of California. Firms generally do not publish this type of information—not how many consumers they have in California, and not how many consumers they have anywhere else.[88] The California regulator, the California Privacy Protection Agency,[89] did not publish a list of subject firms. Given this challenge, I developed two strategies to find firms that published the data.[90] First, I used websites' traffic rankings based on the assumption that websites that attract a lot of traffic are likely processing the personal information of many consumers.[91] Second, I

g/web/20210922155416/https://www.hulu.com/ca-privacy-rights [https://perma.cc/5MVF-JB7D] (showing Hulu's 2020 metrics report); *Your California Privacy Rights*, HULU (June 27, 2022), https://web.archive.org/web/20220831135053/https://www.hulu.com/ca-privacy-rights [https://perma.cc/FJ5K-WVLP] (showing Hulu's 2021 metrics report).

86. *See* CAL. CODE REGS., tit. 11, § 7102(b) (2021) ("A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.").

87. At the time of data collection, firms that published their metrics had published metrics for either 2020 or 2021, or both. At the time firms published those metrics, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2018) and CAL. CODE REGS., tit. 11, §§ 7000–7500 (2021) were in force, so throughout the Article, I cite those versions of the law and regulations. But where it is applicable, I also include a citation to the current version of the law and regulations in 2023.

88. *See supra* notes 83–84 and accompanying text.

89. *See About CPPA*, CA.GOV: CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/about_us [https://perma.cc/WU9V-L6CV] ("In November of 2020, California voters approved Proposition 24, the California Privacy Rights Act of 2020 (CPRA). The CPRA added new privacy protections to the California Consumer Privacy Act of 2018. The California Privacy Rights Act established a new agency, the California Privacy Protection Agency (CPPA) to implement and enforce the law. The CPPA is governed by a five-member Board.").

90. My goal was to find as many firms as I could, not knowing how many firms had published the data. Naturally, because of the fuzzy regulatory threshold which is based on inside information rather than on public information, there could be firms that published the data that I have missed.

91. Similarweb's top 50 websites in the U.S. (collected on June 16, 2022), and the top 100 domains in Tranco's top 1 million domains as of July 1, 2022. *See* Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński & Wouter Joosen, *Tranco: A Research-*

used a keywords search on Google,[92] expecting that firms who publish the usage metrics might include specific terms in their reports, thereby allowing the tracing of the firms and the reports. Among other results, this search led me to a GitHub repository that was created by Sebastian Zimmeck, a computer science professor, who collected CCPA reports for the year 2020.[93] Zimmeck collected the data by running a Google keywords search and working through all of the search results.[94] Combining the strategies, I created a list of reporting firms which comprises all firms found by Zimmeck and the additional firms I found through my independent searches.[95] I then created a dataset that includes the CCPA metrics of reporting firms for the years 2020 and 2021.[96]

For each firm that published a metrics report on its website, I located the report and inserted the information into an Excel spreadsheet. For documentation purposes for each such firm, I saved a copy of the relevant webpage showing the report and the report's Internet link in the spreadsheet. Remarkably, almost all firms *have deleted* the 2020 metrics reports from their websites,[97] which posed another collection challenge. Given this challenge, I used two strategies to collect all metrics reports for 2020: I first tried to locate the deleted information on the Wayback Machine Internet Archive,[98] and for most firms, I was able to do so. For the few firms that did not have their 2020 report archived on the Wayback Machine, I used copies of the 2020 reports archived by Zimmeck.[99]

Reading through the reports, I learned that firms do not use a uniform standard or template to report the metrics (and the CCPA Regulations do not define or require a standardized report). Among other variations in reporting, a few firms broke down their metrics by different services or products they offer (including through a subsidiary) or by different methods of request. But most firms provided their metrics in a unified manner, not revealing which services, products, or subsidiaries are included and reflected in the data or what their relative part in the data is. Hence, to analyze the results consistently and fully across all firms, I summed up the data of the few firms that provided more detailed reports across their different services, products, subsidiaries, and

---

Oriented Top Sites Ranking Hardened Against Manipulation, NETWORK & DISTRIBUTED SYS. SEC. (NDSS) SYMP., Feb. 2019, at 1–5, https://dx.doi.org/10.14722/ndss.2019.23386 [https://perma.cc/2CQ8-QQ2P].

92. I searched for "privacy CCPA 'metrics,'" "CCPA report," and "CCPA metrics."

93. Sebastian Zimmeck, *California Consumer Privacy Act (CCPA) Metrics*, GITHUB, https://github.com/privacy-tech-lab/ccpa-metrics [https://perma.cc/GBT9-54BB].

94. Zoom Interview with Sebastian Zimmeck, Assoc. Prof. of Comput. Sci., Wesleyan Univ., (June 23, 2022).

95. Gaining or Losing Control Dataset, *supra* note 11.

96. I did not use Zimmeck's metrics database, only the list of firms he had compiled.

97. If they had reported the metrics in 2021, almost all firms have simply replaced the 2020 report with the 2021 report. If they had not reported metrics in 2021, some firms left the 2020 data on their websites.

98. *Wayback Machine*, INTERNET ARCHIVE, https://archive.org/web [https://perma.cc/47LX-B2KV].

99. *See* Zimmeck, *supra* note 93.

methods of request.[100] A handful of firms provided fully separate metrics for non-California requests in addition to metrics on California alone, in which case I used the California numbers for the analysis.

Following this process, the dataset includes a total of 137 firms in 2020 and 121 firms in 2021.[101] The main reason for the difference in cohorts' sizes is that some firms who reported metrics in 2020 did not report in 2021.

My analysis of the data is descriptive—I describe what firms have reported and show and compare the main trends. My main presentation of the results is a histogram of the number of requests received for each right in each year.[102] I use a modified logarithmic scale for the number of requests, grouping together: 0–1,000,[103] 1,001–10,000, 10,001–100,000, and more than 100,000.[104] For firms reporting more than 100,000 requests received, I provide a more detailed breakdown in a table based on the territorial scope of their report, and splitting them into 100,001–1,000,000 requests, and above 1,000,000 requests.[105] Finally, for analyzing firms' compliance rates with the requests they received (i.e., how much firms have fulfilled consumer requests rather than rejected them), I use two averages across all firms: mean compliance rate (giving each firm equal weight) and a weighted mean, weighted by the number of requests each firm received.[106]

Section II.C below presents the main results, and Section II.D discusses their implications and interpretation. Both Sections II.C and II.D discuss some limitations of the data as they arise in the analysis.

C. RESULTS

1. Usage of Rights—Measuring Consumer Requests

An overwhelming majority of firms—roughly 80 percent—reported less than 10,000 requests per right per year, corresponding to at most 1 in 1,000 consumers (0.1 percent) a year using their rights to know, to delete, and to opt-out.[107] And a striking 88 to 95 percent of firms reported less than 100,000

100. Unifying broken-down metrics was done for two reasons: First, it reduced an artificial outsized weight such firms would have received in the analysis because of how they provided the metrics; many firms that also have multiple products, services, subsidiaries, or methods of request provided unified metrics to begin with. Second, it increased the overall numbers for a single reporting entity, thereby providing a "strict assumption" against the hypothesis that the usage of the rights was low.

101. Gaining or Losing Control Dataset, *supra* note 11.

102. *See infra* Figures 1, 2 and accompanying text.

103. As firms process the personal information of millions of consumers or more, I did not find it meaningful to distinguish between 0–10, 11–100, and 101–1,000 requests.

104. *See infra* Figures 1, 2. I chose the upper threshold to be 100,000 since relatively few firms received more than 100,000 requests.

105. *See infra* Table 1 and accompanying text.

106. *See infra* Section II.C.2.

107. *See infra* Figures 1, 2 and accompanying text.

requests per right per year, corresponding to at most 1 in 100 consumers (1 percent).[108]

Figure 1 shows a breakdown of the 137 firms that reported data in 2020 according to how many requests they received for each of the three rights—the right to know, the right to delete, and the right to opt-out. For each right, Figure 1 shows the fraction of firms that received under 1,000 requests, between 1,001 and 10,000 requests, between 10,001 and 100,000 requests, and more than 100,000 requests (all percentages are rounded to the nearest whole number). For example, in 2020, for the right to delete, 72 percent of the 137 reporting firms received less than or equal to 1,000 requests.

Figure 1: Data Control Rights Usage—Received Requests in 2020.
Total Number of Firms: 137

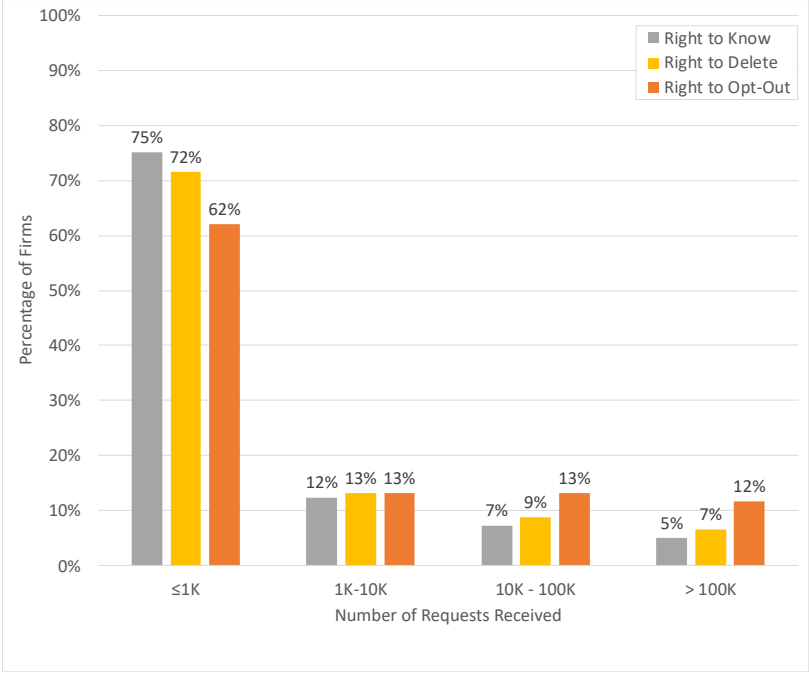
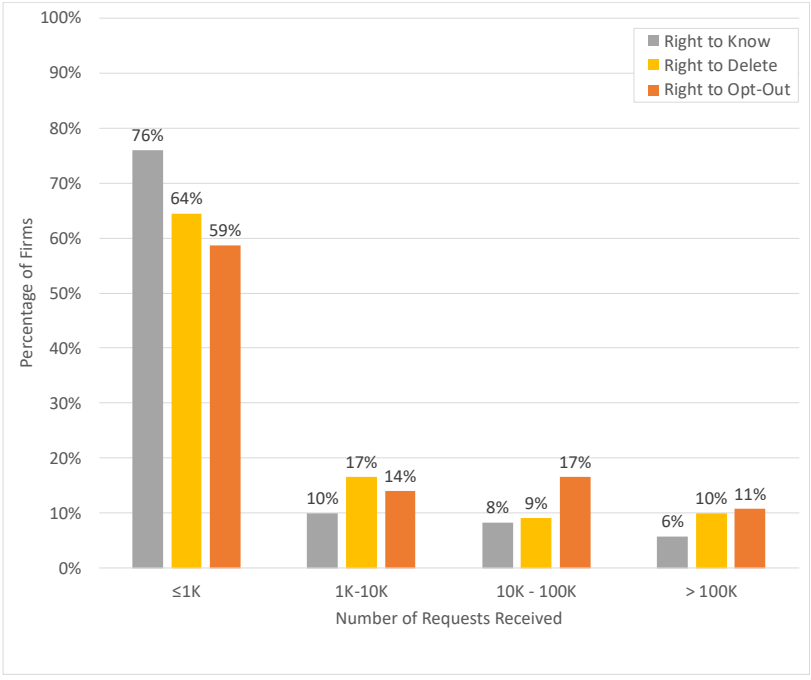


Figure 2 shows a similar breakdown for 2021, in which 121 firms reported the data. Note that both Figure 1 and Figure 2 show percentages, but not out of exactly the same cohort of firms, as some firms that reported in 2020 did not report in 2021, and a few firms started reporting in 2021.

108. *See infra* Figures 1, 2 and accompanying text. I explain and discuss these consumer percentages in Section II.D.1.

Figure 2: Data Control Rights Usage—Received Requests in 2021.
Total Number of Firms: 121



Some firms did not provide metrics for all three rights. This phenomenon is most prevalent for the right to opt-out, as discussed below,[109] but some firms did not provide metrics for the right to know or the right to delete without explaining the omission.[110] In Figures 1 and 2, such firms are counted in the ≤1,000 bin, as they effectively reported on zero requests.

While the right to know and the right to delete generally apply to all firms, the right to opt-out in principle applies only to firms that "sell" personal information to "third parties."[111] And indeed, some firms—which have reported the metrics for the right to know and the right to delete—have not reported metrics for the right to opt-out, claiming in their metrics report or in their privacy policy that they did not provide the right to opt-out because they did not "sell" personal information, and thus did not have metrics to report on.[112]

109. *See infra* notes 111–15 and accompanying text.

110. In 2020, there was one nonreporting firm for the right to know and two nonreporting firms for the right to delete. In 2021, there were two nonreporting firms for the right to know and three nonreporting firms for the right to delete. *See* Gaining or Losing Control Dataset, *supra* note 11.

111. See CAL. CIV. CODE § 1798.120 (West 2018) for the right to opt-out, *id.* § 1798.140(t) (West 2018) for the definition of "sale" (after January 1, 2023, see CAL. CIV. CODE § 1798.140(ad) (West 2022)), and CAL. CIV. CODE § 1798.140(w) (West 2018) for the definition of "third party" (after January 1, 2023, see CAL. CIV. CODE § 1798.140(ai) (West 2022)).

112. *See* Gaining or Losing Control Dataset, *supra* note 11.

In 2020, there were 39 such firms (out of 137), and in 2021 again there were 39 such firms (out of 121).[113] In addition to those self-proclaiming "non-selling" firms, a few firms did not report data on the right to opt-out without providing an explanation.[114] In 2020, there were 9 such firms, and in 2021 there were 5 such firms.[115] As mentioned above, in Figures 1 and 2, such firms are counted in the ≤1,000 bin, as they effectively reported on zero requests to opt-out.[116]

Figures 1 and 2 are based on the numbers as reported by firms.[117] I analyze and discuss the results under the assumption that each reported request represents a unique requesting consumer. If, on the other hand, some consumers have initiated more than one request, or if firms counted automatic privacy signaling (an "opt-out preference signal" such as the Global Privacy Control ("GPC")[118] and cookie-blockers), changes in privacy settings, or choices made from different devices used by the same consumer, multiple times for the same consumer (as has likely happened),[119] then the numbers actually represent an overestimation of the number of consumers that utilize their data control rights.

The results reveal that 88 percent to 95 percent of firms reported less than 100,000 requests per right per year.[120] Now we will take a closer look at the minority of firms, which are *high-reporting firms*, i.e., firms that reported above 100,000 requests per right per year. As shown in Figure 1, in 2020, high-reporting firms are 5 percent of firms for the right to know, 7 percent of firms for the right to delete, and 12 percent of firms for the right to opt-out.[121] As shown in Figure 2, in 2021, high-reporting firms are 6 percent of firms for

113. *Id.*

114. *Id.*

115. *Id.* It is possible that some of these firms *did* receive opt-out requests but did not report on these requests as part of their annual metrics report. It could also be that some of them did not comply with the *substantive* requirement of the CCPA to provide the right to opt-out and, for that reason, did not have the metrics to report on. It could also be that they provided the right but did not receive any opt-out requests.

116. *Id.*

117. *See id.*

118. *See* CAL. CIV. CODE § 1798.135(b)(1) (West 2022); *see also* California AG Website, *supra* note 55 ("B. Right to Opt-Out of Sale or Sharing. . . . 8. What is the GPC? . . . [O]ne acceptable method for consumers to opt-out of sales or sharing is via a user-enabled global privacy control, like the GPC. Developed in response to the CCPA and to enhance consumer privacy rights, the GPC is a 'stop selling or sharing my data switch' that is available on some internet browsers . . . ."); GLOB. PRIV. CONTROL, https://globalprivacycontrol.org [https://perma.cc/4KHB-JW6Y] (the official website of the GPC, describing how to download, use, and implement the GPC tool); Sebastian Zimmeck & Kuba Alicki, *Standardizing and Implementing Do Not Sell*, 19TH WORKSHOP ON PRIV. ELEC. SOC'Y 15, 15–20 (2020) (developing the GPC); Press Release, State of Cal. Dep't of Just., Off. Att'y Gen., Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act (Aug. 24, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement [https://perma.cc/YH5A-6RPB].

119. *See infra* notes 135–37 and accompanying text (the Oracle example).

120. *See supra* Figures 1, 2 and accompanying text.

121. *See supra* Figures 1, 2 and accompanying text.

the right to know, 10 percent of firms for the right to delete, and 11 percent of firms for the right to opt-out.[122]

As I discuss in Section II.D.1., to understand the actual level of data control rights usage among consumers, we need to know or at least approximate the *fraction* of consumers who have used their rights out of the entire consumer base beyond the raw numbers. The reported number of requests received by firms should, therefore, be considered and understood in the context of 10,000,000 consumers (at least). Because firms do not provide information about the fraction of consumer usage out of their entire consumer base, or on their total number of consumers, to understand the results for high-reporting firms I use their reported territorial scope as a proxy for their overall consumer base. As the reporting requirement is based on 10,000,000 or more consumers *in California*, when firms report on a territory larger than California (e.g., the United States or the world), they are likely reporting on a consumer base that is significantly larger than 10,000,000.[123]

In that context, the 100,000 requests threshold I use between low- and high-reporting firms represents less than or equal to 1 percent of consumers (out of 10,000,000) and, as such, is very conservative. Table 1 provides the data for high-reporting firms in two groups: firms reporting between 100,000 and 1,000,000 requests (Panel A) and firms reporting above 1,000,000 requests (Panel B). Table 1 provides the territorial scope on which high-reporting firms have reported—whether they reported on California alone, on a territory broader than California, or they have not explicitly specified the territory on which they reported.

Table 1: High-Reporting Firms and Territorial Scope in 2020 and 2021[124]

Panel A						
100K-1M Requests	2020			2021		
Territorial Scope	Right to Know	Right to Delete	Right to Opt-Out	Right to Know	Right to Delete	Right to Opt-Out
Only California	0	0	4	0	0	2
Broader than California	4	3	4	5	7	3
Unspecified	2	2	5	1	1	1
Total	6	5	13	6	8	6
Panel B						
1M+ Requests	2020			2021		
Territorial Scope	Right to Know	Right to Delete	Right to Opt-Out	Right to Know	Right to Delete	Right to Opt-Out
Only California	1	1	1	1	1	3
Broader than California	0	2	2	0	2	3
Unspecified	0	1	0	0	1	1
Total	1	4	3	1	4	7

122. *See supra* Figures 1, 2 and accompanying text.

123. *See infra* notes 128–31 and accompanying text (the Discord example).

124. *See* Gaining or Losing Control Dataset, *supra* note 11.

For high-reporting firms, and especially for firms reporting more than 1,000,000 requests, the main question is whether the reported numbers indicate a wide usage of the rights by consumers or not. The answer is not straightforward, given that a few important factors arise from the data and must be considered.

First, firms vary in the territory they report on, and some firms even report on different territories for different rights in the same year. As Table 1 shows, the majority of metrics reported per right that exceed 100,000 requests represent a territory broader than California. Across both years, 55 percent of these higher metrics were reported for a territory explicitly broader than California, 23 percent of these higher metrics were reported for an unspecified territory, and 22 percent of these higher metrics were reported for California only.[125] As for those metrics reports that did not explicitly specify their territorial scope, given the high numbers they provide, their territorial scope is likely broader than California. For example, in 2020, Discord (a Voice over Internet Protocol ("VoIP") and instant messaging social platform popular among gamers)[126] reported more than 14 million requests for the right to delete without specifying the territory for which the metrics apply.[127] Given the size of the population in California, which is about 39 million people, with almost 8 million either younger than 5 years old or older than 65 years old, it is not likely that all requests came from California consumers.[128] Furthermore, in 2021, Discord did not provide a metrics report at all. It could be that after the firm provided a report for a territory broader than California in 2020, it realized that since it has less than 10,000,000 consumers *in California*, it is not obligated to report the metrics, and so it decided not to do so the following year. For firms that reported on a territory explicitly broader than California or on an unspecified territory that is likely broader than California, the point of reference changes from 10,000,000 consumers to possibly much larger numbers, representing a consumer base in the entire United States or globally. For example, it has been estimated that Discord has over 350 million registered users worldwide.[129]

A second factor we must consider in interpreting high-reported numbers is that some high-reporting firms offer several services and products that

125. These percentages represent the fraction of high-ranking metrics per right out of all high-ranking metrics for all rights. That is, I have counted some firms ("repeat players") more than once, both in the numerator and in the denominator.

126. *See* Shannon Liao, *What is Discord, the Voice and Text Chat App Popular with Gamers?*, WASH. POST (Dec. 1, 2022, 4:17 PM), https://www.washingtonpost.com/video-games/2022/11/30/what-is-discord-app-explainer-twitter (on file with the *Iowa Law Review*).

127. *See* Librarian, *Data Request Reporting Metrics*, DISCORD, https://support.discord.com/hc/en-us/articles/4410339387671-Data-request-reporting-metrics [https://perma.cc/TJ38-NSGV].

128. *See QuickFacts: California*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/CA [https://perma.cc/JJD9-7ZP3].

129. *See* Alys Key, *How Do I Change My Discord Username? Identity Overhaul to Affect 350 Million Users*, STANDARD (May 7, 2023), https://www.standard.co.uk/news/tech/discord-username-change-b1079146.html [https://perma.cc/KK8K-7APF] ("Discord has an estimated 350 million registered users, of which 140 million are regularly active.").

were, presumably, all measured and counted together. The "bundling" of measurements for more than one product or service can also explain the high numbers. For example, Microsoft offers a voluminous number of services and products under its brand,[130] and it did not distinguish among these in its reports while reporting very high numbers.[131] Notably though, Microsoft provided separate reports for LinkedIn, with extremely low numbers.[132]

A third factor we must consider in interpreting high-reported numbers is that some of the numbers provided by firms, especially those above 1,000,000 requests, could be the result of measurement problems and inaccuracies. For example, in both years, Oracle provided metrics for its Oracle General Marketing, Sales, and Events business, as well as its Oracle Advertising business. In its reports, per its Oracle Advertising business, which accounts for the lion's share of the reported metrics, the firm provides extremely high numbers—more than 88 million requests to delete and opt-

130. Including, for example, msn.com, live.com, Office products, Bing, Edge, Windows, Xbox, Skype, but excluding LinkedIn who provides metrics separately. *See CCPA Annual Metrics: Calendar Year 2020*, *infra* note 132 and accompanying text. *See also* Julie Brill, *Millions Use Microsoft's GDPR Privacy Tools to Control Their Data — Including 2 Million Americans*, MICROSOFT: MICROSOFT ON THE ISSUES (Sept. 17, 2018), https://blogs.microsoft.com/on-the-issues/2018/09/17/millions-use-microsofts-gdpr-privacy-tools-to-control-their-data-including-2-million-americans [https://perma.cc/HKP9-NU6J] ("[W]e built a privacy dashboard where our customers can manage their privacy settings, see what data we have stored, and delete that data if they want to. This includes everything from browsing and search history to location activity, movies and TV viewed through a Microsoft app or service, and health data in Microsoft Health.").

131. In 2020, Microsoft reported about 2,950,000 requests for the right to know and about 2,850,000 requests for the right to delete. *See U.S. State Data Privacy Laws Notice*, MICROSOFT: PRIVACY (July 2023), https://privacy.microsoft.com/en-us/ccpa [https://perma.cc/FHC7-QCYQ]. In 2021, Microsoft reported a little less than 2,000,000 requests for the right to know and about 1,700,000 requests for the right to delete. *Id.* Microsoft did not report metrics for the right to opt-out in any of the years, declaring it is not applicable. *Id.* In both years, Microsoft noted that these numbers are for California only. *Id.* Such high numbers for California are an extreme outlier among all reporting firms and are very hard to understand without more information. *See also* Susannah Luthi, *'Functionally Useless': California Privacy Law's Big Reveal Falls Short*, POLITICO (Aug. 6, 2021, 4:07 PM), https://www.politico.com/states/california/story/2021/08/05/functionally-useless-california-privacy-laws-big-reveal-falls-short-1389429 [https://perma.cc/X8YS-Z8EX] ("Microsoft says it received 2.8 million petitions to delete Californians' data, while Apple got fewer than 295,000. Google, a company with billions of users worldwide, reported a mere 276 deletion requests from Californians. And Twitter hasn't posted any data at all.").

132. In 2020, LinkedIn reported six requests for the right to know and two requests for the right to delete. *See CCPA Annual Metrics: Calendar Year 2020*, LINKEDIN (July 1, 2021), https://web.archive.org/web/20210808121541/https://www.linkedin.com/legal/l/california-privacy-disclosure-annual-metrics [https://perma.cc/TMF8-SMEZ]. In 2021, LinkedIn reported eighteen requests for the right to know and four requests for the right to delete. *See CCPA Annual Metrics: Calendar Year 2021*, LINKEDIN (May 25, 2022), https://web.archive.org/web/20220818172641/https://www.linkedin.com/legal/l/california-privacy-disclosure-annual-metrics [https://perma.cc/N6L2-432E]. LinkedIn did not report metrics for the right to opt-out in any of these years, declaring it was not applicable. *Id.* In both years, LinkedIn noted that these numbers are for California only. *Id.*

out in 2020[133] and almost 9 million requests to delete and opt-out in 2021.[134] But these extremely high numbers represent requests for *both* deletion and opt-out, without distinguishing the two rights; *global* requests Oracle received; and three different request-type identifiers,[135] which could have caused consumer requests to be counted more than once because of the use of different identifiers. It is less likely that 88 million Oracle consumers worldwide utilized their data control rights and more likely that the metrics are either erroneous or represent a technical count based on all website visits (e.g., number of API calls or HTTP requests) that is many times more than the number of actual consumers that utilized each right.

2. Firm Compliance with Consumer Requests

Recall that the reporting requirement requires firms to provide metrics not only on how many consumers have made data control rights requests but also on how many of these requests were complied with or denied.[136] Table 2 provides data on firms' compliance rates with consumers' requests, i.e., how many of those requests received by firms were fulfilled or rejected.

Table 2: Compliance Rates[137]

Compliance Rates	2020			2021		
	Right to Know	Right to Delete	Right to Opt-Out	Right to Know	Right to Delete	Right to Opt-Out
Average compliance rates for reporting firms	74%	70%	85%	74%	70%	91%
Weighted average of compliance for reporting firms	97%	88%	99.84%	89%	90%	99.93%
Firms not reporting compliance rates	11	15	20	14	17	16
Firms declaring right is N/A	0	0	39	0	0	39
Total reporting firms	126	122	78	107	104	66
Total firms	137			121		

Notably, 8 percent to 15 percent of firms in 2020 and 12 percent to 13 percent of firms in 2021 did not report data on their compliance with consumer

133. This is the highest number reported in both years across all rights. *See CCPA Annual Consumer Privacy Reporting*, ORACLE, https://web.archive.org/web/20210925134717/https://www.oracle.com/legal/privacy/ccpa [https://perma.cc/6CXU-86AW] (reporting data from 2020).

134. *See CCPA Annual Consumer Privacy Reporting*, ORACLE, https://web.archive.org/web/20220813154246/https://www.oracle.com/legal/privacy/ccpa [https://perma.cc/3HLC-JVUR] (reporting data from 2021).

135. In 2020, for example, these different request-type identifiers included "offline (direct identifiers)" (about 17,300, seems to be only Californians), "cookie-based" (about 84,900,000, global), and "Mobile advertising identifiers (MAID)" (about 3,180,000, global). *See CCPA Annual Consumer Privacy Reporting*, *supra* note 133.

136. *See supra* Section II.A.

137. Gaining or Losing Control Dataset, *supra* note 11.

requests, though they did provide the number of requests they have received. These nonreporting firms (per compliance) include some high-reporting firms (per received requests)—e.g., Oracle, who provided extremely high numbers for received requests[138] but did not provide data on its compliance with such requests. Additionally, as also noted above, 39 firms in both years did not report any metrics on the right to opt-out, claiming it was not applicable to them.[139]

The first line in Table 2 shows the average compliance rates per right per year across all reporting firms, where each reporting firm received the same weight. The second line in Table 2 provides a weighted average of compliance rates that takes into account the number of requests each reporting firm received such that firms receiving a lower number of requests proportionally affect the average less than firms receiving a higher number of requests. The reason for the relatively lower compliance rates reflected in the simple average is that many firms that received a low number of requests also had low compliance rates with those requests, while the opposite was generally true for firms that received a higher number of requests.

D. Discussion

1. Very Low Usage of Data Control Rights

The reported data reveals disappointing results for a regime centered around data control rights. Across the three rights, 75 percent to 87 percent of firms in 2020, and similarly 73 percent to 86 percent of firms in 2021, received no more than 10,000 requests a year.[140] Even worse, 62 percent to 75 percent of firms in 2020, and similarly 59 percent to 76 percent of firms in 2021, received no more than 1,000 requests a year for each of the rights.[141]

These are strikingly low numbers of consumer requests. But *how low* are these low usage numbers? While we do not know how many consumers (in or out of California) each firm has, we do know that the trigger for reporting the metrics is that a firm processed the personal information of more than 10,000,000 consumers a year.[142] Thus, we can put these numbers in context: For an overwhelming majority of firms—75 percent to 87 percent of firms in 2020, and similarly 73 percent to 86 percent of firms in 2021—no more than 0.1 percent of consumers have used their rights to know, to delete, and to opt-out. Looking at an even bigger majority of firms—88 percent to 95 percent of firms in 2020, and similarly 89 percent to 94 percent of firms in 2021—no more than 1 percent of consumers have used their right to know, to delete, and to opt-out.

Notably, however, contextualizing the metrics as percentages out of 10,000,000 is *conservative*. This is because the reporting requirement is

138. *See supra* notes 135–37 and accompanying text.
139. *See supra* notes 112–14 and accompanying text.
140. *See supra* Figures 1, 2.
141. *See supra* Figures 1, 2.
142. *See supra* note 22 and accompanying text.

10,000,000 consumers a year *or more*.[143] Additionally, we know that most high-reporting firms have reported metrics for a consumer base larger than California, i.e., the entire United States or globally, where we can expect firms to have many times more consumers. In these cases, 10,000,000 does not represent our 100 percent, and the fraction of consumers using their rights is likely smaller than 1 percent. One of the main limitations of the reporting requirement, and consequently, of the data provided by firms, is that it does not require firms to contextualize their metrics by providing the sum of consumers for which a firm is processing information, nor the applicable territory. These shortcomings prevent us from obtaining a fuller picture of data control rights usage.

2. The Right to Opt-Out: Most Used, Least Provided

Relative to the rights to know and delete, the right to opt-out is the most used right by consumers, if only mildly. It has the lowest percentage of firms in the bottom bin of no more than 1,000 requests a year,[144] and it has the largest percentage of firms in the top bin of more than 100,000 requests a year.[145] The right to opt-out also enjoys the highest compliance rates by firms, close to 100 percent in both years.[146]

These results are not entirely surprising since the right to opt-out is the only right that firms are specifically required to provide via "a clear and conspicuous 'Do Not Sell My Personal Information' link on their website."[147] On the other hand, the other two rights can be provided through several methods, some of them cumbersome, and the ways in which some firms have implemented them are the opposite of user-friendly.[148] For its ease of use or

143. *Id.*

144. 62 percent in 2020, compared to 72 percent to 75 percent for the other two rights, and 59 percent in 2021, compared to 64 percent to 76 percent for the other two rights. *See supra* Figures 1, 2.

145. 12 percent in 2020, compared to 5 percent to 7 percent for the other two rights, and 11 percent in 2021, compared to 6 percent to 10 percent for the other two rights. *See supra* Figures 1, 2.

146. *See supra* Table 2.

147. *See, e.g.*, California AG Website, *supra* note 55 (explaining under title "B. Right to Opt-Out of Sale or Sharing[,]" subtitle "3. How do I submit my opt-out request?": "Businesses that sell personal information are subject to the CCPA's requirement to provide a clear and conspicuous 'Do Not Sell or Share My Personal Information' link on their website that allows you to submit an opt-out request. Businesses cannot require you to create an account in order to submit your request. Businesses also should not require you to verify your identity, though they can ask you basic questions to identify which personal information is associated with you.").

148. *See, e.g.*, *id.* (describing under title "C. Requests to Know," subtitle "2. How do I submit my request to know?": "Businesses must designate at least two methods for you to submit your request—for example, an email address, website form, or hard copy form. One of those methods has to be a toll-free phone number and, if the business has a website, one of those methods has to be through its website. However, if a business operates exclusively online, it only needs to provide an email address for submitting requests to know. . . . Make sure you submit your request to know through one of the business's designated methods, which may be different from its normal customer service contact information. If you can't find a business's designated methods, review its privacy policy, which must include instructions on how you can submit your request.").

otherwise, the fact that the right to opt-out is the most used right, and complied with the most, is an important insight to policymakers. If policymakers are interested in raising the level of data control rights usage, they should consider aligning the methods by which the rights to know and delete are provided with the user-friendly and straightforward method of the right to opt-out.

But not all is rosy with the right to opt-out: In light of its superior provision method, it is perhaps surprising that the right to opt-out is not performing *significantly* better than the other two rights. Indeed, firms are using hard-to-understand or hard-to-find options and other dark patterns to skew consumer choice even in the case of the supposedly easy-to-use right to opt-out.[149] Moreover, one of the interesting facts that the results reveal is that many firms are evading the right to opt-out—to be exact, 35 percent of reporting firms in 2020 and 36 percent of reporting firms in 2021.[150] Such firms take the legal position that they do not "sell" personal information to "third parties."[151] But the definitions of "sale" and "third party" are complex, and it is not at all clear whether such definitions serve consumer-protection and privacy goals or benefit firms by providing a simple way to circumvent the law.[152] This is also

---

And similarly for the right to delete (under the title "D. Requests to Delete," subtitle "2. How do I submit my right to delete?"). *Id.*

149. *See, e.g.*, Maggie Van Nortwick & Christo Wilson, *Setting the Bar Low: Are Websites Complying with the Minimum Requirements of the CCPA?*, 2022 PROC. ON PRIV. ENHANCING TECHS. 608, 621–22; Hana Habib et al., *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, 2019 PROC. FIFTEENTH SYMP. ON USABLE PRIV. & SEC. 387, 395–98 [hereinafter Habib et al., *An Empirical Analysis*]; Hana Habib et al., *"It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices*, 2020 PROC. CHI. CONF. ON HUM. FACTORS COMPUTING SYS., at 1, 2, 5–9; Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger & Lalana Kagal, *Dark Patterns After the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence*, 2020 PROC. CHI. CONF. ON HUM. FACTORS COMPUTING SYS., at 1, 8–10; Jen King, *Dark Patterns and the CCPA*, STANFORD L. SCH., CTR. INTERNET & SOC'Y (Oct. 30, 2020, 10:06 AM), https://cyberlaw.stanford.edu/blog/2020/10/dark-patterns-and-ccpa [https://perma.cc/9CKE-6DG3]; Waldman, *Privacy's Rights Trap*, *supra* note 8, at 95–96.

150. Gaining or Losing Control Dataset, *supra* note 11. In calculating these percentages, I have included firms that explicitly noted that they believe the right does not apply to them (39 out of 137 in 2020 and 39 out of 121 in 2021) and the few firms that did not report data on the right to opt-out without providing an explanation (9 out of 137 in 2020, and 5 out of 121 in 2021).

151. *See, e.g.*, *Data Access and Deletion Transparency Report*, GOOGLE: PRIVACY & TERMS, https://web.archive.org/web/20220817070518/https://policies.google.com/privacy/ccpa-report?hl=en-US [https://perma.cc/295B-HCSQ] (reporting metrics from 2021) ("As explained in our Privacy Policy, Google does not sell our users' personal information."); *California Privacy Rights Report*, FACEBOOK, (on file with the *Iowa Law Review*) (reporting metrics from 2021) ("Since Meta does not sell personal information, the requirement to provide an opt-out of the 'sale' of data under the CCPA is not applicable.").

152. For the definition of "sale," see CAL. CIV. CODE § 1798.140(t) (West 2018), and after January 1, 2023, see CAL. CIV. CODE § 1798.140(ad) (West 2022). For the definition of "third party," see CAL. CIV. CODE § 1798.140(w) (West 2018), and after January 1, 2023, see CAL. CIV. CODE § 1798.140(ai) (West 2022). *See also* Amy de La Lama & Brian Hengesbaugh, *How to Know if Your Vendor Is a 'Service Provider' Under CCPA*, IAPP: PRIV. ADVISOR (July 30, 2019), https://iapp.org/news/a/how-to-know-if-your-vendor-is-a-service-provider-under-ccpa [https://perma.cc/5EJN-EAGR] ("[T]he CCPA imposes strict requirements on the 'sale' of personal information (e.g., 'Do Not Sell My Personal Information' button on homepages, rights to opt out, and the like). Businesses should, therefore, conduct due diligence on a case-by-case basis as to whether to seek shelter from the definition of 'sale' under the CCPA for disclosures to a 'service provider.' The due diligence

an important insight to policymakers: The data shows that the right to opt-out is relatively popular among consumers but also that consumers of many firms are effectively blocked from using it.

3. Current Lack of Clear Standard and Enforcement

The reporting requirement is meant to promote values of transparency and accountability, but it is lacking in ways that undermine those same values.

First, the reporting requirement does not present firms with a clear standard. The language of the reporting requirement provides a vague threshold that is subject to interpretation: "A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall: (1) Compile the following metrics . . . ."[153] This language suggests that not all firms know how many consumers they actually have or on how many consumers they process personal information. It opens the door for firms to not comply with the reporting requirement based on their alleged lack of knowledge of this matter. Indeed, the regulation was drafted with the intention of capturing not only those firms that "know" but also those that "reasonably should know."[154] But since the number of consumers for which a firm processes personal information is nonpublic information, this language seems toothless. In most cases, therefore, it seems that the regulator will not be able to determine which firms know or reasonably should know that they process the information of a certain number of consumers (without relying on information from within firms).

Second, the language of the reporting requirement covers only specific processing activities—"buy[ing], receiv[ing] for the business's commercial purposes, sell[ing], [or] shar[ing] for commercial purposes"—which are underinclusive.[155] These activities are focused only on the *transfer* of personal information from hand to hand instead of any sort of data use or operations on data.[156] This narrow focus seems to be at odds with the purpose of the reporting requirement to track and measure the overall usage of data control rights. In this context, it should not matter whether the firm has specifically

---

should involve a review under the existing contractual terms and may require modifications to the underlying agreement and obligations of the parties."); Jan Charatan & Eleanor Birrell, Two Steps Forward and One Step Back: The Right to Opt-out of Sale Under CPRA 1 (unpublished manuscript), https://arxiv.org/abs/2312.15094 [https://perma.cc/L2JP-TCYP] (based on two studies finding that the recent amendment to the CCPA that went into effect on January 1, 2023, although "framed as expanding and enhancing privacy rights," included three changes to the law that have "negatively impacted the usability, scope, and visibility of the right to opt-out of sale").

153. CAL. CODE REGS. tit. 11, § 7102(a) (2021).

154. *Id.*

155. *Id.*

156. For the CCPA's definition of "processing," see CAL. CIV. CODE § 1798.140(q) (West 2018) ("'Processing' means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means."). After January 1, 2023, see CAL. CIV. CODE § 1798.140(y) (West 2022).

transferred the personal information of a large amount of people rather than collected or made any other use of a large amount of information.

Third, the reporting requirement does not require firms to report on the reasons they have denied requests, which is a crucial piece missing from the puzzle.[157] Without knowing the reasons for denial, consumers and the regulator cannot ascertain whether firms fully comply with the law, nor whether data control rights include too many exemptions that undercut their potential utility.[158]

Fourth, there is no template for how firms should provide and present their metrics. Consequently, many firms provide metrics in all sorts and fashions, which makes the analysis and comparison of the data challenging. One such example is the lack of coherence in whether firms report on consumers inside or outside of California, and if firms choose to report metrics on a broader territory, they are not required to note what territory they report on.[159] The empirical data suggests that firms are reporting on various territories but without transparency.[160] Another example for the lack of reporting consistency is that firms are not required to note in their report for which products, services, or subsidiaries their metrics apply, which is a major obstacle to understanding the reported data and its scope. And crucially, it is not always clear what exactly firms are counting. This unclarity arises in the case of high-reporting firms,[161] as well as in the case of some low-reporting firms.[162]

Fifth, the reporting requirement is probably not currently enforced. The law does not direct firms' reports to the regulator. The reports are only required to be published on firms' websites.[163] If the regulator wanted to keep track of the metrics, why not require that firms provide the metrics directly to the regulator, in addition to the online publication? Recall, also, that the regulator does not know exactly which firms are supposed to report. The fact that the reporting requirement is set up this way indicates that the regulator is likely not analyzing the metrics or enforcing the reporting requirement.[164]

---

157. The reporting requirement only notes that firms may *choose* to do that, and if so, in a very limiting fashion. *See supra* note 79 and accompanying text.

158. See, for example, the case of the right to opt-out *supra* Section II.D.2.

159. CAL. CODE REGS. tit. 11, § 7102(b) (2021).

160. *See supra* Section II.C.1.

161. *See* discussion *supra* Section II.C.1.

162. *See, e.g.*, *California Privacy Rights*, TIKTOK, https://web.archive.org/web/20221022100520/https://www.tiktok.com/transparency/en-us/california-privacy-rights-2021 [https://perma.cc/6VHK-J594] (noting in their 2021 report that "[t]he above metrics do not include instances where an individual used the 'download your data' and 'delete my account' features without contacting TikTok directly"). This means that the total numbers TikTok has provided for access and deletion requests were partial, but we do not know (and perhaps TikTok does not keep track on) how many more requests were made.

163. CAL. CODE REGS. tit. 11, § 7102(a)(2) (2021).

164. *See* Luthi, *supra* note 131 ("The state DOJ wrote the transparency rule into the regulations, but it does not keep a full list of firms that must comply with it — those that collect the personal data of at least 10 million Californians each year. There is no central repository for the businesses' data, forcing the public to track down each company's numbers in a time-consuming and convoluted way.").

Not monitoring or enforcing the reporting requirement may also lead to weakened enforcement of the substantive rights under the CCPA, as the metrics have the potential to reveal behaviors of noncompliance with the law.

Lastly, 10,000,000 consumers is a significant number that poses a very high threshold. If only a small group of firms is required to report, the regulator and the public receive partial information on the law's performance on the ground. The threshold was not always so high. In 2019, the originally proposed CCPA Regulations included a much lower threshold of 4,000,000 consumers, but industry lobbying had raised the threshold to what it is today.[165]

These deficiencies boil down to a structural problem: Why did the regulator choose to institute a reporting requirement that applies only to a small pool of firms, is unclear and subject to interpretation, where the reported information is hard to follow, compare, and analyze, and carrying out effective enforcement seems to be a challenge?

III. THE NATURE OF DATA CONTROL RIGHTS AND RAMIFICATIONS OF LOW USAGE

We now have empirical evidence that very few people use their data control rights. The next step is to ask: What does it mean?

Broadly, there are three potential perspectives to understanding the results. First, we can focus on firms. Perhaps firms are doing a good job—they handle personal information with care and loyalty toward consumers and do not digress from consumers' preferences and interests with respect to their personal

165. *See* State of Cal. Dep't of Just., Text of Proposed California Consumer Privacy Act Regulations § 999.317(g) (proposed Oct. 11, 2019), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf [https://perma.cc/2F5A-ZJLY] ("A business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall . . . [c]ompile the following metrics for the previous calendar year . . . ."); *see also* State of Cal. Dep't of Just., Proposed California Consumer Privacy Act Regulations, FSOR Appendix C: Summary and Response to Comments Submitted During First 15-Day Comment Period, Public Comments #W256-5, #W297-6 and Response #231, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-c.pdf [https://perma.cc/QDK8-9RQF] ("Summary of Comment[:] . . . Lower the 10 million threshold in this subsection. Comments claim that the modified threshold would decrease transparency and exclude virtually all businesses whose entire business model is premised on collecting and selling personal information, such as biometrics firms, attribution firms, data analytics firms, and facial imaging, recognition, and image matching firms and insurers, as well as businesses that specialize in intelligence gathering, covert operations, data harvesting, and untraceable equipment interference. . . . [OAG] Response[:] . . . No change has been made in response to this comment. In drafting the regulation, the OAG balanced the burden and the benefits of compilation and reporting by limiting the requirements to those businesses that handle a large amount of personal information. Upon consideration of previous comments, the threshold was modified to 10 million consumers, which amounts to approximately 25 [percent] of California's total population, to alleviate the burden on smaller businesses."); State of Cal. Dep't of Just., Proposed California Consumer Privacy Act Regulations, FSOR Appendix E: Summary and Response to Comments Submitted During Second 15-Day Comment Period, Public Comment #W352-5 and Response #79, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-e.pdf [https://perma.cc/GU8R-AHC5] ("Summary of Comment[:] . . . Supports the increase in the threshold from 4 million to 10 million consumers. . . . [OAG] Response[:] . . . The OAG appreciates this comment of support. . . . The comment concurred with the proposed regulations, so no further response is required.").

information. For these reasons, there is no wide need among consumers to use the rights, hence the low usage. But this explanation seems unlikely. We know firms are *not* doing a good job: Countless data breaches,[166] covert surveillance techniques,[167] scandals (like Cambridge Analytica),[168] and misaligned financial interests,[169] tell us so. If anything, the behavior of firms is what prompted these rights in the first place. Beyond that, how would consumers know whether firms are doing a good job of maintaining their privacy? There is an epistemic leap in this explanation—if consumers do not use their right to know, they cannot tell what information firms keep on them and what information firms potentially exploit or sell to others. And the results reveal that the right to know is the least used right. Thus, the low usage of data control rights does not stem from firms' good behavior.

Second, we can focus on consumers. The reason for the low usage of data control rights could be that consumers are uninterested in their rights; while consumers repeatedly *say* they are concerned about their privacy and that they want more privacy controls, they do not act accordingly.[170] This dynamic has been called the "privacy paradox."[171] According to the logic of the privacy paradox argument, it seems most California voters, through their vote to approve the CCPA, demonstrated that they want data control rights,[172] but in reality most of them refrained from using those same rights. If we embrace this logic, the results are similar to other cases indicating the privacy paradox, though on a larger scale. But there are good reasons not to embrace this logic—either because, for various reasons, people's behavior does not accurately reflect their preferences or needs,[173] or, as Solove explains, because the

166. *See, e.g.*, DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 5–7 (2022).

167. *See, e.g.*, Corren, *supra* note 9, at 584–86.

168. *See, e.g.*, sources cited *supra* note 2.

169. Ayelet Gordon-Tapiero & Yotam Kaplan, *Unjust Enrichment by Algorithm*, 92 GEO. WASH. L. REV. 305, 334–35(2024).

170. Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 2–4 (2021).

171. *Id.* at 2.

172. *See California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)*, BALLOTPEDIA, (2020), https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020) [https://perma.cc/45CZ-MGY3] (56 percent of the voters voted to approve the law).

173. *See, e.g.*, Solove, *supra* note 170, at 15–22; Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038, 1039 (2017); Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, *in* ECONOMICS OF INFORMATION SECURITY 165, 172–75 (L. Jean Camp & Stephen Lewis eds., 2004); Laura Brandimarte, Alessandro Acquisti & George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCH. & PERSONALITY SCI. 340, 341 (2012); Serge Egelman, Janice Tsai, Lorrie Faith Cranor & Alessandro Acquisti, *Timing Is Everything?: The Effects of Timing and Placement of Online Privacy Indicators*, 2009 PROC. SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS. 319, 324; Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249, 268 (2013); SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING: (AND WHY WE SHOULD WORRY) 84 (2011); WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2018); Ari Ezra

privacy paradox is but a myth.[174] The results could also mean that consumers are underinformed about the rights, that the rights are not widely available, that consumers do not believe the benefits of the rights exceed the costs of using them, that the rights are not usable enough, or that firms use dark patterns to dissuade consumers from using their rights. I address these potential explanations in Part IV.

The first two perspectives focused on firms and consumers pose potential *causes* for the empirical results. The rest of this Part, however, develops a third perspective that focuses on the rights themselves and sheds light on the *ramifications* of the empirical results. I argue that the results expose that data control rights are weak rights that are prone to fail. This weakness stems from the fact that data control rights require constant activity and invocation by right holders, otherwise, they provide no protection.

Section III.A develops a better understanding of the nature and logic of data control rights. Then, Section III.B maps the desired effects of data control rights, in theory, and explores how their regulatory design mostly fails to achieve such effects.

A. THE LOGIC OF DATA CONTROL RIGHTS

This Section sheds light on how data control rights work and their logic. Such logic dictates the level of protection data control rights offer, and importantly, it makes data control rights weaker rights that are prone to fail in achieving their goals.

The idea behind data control rights is to create new abilities for individuals to ask firms to do certain things with personal data, such as have access to such data, delete it, or stop its sale. Data control rights are thus a regulatory mechanism that is premised on the action of individuals: At their core, data control rights are meant, essentially, to be invoked. Such invocation is necessarily a high-intensity activity—there are hundreds if not thousands of firms that participate in the information economy, and the relationship between individuals and each and every one of those firms is potentially impacted and entangled by data control rights. Not only that, but the information economy is far from being a set of static transactions. Rather, it is a network of dynamic relationships where each decision and each piece of data collected may impact

Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OP. PSYCH. 105, 105 (2020); Arvind Narayanan, Arunesh Mathur, Marshini Chetty & Mihir Kshirsagar, *Dark Patterns: Past, Present, and Future*, COMMC'NS ACM, Sept. 2020, at 42, 42–43; Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, PROC. ACM ON HUM.-COMPUT. INTERACTION, Nov. 2019, at 1, 2; Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 43–44 (2021); Lauren E. Willis, *Deception by Design*, 34 HARV. J.L. & TECH. 115, 116–17 (2020).

174. Solove, *supra* note 170, at 23 ("Properly understood, the behavior in the privacy paradox studies is about preferences that involve risk assessments in contextual situations. In contrast, people's attitudes about privacy are often stated more generally—applying across different contexts. Thus, there is no inconsistency between behavior and attitudes because they are about very different things.").

downstream decisions and further data collection, thus making invocation a continuous effort.[175]

What happens if data control rights are not invoked? Since we now know that, for the most part, data control rights are left unused, this is a crucial question. Do data control rights offer protection if they are unexercised? The trouble with data control rights is that to be useful and have an effect, individuals need to actively use them against firms. Unless operationalized, data control rights do not offer protection, and they do not otherwise impact firms or individuals in any significant way. And in the event they are indeed invoked—their successful exercise is contingent on the firm's cooperation and compliance.

Another way to think about data control rights' lack of protection sans invocation is to consider how deeply conditional they are. Correlated with every right is a duty.[176] What duty is correlated with data control rights? These rights are mostly rights *to request* certain action from a firm,[177] thus the correlated duty transpires only when the right is invoked. Data control rights require individuals to be aware of their existence and be proficient in requesting them. Moreover, because these rights are typically far from absolute—they include many limitations and exemptions[178]—the duty of the firm is to receive the request, consider it, and decide (and communicate) whether the firm will

175. *See* Solove, *Limitations of Privacy Rights*, *supra* note 6, at 978, 984–93.

176. *See* Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16, 32 (1913) ("When a right is invaded, a duty is violated.") (citation omitted); J. Raz, *On the Nature of Rights*, 93 MIND 194, 196 (1984).

177. For the right to know, see CAL. CIV. CODE §§ 1798.100(a), 1798.110(a), and 1798.115(a) (West 2018). After January 1, 2023, see only CAL. CIV. CODE §§ 1798.110(a) and 1798.115(a) (West 2022). For the right to delete, see *id.* § 1798.105(a) (West 2018). For the right to opt-out, see *id.* § 1798.120(a) (West 2018).

178. Firms may use several denial grounds, or exemptions, like that the request is found by the firm to be "unverifiable," *id.* §§ 1798.110(b), 1798.115(b) (West 2018), "unfounded or excessive," *id.* § 1798.145(i)(3) (West 2018), and after January 1, 2023, see *id.* § 1798.145(h)(3) (West 2022), or that the firm holds compliance to be restrictive of its ability to comply with laws and legal obligations, exercise its legal claims or rights, or defend its legal claims, *id.* § 1798.145(a) (West 2018). There are additional general exemptions from complying with the CCPA. *Id.* § 1798.145 (West 2018). Specifically for the right to delete, the firm is entitled to broad exemptions—nine specific grounds to deny requests to delete, in addition to the exemptions that apply to the other rights—making the right to delete quite limited. *See* CAL. CIV. CODE § 1798.105(d) (West 2018). As of January 1, 2023, a firm can also deny the request on the grounds that it is a "service provider" serving another firm and thus not required to respond to an individual's deletion request, although the individual may not even know who is the firm for which the service provider processes their personal information. *See* CAL. CIV. CODE § 1798.105(c)(3) (West 2022); *see also* California AG Website, *supra* note 55 ("D. Requests to Delete. . . . 6. Why did I get a response that the business is a service provider that does not have to act on my request? . . . The CCPA treats service providers differently than the businesses they serve. It is the business that is responsible for responding to consumer requests. . . . If a service provider has said that it does not or cannot act on your request because it is a service provider, you may follow up to ask who the business is. However, sometimes the service provider will not be able to provide that information. You may be able to determine who the business is based on the services that the service provider provides, although sometimes this may be difficult or impossible."). Regarding the right to opt-out, firms are exempted from complying with the right when requests are suspected as fraudulent. CAL CODE REGS. tit. 11, § 7026(g) (2021). After March 29, 2023, see CAL CODE REGS. tit. 11, § 7026(e) (2023).

comply with the request or deny it.[179] Thus, data control rights create a duty which is *conditional* and often *partial*.[180] They are conditional both on the individual's invocation of them, and on the firm's granting or denying them. They are partial because of their many limitations and exemptions. In other words: Not only do data control rights require constant invocation, but firms also have the power to deny invoked rights.

Unlike other rights, data control rights also lack *perceptibility*. Individuals may try to use their data control rights, but can they tell whether it made a difference? The answer is often no. Unlike other rights, where it is typically observable and clear what effects they have or do not have—e.g., my property remains intact, my speech is not limited (or the opposite)—data control rights have an impact, to the extent they do, on an unreachable and unseen object: the trade-secrecy- and intellectual-property-protected information systems of firms.[181] If an individual invoked their data control right, and the firm responded that it has complied, still the individual cannot really tell whether and to what extent their right was realized. For example, after invoking the right to opt-out, it is not transparent to the individual whether the firm has truly stopped selling the individual's personal information. This lack of transparency means that the individual cannot be certain that their right was fulfilled and that their information is off the market. Indeed, a few studies found that the right to opt-out is not consistently fulfilled, and personal information of consumers who have opted-out still circulates through the market.[182] This could also be true for the right to delete information.[183]

B. BACK TO THE GOALS: ARE DATA CONTROL RIGHTS EFFECTIVE?

If only very few people use their data control rights, are data control rights working as lawmakers intended? The answer depends on the goals of the law. Recall that the standard articulation of the goals of data control rights is power balancing, as discussed in Part I. According to this view, the goal of data control rights is to increase the power of consumers vis-à-vis firms by allowing consumers to make certain decisions about the personal information that is collected and used by firms.

---

179. CAL. CIV. CODE §§ 1798.110(b), 1798.115(b) (West 2018) (right to know); *id.* § 1798.105(c) (West 2018) (right to delete).

180. *See* Raz, *supra* note 176, at 196–97.

181. *See, e.g.*, Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1515 (2020); Amy Kapczynski, *The Public History of Trade Secrets*, 55 U.C. DAVIS L. REV. 1367, 1370–71 (2022).

182. *See, e.g.*, Zengrui Liu, Umar Iqbal & Nitesh Saxena, *Opted Out, Yet Tracked: Are Regulations Enough to Protect Your Privacy?*, 2024 24TH PRIV. ENHANCING TECHS. SYMP. (forthcoming 2024) (manuscript at 12), https://arxiv.org/pdf/2202.00885.pdf [https://perma.cc/HL75-ZUDH]; Duc Bui, Brian Tang & Kang G. Shin, *Do Opt-Outs Really Opt Me Out?*, 2022 PROC. ACM SIGSAC CONF. ON COMPUT. & COMMC'NS SEC. 425, 433–35.

183. *See, e.g.*, Alex Hern, *Ashley Madison Database Suggests Paid-Delete Option Left Identifiable Data Intact*, GUARDIAN (Aug. 19, 2015 4:08 PM), https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-paid-delete-option-left-data-identifying-users-post-claims [https://perma.cc/R79U-DN86] ("Date of birth, postcode and other personal data still appear on hacked database of infidelity site – even for accounts that paid for 'full delete' service . . . .").

In this Section, I propose a more granular account of how data control rights might achieve their power-balancing goal. I first examine the question of what desired effects can theoretically be accomplished by the invocation of data control rights. I then analyze whether it is likely that those desired effects can be accomplished with the very low usage of data control rights.

1. Desired Effects

I propose two power-balancing effects. First, an *individual upshot*. If an individual knows a record about them contains a mistake, they could get the mistake corrected; if they want out of a service, they could delete the information the firm holds on them; if they are not interested in the firm selling their personal information, they can opt-out, and so on. We need to assume the firm will comply with such requests—this is not a given—but if the firm complies, then the right arguably works well.[184] In economic terms, data control rights potentially increase consumer choice; if one can choose to delete their account or opt-out of the sale of personal information at any time, it means one is free to make choices about their personal information, including moving between services without informational "strings attached."[185] Similarly, the right to know potentially provides information about what data was collected on a consumer, thereby facilitating and encouraging consumers to make informed choices in the market about what services they use and what information they share with those services.

These rights may also assist individuals in avoiding or overcoming harms that stem from online abusive behavior such as stalking, harassment, defamation, fraud, and nonconsensual sharing of intimate details and images.[186] By using their data control rights to require a website to delete or stop sharing harmful, abusive, defamatory, or fraudulent information about them, an individual is not left helpless in the face of abuse that is made possible by a firm's platform.[187]

The second power-balancing effect is *market-scale control*.[188] If enough individuals use their rights on an ongoing basis, in theory, it can lead to

184. *But see supra* notes 182–83 and accompanying text.

185. *See, e.g.*, DAVID SINGH GREWAL, NETWORK POWER: THE SOCIAL DYNAMICS OF GLOBALIZATION 106–16 (2008) (discussing the importance of alternatives for decision-making).

186. *See, e.g.*, Thomas E. Kadri, *Brokered Abuse*, 3 J. FREE SPEECH L. 137, 138 (2023); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1874 (2019).

187. *See, e.g.*, Kadri, *supra* note 186, at 148; *cf.* Farai Chideya, *Some Dude Created an Ashley Madison Account Linked to My Gmail, and All I Got Was This Lousy Extortion Screen*, INTERCEPT (July 21, 2015, 2:13 PM), https://theintercept.com/2015/07/21/ashley-madison-breach-why-am-i-getting-their-emails [https://perma.cc/TQM3-MNC5] ("A man with my name somehow created an Ashley Madison account, which — as the latest hack reveals — I am unable to delete without paying.").

188. *Cf.* Solove, *Limitations of Privacy Rights*, *supra* note 6, at 989 ("Privacy rights work differently than many constitutional or statutory rights. For example, when a person challenges a law based on the right to free speech under the First Amendment to the U.S. Constitution, the judicial decision has effects that go far beyond the person's case. The law might be partially or fully invalidated. The person's challenge thus leads to a result that has broader societal effects. In contrast, exercising a privacy right often merely affects that individual. For example, if an individual gains access to her records or deletes data from her records, this has no larger societal impact. More generally, privacy rights contribute only in a minor way to the larger societal

improved quality of products and services and enhance competition over quality in the market. That is because intensive use of rights by consumers can potentially put pressure on firms to improve their privacy and data processing practices for the purpose of minimizing the need for consumers to use their rights and thus save the costs of dealing with such individual requests. From receiving complaints to processing them, including providing access to records, correcting or deleting records, and eventually responding to each individual—handling intensive invocation of data control rights could be costly.[189] Beyond the incentive to avoid these costs, if enough individuals use their rights on an ongoing basis, firms might be incentivized to prevent other consequences of their data processing practices. For example, if a firm's exploitative or unsafe practices result in a data breach that causes consumers to delete their information or abandon the business in droves, the firm will likely want to change its data processing practices. Additionally, if consumers are paying (fully or partly) for services and products by giving away their personal information, rights that limit such giveaways—such as the right to delete and the right to opt-out—may effectively lower the probably overcharged informational price consumers pay.[190]

Specifically for rights such as California's right to opt-out of the sale of personal information, we could expect that if enough individuals indeed opt-out, then firms' databases will shrink over time, and that could have a lasting effect on shifting the information economy from monetizing personal information to other business models,[191] such as paid services.[192]

2. Can Low Usage Yield the Desired Effects?

Given the logic of data control rights, what amount of usage is likely to yield the desired effects? Put another way, is it likely that the very low usage of data control rights is capable of accomplishing the desired effects?

Per the market-scale control effect, it seems safe to posit that this effect is not materializing and will not be materializing anytime soon. The very low usage does not sit well with our expectations for how data control rights would have a market-scale impact. If only very few consumers use their rights, we can expect nothing to change as a result of having these rights in the law. The

interests involved with privacy. Their effects are far more individualistic than constitutional rights."); Waldman, *Privacy, Practice, and Performance*, *supra* note 8, at 1254 ("[*I*]*ndividual* rights will not solve *collective* privacy problems.").

189. This is assuming firms do not find noncompliance costs lower, and noncompliance benefits higher, than compliance costs and benefits respectively.

190. *See, e.g.*, Rory Van Loo, *Broadening Consumer Law: Competition, Protection, and Distribution*, 95 NOTRE DAME L. REV. 211, 216–17 (2019).

191. *See also* Waldman, *Privacy's Rights Trap*, *supra* note 8, at 94 ("I suppose it is possible that if enough of us exercise our individual rights to delete, port, and opt out of tracking, things might change. We could conceivably starve the information industry of the materials and labor it needs to extract population-level insights from individual users.").

192. Cristobal Cheyre, Benjamin T. Leyden, Sagar Baviskar & Alessandro Acquisti, *The Impact of Apple's App Tracking Transparency Framework on the App Ecosystem* 18 (CESifo, Working Paper No. 10456, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4467977 [https://perma.cc/5DP4-ZH7W].

potential market-scale scenarios and outcomes we explored depend on individuals using their rights on an ongoing basis, and such use needs to be done by a significant number of consumers. This deficiency in how the law plays out in the market leaves a gaping hole: If data control rights are the main solution advanced by the law, and it does not work, what are we left with?[193] The crux of the problem is that if data control rights lie dormant, they are just rights on paper. And if we expect these rights to act as forces that make markets work better, then their lack of invocation is bad news.

As for the individual upshot effect, it is harder to say whether it works as intended. First, we do not have information on who the individuals that invoked their data control rights are, what their motivation and needs were,[194] and finally, whether the invocation of their rights was complied with by firms *and* fulfilled their particular need. Additionally, as discussed in Section III.A, one dubious quality that sets data control rights apart from other rights is that *we cannot tell* whether data control rights were actually fulfilled, even when the firm tells us so. Data control rights involve unseen mechanisms and opaque results, lacking crucial transparency.

Second, it is also hard to quantify how many individuals are likely to *need* those rights in the first place. If we had known or had an estimation of the number of individuals needing to use their rights, we could approximate, based on the usage metrics, whether most such individuals benefitted from having the rights. Though we do not have direct information on this question, we can focus on one important right—the right to delete—and learn from an illustrative example how many people might need to use it.

The right to delete is a good remedy for when one discovers inaccuracies or errors in their personal information.[195] Although it is unknown how many mistakes are generally made in the dossiers firms continuously collect, process, and update on individuals, we do have information on how many mistakes are made in consumer credit reports prepared by consumer reporting agencies. In 2004, Congress instructed the FTC to complete by 2014 "an ongoing study of the accuracy and completeness of information contained in consumer reports prepared or maintained by consumer reporting agencies."[196] The main results of this national study were concluded in 2012 and indicated that 26 percent of participants in the study "identified at least one potentially material error on at least one of their three credit reports,"[197] with "[c]onfirmed

193. *See, e.g.*, Waldman, *Privacy's Rights Trap*, *supra* note 8, at 91–93.

194. *See* Solove, *Limitations of Privacy Rights*, *supra* note 6, at 995–97, 1002.

195. Another good remedy for errors and inaccuracies is the right to correct, but it only became operable under the CCPA on January 1, 2023. Consumers' usage of the right to correct is expected to be included in metrics reports as of July 2024.

196. *See* Fair and Accurate Credit Transactions Act of 2003 § 319, 15 U.S.C. § 1681 (2004).

197. FED. TRADE COMM'N, REPORT TO CONGRESS UNDER SECTION 319 OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003 i (2012) [hereinafter FTC REPORT], https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf [https://perma.cc/B9EM-PU5R]; Press Release, Fed. Trade Comm'n, FTC Testifies on Credit Reporting Accuracy Study, FCRA Enforcement, Credit Education (May 7, 2013), https://www.ftc.gov/news-event

error rates at the consumer level rang[ing] from 10 [percent] to 21 [percent]."[198] While not an apples-to-apples comparison, if the frequency of errors in firms' personal data dossiers is similar, or even half of that, then these findings suggest that we should expect a much higher percentage of individuals in need of the right to delete than the percentage of consumers actually using it under the CCPA (i.e., no more than 1 percent of consumers for 90 percent to 93 percent of firms in both years).[199]

The low usage of data control rights exposes the weakness of these rights. Without active and constant invocation, data control rights do not provide benefits to consumers—not individually and not as a group, not as a solution to individual problems and needs, and not as a control mechanism on a market scale.

IV. THE MEASUREMENT PUZZLE

The information economy is driven by the accumulation of personal information. It is built on trackable processes and networks. It is run by some of the world's most resourceful firms. And it attracts the attention of citizens, consumers, policymakers, courts, and researchers. Despite all that, our knowledge of how it works and affects individuals and society is still limited.[200] We are in the dark about many questions.[201] One of these questions is how to

---

s/news/press-releases/2013/05/ftc-testifies-credit-reporting-accuracy-study-fcra-enforcement-credit-education [https://perma.cc/2Z6F-K6LE].

198. *See* FTC REPORT, *supra* note 197, at iv.

199. Another example is errors in medical records. *See* Solove, *Limitations of Privacy Rights*, *supra* note 6, at 1009 ("A health IT expert estimates that about 70 [percent] of medical records have errors.") (citing Christina Farr, *This Patient's Medical Record Said She'd Given Birth Twice — In Fact, She'd Never Been Pregnant*, CNBC (Dec. 9, 2018, 8:25 PM), https://www.cnbc.com/2018/12/09/medical-record-errors-common-hard-to-fix.html [https://perma.cc/7FRN-4CWQ]).

200. *See, e.g.*, Waldman, *Privacy's Rights Trap*, *supra* note 8, at 101 ("The information industry is taking its cues from big polluters. Technology companies publish statements about transparency, but fire researchers as soon as their scholarship highlights biases and erasure encoded in profitable algorithms. Industry mouthpieces will focus on consent and access when any issue comes up, but never speak about industry's power to control the collection and processing of data without any accountability from independent researchers. . . . Information companies protect their bottom line by utilizing these sleight of hand tactics to distract the public with empty gestures while continuing to collect and sell their private data." (footnotes omitted)); Thomas E. Kadri, *Platforms as Blackacres*, 68 UCLA L. REV. 1184, 1186–87 (2022); Nathaniel Persily, *Facebook Hides Data Showing It Harms Users. Outside Scholars Need Access.*, WASH. POST (Oct. 5, 2021, 7:20 AM), https://www.washingtonpost.com/outlook/2021/10/05/facebook-research-data-haugen-congress-regulation (on file with the *Iowa Law Review*).

201. *See, e.g.*, Kurt Wagner, *Congress Doesn't Know How Facebook Works and Other Things We Learned from Mark Zuckerberg's Testimony*, VOX (Apr. 11, 2018, 8:19 PM), https://www.vox.com/2018/4/11/17226742/congress-senate-house-facebook-ceo-zuckerberg-testimony-hearing [https://perma.cc/5J6M-5N5B] ("It was clear from the questions this week that a lot of the lawmakers don't full[y] understand how Facebook's business or services work . . . . It's easy to chastise lawmakers for not having a firmer grasp on how this stuff works. But the reality is that, with well over two billion users, it's likely that there are a lot of Facebook users who don't understand how the business or services actually work. That's on Facebook . . . ."); Mike Snider, *Congress and Technology: Do Lawmakers Understand Google and Facebook Enough to Regulate Them?*, USA TODAY (Aug. 2, 2020, 6:02 AM), https://www.usatoday.com/story/tech/2020/08/02/google-facebook-and-amazon-too-technical-congress-regulate/5547091002 [https://perma.cc/3G7L-SFLP] ("Many of us have

explain the empirical finding that very few people use their data control rights, especially in light of the popularity of these rights among regulators. But we do not know enough about data control rights and the ecosystem in which they operate to answer that question. Can we know more? This Part begins to bridge our informational gaps by mapping what we do not know—but should know—in order to fully understand how data control rights operate and what hinders their utility and impact.

California introduced a first-of-its-kind reporting requirement that holds much promise: providing the public and policymakers access to key data about the usage of data control rights and firms' compliance with privacy laws. I argue we should embrace this approach and expand upon it. Privacy laws and other laws governing the information economy should set measurable metrics, including metrics that firms need to collect and provide to regulators and the public. California's regulation is a good starting point, but it can be broadened and improved, as I explore in this Part.

To be clear, despite their low usage, I do not believe, nor do I argue, that lawmakers and regulators should remove data control rights from laws or give up on the potential benefits data control rights might bring to individuals. Firms *should* provide data control rights to individuals, and individuals *should* be able to know, delete, correct, opt-out, and otherwise impact their personal information and what is being done with it, with two qualifications: First, my study reveals that very few people are using data control rights, but it does not directly point to the reasons for that result. While the general experience with consumer markets shows that if curbing certain exploitative firm behavior is mostly dependent on the action of consumers, it likely will not be effectively curbed,[202] this Part proposes concrete (potential) reasons for the low usage together with ways to go about measuring them, with the ultimate goal of *improving* data control rights and their beneficial effects. Second, this last Part is only one piece—the first—of the measurement puzzle. Parts II and III together show that data control rights are currently failing, but even if they were to be improved, they would not be enough to regulate the relationship between firms and individuals in the information economy.[203] Data control rights are therefore important but should not be the only focus for regulation going forward. Thus, I argue that those future supplemental regulatory mechanisms should contain measurable goals and measurement means, and in that sense, this Part is but one example of how this can be done.

---

had the feeling that technology, which continues to change at an ever-dizzying pace, may be leaving us behind. That was embodied . . . during a Congressional hearing . . . investigat[ing] antitrust concerns of four big tech titans: Amazon, Apple, Facebook and Google. . . . [T]he House Judiciary subcommittee hearing laid one thing bare: A sizable disconnect appears to exist between the technology Americans are using and depending on in their daily lives and the knowledge base of people with the power and responsibility to decide its future and regulation.").

202. *See, e.g.*, Corren, *supra* note 9, at 598.

203. *See supra* notes 14–15, 73–74 and accompanying text.

A. WHAT TO MEASURE

If we want to know whether data control rights are useful to people and how much current approaches centered around data control rights are working, we should first measure whether and to what extent data control rights are being used. The CCPA's approach of measuring the number of *invoked rights* is a good start.

However, usage of data control rights and trends in usage can be explained by several different reasons, and each of them is worth measuring separately: (1) the availability of data control rights; (2) the extent to which people are informed on data control rights; (3) data control rights' ease of use; and (4) the benefits data control rights provide to individuals.

First, the overall *availability of data control rights* is determined by the number of firms that provide them. Not all firms fall under the ambit of the CCPA, and those that do not are not required to provide CCPA data control rights. Additionally, exemptions from providing the rights, such as those relating to the right to opt-out,[204] can decrease the overall availability of data control rights.

Second, *the extent to which people are informed* about the existence of data control rights can impact their usage: If people are uninformed, they will not use the rights. The CCPA does attempt to increase awareness among consumers.[205]

Third, *data control rights' ease of use* is crucial: If firms make it hard to invoke data control rights, then most people will not use them. Poor ease of use may result from the law requiring a low usability standard or from the ways in which firms implement the law in their user interfaces (or from both). For example, the CCPA does not require a high level of usability when it comes to the rights to know and delete, but it does require a more streamlined and easy process when it comes to the right to opt-out.[206] Apart from what the law requires, firms might use design ruses and dark patterns to dissuade people from using their rights.[207]

Fourth, *how much benefit data control rights provide* to people will affect their level of use: If rights are very helpful and effective, people will use them more, and vice versa. Recall that the data does not tell us who the individuals who have invoked their data control rights are, their motivation and needs, nor whether the invocation of their rights was complied with by firms and benefitted them as they expected. We also do not know how many individuals are likely to need those rights for their individualized cases in the first place.

Data control rights' usage may be affected by any of these factors. For example, data control rights may be highly available and easy to use, with a

204. *See* discussion *supra* Section II.D.2.

205. *See* discussion *supra* Section II.D.

206. *See supra* Section II.D.2.

207. *See supra* notes 149–52 and accompanying text; *see also* Narayanan et al., *supra* note 173, at 43–44; Mathur et al., *supra* note 173, at 1; Waldman, *supra* note 173, at 107; Luguri & Strahilevitz, *supra* note 173, at 44–48; Willis, *supra* note 173, at 116–21.

high level of awareness among consumers, but without being very beneficial to individuals. They could also be highly beneficial and effective without being highly known, available, or easy to use. Therefore, it is important to measure all these factors and, subject to natural measurement limitations, to measure each factor separately.

Another important measurement is firms' *compliance and noncompliance* with invoked rights, as the CCPA indeed attempts to incorporate. But we should not stop at mere compliance rates—it is important to know what firms' denial reasons are and what the distribution of denial reasons is across all denied rights. Denial rates and denial reasons provide more information on the strength and effectiveness of data control rights, what can be thought of as their "return on investment." If people go through the trouble of invoking their data control rights but end up being denied, they might not try again.

The other important part of data control rights' "return on investment" is whether they are actually fulfilled (when not denied). This question concerns data control rights' *lacking perceptibility*.[208] Regulators should require firms to verify the proper deletion and opting out in response to invoked rights and to provide data on their verification processes and their success.

B. HOW TO MEASURE

Invoked rights

First, to know how many people use their data control rights, firms need to measure the invocation of rights by *unique people*, and not how many browsers or devices have "invoked" data control rights or how many requests were submitted through various channels. Measuring browser requests, device requests, or other types of requests without attaching these requests to a specific person skews and artificially inflates the measurement.

One example of such inflated measurements is the case of Oracle discussed above.[209] Another example is the case of the 2021 metrics report of The Weather Company (weather.com).[210] The Weather Company reported around 2,700,000 opt-out requests for 2021, a very high number.[211] This number is noted to apply only to California consumers.[212] This number is significantly different (by a large gap) from the number of requests for the other rights—around 1,500 requests to know, and around 20,700 requests to delete.[213] What explains this peculiar number is the following note in the report:

> In an effort to take a privacy forward approach, total opt out requests include CA users: 1. Who opted out by accessing the Do Not Sell

208. *See* discussion *supra* Section III.A.

209. *See supra* notes 133–35 and accompanying text.

210. *See Privacy Policy*, WEATHER CHANNEL, https://web.archive.org/web/20221221220055/https://weather.com/en-US/twc/privacy-policy#us-ccpa-notice-new [https://perma.cc/W4A6-2XQG] (reporting in Section 12 metrics from 2021).

211. *Id.*

212. *Id.* ("This section provides metrics of requests from users located in California made between January 1, 2021, and December 31, 2021.").

213. *Id.*

> My Personal Information link on weather.com and our mobile applications[;] 2. Who visited weather.com with Global Privacy Control enabled on web browsers[;] 3. Who visited weather.com with a web browser set to block all cookies, as TWC also honors this as an opt out request[.][214]

The Weather Company's approach is indeed supportive of privacy, but the number they provide does not represent a realistic picture of how many people invoked their data control rights. Since the firm did not provide requests by unique persons but rather a sum of all sorts and types of requests received through multiple channels, it is highly likely that many people were counted more than once. It is also unclear how the firm counted signaling by GPC and cookie blockers since such signaling is made by the user browser to the firm's server per a user website visit, so it could be that a person who uses either (or both) tools was counted every single time they visited the website from the browser on which these tools were installed. It means that if a person with a cookie blocker or GPC installed on their browser is regularly entering weather.com to check the weather, for example, twice a week, then over the course of a year, this one person would be counted as roughly 100 persons.

All that said, it could be that what is good for accurate measuring is bad for privacy. Not knowing exactly who uses GPC or cookie blockers is a pro-privacy approach. Additionally, it could be technologically difficult to connect all these different automatic signals and requests to identify unique people. Even if, for these reasons, policymakers decide that opt-out requests will not or cannot be measured more accurately, firms still need to better explain what it is they are reporting on, like whether they could be counting single consumers more than once (and how many times, at least approximately). Most importantly, the regulator should require firms to report on *the same types of requests, and in the same manner and form*, to allow comparing apples to apples across firms. Currently, each firm decides how and what it reports, and most firms do not provide sufficient details on their choice.

Second, when measuring invoked rights, it is important to know the total number of consumers in the relevant consumer base, or we cannot put the numbers in context or compare between firms. A related point is knowing the territory for which the reported data applies. This is important for comparisons between firms, and because it may reveal specific trends or different usage patterns across different territories.

Data control rights' ease of use

The regulator should adopt a mandatory usability standard as a first step. The usability standard should require that website navigation and the presentation of privacy choices not be misleading but clear and coherent.[215]

---

214. *Id.*

215. *See, e.g.*, Habib et al., *An Empirical Analysis, supra* note 149, at 396; Arunesh Mathur, Mihir Kshirsagar & Jonathan Mayer, *What Makes a Dark Pattern . . . Dark? Design Attributes, Normative Considerations, and Measurement Methods*, 2021 PROC. CHI. CONF. ON HUM. FACTORS COMPUTING SYS., 1, 9–13.

Fonts, sizes, and colors should be standardized so users would have a consistent and intuitive experience across websites.[216] The usability standard could be tested and verified.[217] Based on the usability standard, the regulator could audit and measure data control rights' ease of use on firms' websites. Additionally, the regulator could require firms to report on the "conversion rate,"[218] i.e., how many individuals went into a webpage with a data control right request form or a toggle of privacy choices (or the like) but did not end up filling out the form or making a change to their privacy choices. This metric can be used to indicate problematic usability.

How beneficial are data control rights?

This is perhaps the most complicated factor to measure. The first step is a legal analysis of the respective data control rights, mapping what the rights potentially provide (and what they do not), to whom, and under what conditions. Based on such legal analysis, the regulator should create a consumer survey that examines the costs and benefits consumers attribute to invoking data control rights. Another type of survey could be similar to the FTC's credit report survey,[219] where the regulator follows the whole process of invoking rights with a cohort of consumers to examine in which situations consumers are in need of data control rights, how they experience the process of invoking their rights, what is the outcome of the invocation of their rights (complied or denied), and whether a positive outcome is beneficial to them and meets their initial need. However, because of the imperceptibility problem, such surveys might be limited in their conclusions, as consumers would not be able to verify that their rights were actually fulfilled.

Availability of data control rights

To quantify the availability of data control rights, the regulator should keep track of firms' use of exemptions and firms' noncompliance behavior by analyzing reported compliance rates and noncompliance reasons, especially focusing on firms that report relatively low or zero usage for certain rights, e.g., as discussed above for the right to opt-out.[220]

C. *WHO MEASURES AND REPORTS*

There are two problems with the current threshold that defines which firms should measure and report the metrics: First, it is underinclusive, and second, it is based on nonpublic information. To have a fuller picture of the impact and usage of data control rights and privacy laws, a larger pool of firms

216. *See, e.g.*, Lorrie Faith Cranor, *Informing California Privacy Regulations with Evidence from Research*, COMMC'NS ACM, Mar. 2021, at 29, 32.

217. *Id.* at 30–31.

218. *See, e.g.*, *What Is Conversion Rate?*, COURSERA (Nov. 29, 2023), https://www.coursera.org/articles/what-is-conversion-rate [https://perma.cc/7RP6-Q49E] (in marketing, the conversion rate "calculates the percentage of [website visitors] who complete a specific desired action").

219. *See* FTC REPORT, *supra* note 197.

220. *See supra* Sections II.C.1 and II.D.2.

should collect and report metrics. And if the regulator intends to monitor and enforce firms' compliance with the reporting requirement, it needs to institute a threshold that is based on information known, or potentially known, to it. Both problems would likely be solved if the reporting threshold would be changed to be all firms that fall under the CCPA's ambit.[221]

CONCLUSION

Regulating the information economy is a challenging task: The technology is complicated, not easily explainable, and keeps changing; so are many of the risks and harms that are associated with the information economy; and the business and economic relationships that underpin it are intricate and opaque, and controlled by the world's most powerful firms. But there is another problem: Regulators and the public do not currently know how and to what extent privacy laws are having a positive impact and whether they are solving any of these problems. This must change.

Accordingly, this Article examines privacy law's leading regulatory model—data control rights. It explores why data control rights are weak on a theoretical level, and it reveals the extent to which data control rights are underused and restricted in their impact on an empirical level.

This Article also argues that, normatively, it is crucial to measure and collect empirical data on the impact of privacy laws and other laws governing the information economy, and that such empirical effort should be part of the laws themselves and the regulatory mission in this space. Policymakers and the public are in an informational deficit. We should not ignore it. We should strive to know more, and we should shape our laws and regulations in a way that brings real transparency, accountability, and knowledge to the benefit of individuals and society alike.

The findings in this Article can take the policy debate a step further from where it currently is: If data control rights are not working as intended, how can we improve them, and what should we try next?

221. See the definition of "business." CAL. CIV. CODE § 1798.140(c) (West 2018). As of January 1, 2023, see CAL. CIV. CODE § 1798.140(d) (West 2022).