NOTES

BEYOND REQUEST-AND-RESPOND: WHY DATA ACCESS WILL BE INSUFFICIENT TO TAME BIG TECH

David Alpert[*]

The California Consumer Privacy Act (CCPA) is the first-of-its-kind law in the United States providing Californians (and effectively citizens nationwide) with comprehensive protection of their online data. The CCPA provides consumers with four meaningful rights: (1) a right to access the data companies collect from and about them; (2) a right to have said data deleted; (3) a right to know which categories of third parties these companies are sharing their data with or selling their data to; and, (4) a right to opt out of such sales. This Note focuses specifically on the first right, the right of data access.

While the CCPA's shift from sectoral to comprehensive breadth represents a strong break from past regulatory practice in this field, the law's focus on empowering citizens and consumers through information is a far more familiar move. This Note connects this right to data access to the federal Freedom of Information Act (FOIA) and argues that the problems of current corporate data practices dwarf the CCPA's individual request-and-respond right to data access. This Note uses past FOIA practice to identify the likely shortcomings in a request-and-respond data access regime. These shortcomings include an overreliance on individuals that does not facilitate broader transparency aims, past failures of targeted transparency in the consumer protection space, and a failure to learn the lessons of past privacy practice. Instead, this Note considers alternative solutions before recommending ex ante measures like a Pigouvian tax modeled off the environmental pollution space.

INTRODUCTION

In March 2018, the *New York Times* revealed that Cambridge Analytica, a political data firm tied to President Donald Trump's 2016 presidential campaign, had accessed private information on more than fifty million Facebook

* JD/MBA Candidate 2020, Columbia University. The author would like to thank David Pozen for his critical guidance and support through all stages of drafting, Vickie Baranetsky for her helpful comments, and Alex Alben, Rick Arney, and Bruce Sewell for their time. The author also thanks *Columbia Law Review*'s staff for their invaluable assistance through the publication process, my parents and sisters for their encouragement, and Na'ama for her unwavering love and support through this and all of life's adventures.

users, including their identities, friend networks, likes, and locational data.[1] It was not immediately obvious whether this access constituted a hack, a breach, or a leak.[2] But what became clear was that data and privacy issues had resonated in the public consciousness in an unprecedented manner.[3]

The Cambridge Analytica scandal came on the heels of a string of high-profile corporate and governmental data breaches over the last five years, including those of Under Armour,[4] Equifax,[5] Uber,[6] Ashley Madison,[7] the U.S. Office of Personnel Management,[8] and Home Depot.[9] But unlike the steady drip-drip of another corporate data breach, Cambridge Analytica arrived as a true watershed moment, helping spark more significant discussions about the misuse of consumer data.[10]

---

1. Kevin Granville, Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, N.Y. Times (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (on file with the *Columbia Law Review*).

2. See Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, How Trump Consultants Exploited the Facebook Data of Millions, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (on file with the *Columbia Law Review*) (describing the incident alternatively as a leak and a breach).

3. See "Data" and "Privacy", Google Trends, https://trends.google.com/trends/explore?date=2006-10-01%202018-10-28&geo=US&q=data%20AND%20privacy (on file with the *Columbia Law Review*) (last visited Jan. 27, 2020) (demonstrating a significant spike (and peak) in interest in Google searches for "data" and "privacy" soon after news of the Cambridge Analytica scandal broke in March).

4. Dave Lee, MyFitnessPal Breach Affects Millions of Under Armour Users, BBC (Mar. 29, 2018), https://www.bbc.com/news/technology-43592470 [https://perma.cc/VA45-TDLS].

5. Alfred Ng & Steven Musil, Equifax Data Breach May Affect Nearly Half the U.S. Population, CNET (Sept. 7, 2017), https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population [https://perma.cc/Y4SQ-6lQH?type-image] (detailing the 2017 breach that affected as much as half the U.S. population).

6. Dara Khosrowshahi, 2016 Data Security Incident, Uber (Nov. 21, 2017), https://www.uber.com/newsroom/2016-data-incident [https://perma.cc/K33V-8J3L] (describing a previously unreported 2016 incident that allowed hackers to access the personal information of fifty-seven million users worldwide).

7. Robert Hackett, What to Know About the Ashley Madison Hack, Fortune (Aug. 26, 2015), http://fortune.com/2015/08/26/ashley-madison-hack (on file with the *Columbia Law Review*) (describing a hack of thirty-two million members of an extramarital affairs dating website).

8. Julie Hirschfield Davis, Hacking of Government Computers Exposed 21.5 Million People, N.Y. Times (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html (on file with the *Columbia Law Review*) (describing the scope of the hack of the government's security clearance office, including compromised addresses, financial information, foreign contacts, and personal health data).

9. Jeff John Roberts, Home Depot to Pay Banks $25 Million in Data Breach Settlement, Fortune (Mar. 9, 2017), http://fortune.com/2017/03/09/home-depot-data-breach-banks (on file with the *Columbia Law Review*) (describing the theft of over fifty million customers' email or credit card information).

10. See Facebook Data Breach Is "Turning Point" for Online Privacy, Says Matt Hancock, BBC (Mar. 22, 2018), https://www.bbc.com/news/uk-politics-43504436 [https://perma.cc/X5ZP-L8KW] (quoting the United Kingdom's Culture Secretary as finding Facebook's

The scandal also significantly accelerated reformers' efforts to pass sweeping consumer data privacy laws.[11] In June 2018, California's legislature unanimously passed the California Consumer Privacy Act (CCPA).[12] The law provides Californians with a right to access the data companies collect on them,[13] a right to have said data deleted,[14] a right to know which categories of third parties these companies are sharing data with or selling data to,[15] and a right to opt out of such sales.[16] The rights are enforceable by a private right of action by consumers if a company fails to take reasonable safeguards before a data breach,[17] and a public right of action by the state Attorney General for any violation.[18] The law represents a seismic shift from sector-specific regulation (such as financial or personal health information) to a comprehensive data privacy regime.[19]

---

actions to be "totally unacceptable" and a "turning point"); Why the Cambridge Analytica Scandal Is a Watershed Moment for Social Media, Knowledge@Wharton (Mar. 22, 2018), http://knowledge.wharton.upenn.edu/article/fallout-cambridge-analytica [https://perma.cc/QL2D-FMYZ].

11. See Nicholas Confessore, The Unlikely Activists Who Took On Silicon Valley—And Won, N.Y. Times Mag. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html (on file with the *Columbia Law Review*) [hereinafter Confessore, Unlikely Activists] ("[I]t was suddenly easy to get people to sign their ballot petition. 'After the Cambridge Analytica scandal, all we had to say was "data privacy."'").

12. Gilad Edelman, California's Privacy Law Goes into Effect Today. Now What?, WIRED (Jan. 1, 2020), https://www.wired.com/story/ccpa-guide-california-privacy-law-takes-effect [https://perma.cc/PB9W-8QUP].

13. Cal. Civ. Code § 1798.100 (2018). This right includes not only the categories of data collected but also the specific pieces. Id.

14. Id. § 1798.105.

15. Id. § 1798.110(a)(4).

16. Id. § 1798.120.

17. Id. § 1798.150. If a violation is proven, consumers are entitled to the greater of between $100 and $750 per "incident" or actual damages. Id. § 1798.150(a)(1)(A).

18. Id. § 1798.155(b)–(c). But civil penalties in the amount of $2,500 per infraction or $7,500 per intentional violation are assessed only when a company fails to cure an alleged violation thirty days after notification by the state. Id. § 1798.155(b).

The CCPA applies to for-profit entities collecting Californians' data that either have upwards of twenty-five million dollars in gross revenue, traffic in the personal information of more than 50,000 Californians, or derive at least half of their annual revenue from selling Californians' personal information. Id. § 1798.140(c)(1)(A)–(C), (g). The law went into effect on January 1, 2020. Id. § 1798.198(a).

19. Lothar Determann, Analysis: The California Consumer Privacy Act of 2018, Int'l Ass'n of Privacy Prof'ls (July 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018 [https://perma.cc/9ALV-9C6B].

Historically, the "most sensitive data—such as financial, medical, health, electronic communications, and children's information—are protected by nearly two dozen federal sector-specific laws and numerous state laws." Sidley Austin LLP, Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States 7 (2016), https://www.sidley.com/-/media/publications/essentially-equivalent—final.pdf [https://perma.cc/RF9E-483B]. Instead of comprehensive data privacy regulation, this sectoral approach allowed for data outside of the specified sectors to be protected only "through the general enforcement authority of the FTC, state Attorneys General, and other federal and state regulators." Id.

Though the CCPA grants Californians many rights with respect to their data, this Note focuses more narrowly on the right of consumer data access. Specifically, this Note argues that the CCPA's individual request-and-respond approach to data access is fundamentally mismatched to the problems posed by current corporate data practices.[20] This Note's critique of the CCPA's request-and-respond provision is inspired by the half century legacy of the federal Freedom of Information Act (FOIA), which contains an analogous individual right and shares similar transparency roots. Using an understanding of both FOIA's operative provision and how it has worked in practice, this Note argues that an individualistic, request-and-respond model of private data disclosure will fail to achieve the progressive aims of privacy advocates and tech reformers. This Note concludes by suggesting that an alternative model of prophylactic, command-and-control regulation will better stem harmful data collection, retention, analysis, and sales.

In Part I, this Note reviews the advent of request-and-respond data access provisions, contextualizes these provisions by providing a primer on what makes data personal and why consumers care, and identifies the connection between the CCPA's specific provision and FOIA's. Part II lays out a substantive critique of how past FOIA practice informs future shortcomings in a request-and-respond data access regime. The Note concludes in Part III by considering and rejecting a tailored affirmative disclosure solution before settling on prophylactic, command-and-control directives as the proper means to regulate the booming consumer personal data industry.

I. BACKGROUND ON DATA, PRIVACY, AND THE RIGHT TO KNOW

This Part discusses the applicable background law on the CCPA's request-and-respond provision. Section I.A details how data access provisions rooted in a request-and-respond model are entering into the consumer data privacy sphere, both in California and beyond, and why this data matters to both individual consumers and society as a whole. Section I.B links the request-and-respond provisions in consumer data privacy regulations to FOIA. Section I.C describes how request-and-response works in FOIA and how it is working so far in the new California law.

A. *Request-and-Respond Data Access Provisions Are Coming*

This section details the relevance of request-and-respond provisions to the consumer privacy realm. Section I.A.1 explores the recent spate of consumer protection laws, both proposed and enacted, that contain a request-and-respond right to data access. Section I.A.2 then provides a fuller back-

20. In general, request-and-respond provisions obligate a company to provide a consumer with the personal data it has collected when a consumer so requests. See infra section I.C (describing these provisions' operation in greater detail).

ground on consumer data and its relevance to the current debate on privacy, focusing on data's economic value, private sentiment about its use and abuse, and public harms.

1. *Recent Consumer Protection Laws with Request-and-Respond Provisions.* — Request-and-respond provisions are appearing more frequently across the globe as a way to let consumers gain further information about their data. While there is limited scholarship on them, these provisions have a relatively long history in international law. California's law, on the other hand, is the first example of this right of data access at the state or federal level in the United States.

a. *Request-and-Respond Provisions Abound in International and Foreign Law.* — There are multiple forms of request-and-respond provisions in international and foreign law. Perhaps most notably, the European Union's (EU) comprehensive General Data Protection Regulation (GDPR) passed in 2016 and took effect in May 2018.[21] GDPR provides a right of access by the data subject, which includes both access to the personal data being collected and the categories of it.[22] Big tech firms doing business in both Europe and the United States are beginning to extend some of the same consumer protections, including request-and-respond data access rights, to their American customers.[23] Beyond Europe, Canada's 2000 Personal Information Protection and Electronic Documents Act includes a right of data access "[u]pon request."[24] So, too, does South Korea's 2011 Personal Information Protection Act.[25] Finally, Japan's Act on the Protection of Personal Information requires

---

21. See Mike Moore, What Is GDPR? Everything You Need to Know About the New EU Data Laws, TechRadar (Jan. 25, 2019), https://www.techradar.com/news/what-is-gdpr-everything-you-need-to-know (on file with the *Columbia Law Review*).

22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 43 [hereinafter General Data Protection Regulation]. GDPR also requires companies to obtain affirmative permission from a user to collect their data and provides the user with the opportunity to port, correct, or delete their data, or to otherwise restrict processing. Id. at 43–45.

23. See Wayne Rash, Apple Rolls Out GDPR-Like Features for U.S. Users, EWeek (Oct. 17, 2018), http://www.eweek.com/apple/apple-rolls-out-gdpr-like-features-for-u.s.-users [https://perma.cc/2VFH-4ZTZ] (explaining that Apple will allow its American customers to download the data the company has on them, just as the GDPR mandates for European customers).

24. Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5, cl. 4.9 (Can.) (allowing consumers to exercise their right, "[u]pon request," to "be informed of the existence, use, and disclosure of his or her personal information and . . . be given access to that information").

25. Gaein jungbo boho beob [Personal Information Protection Act], Act No. 10465, Mar. 29, 2011, amended by Act No. 14107, Mar. 29, 2016, art. 4(3) (S. Kor.), translated in Personal Information Protection Act, Korea Legislation Research Institute: Korea Law Translation Ctr., https://elaw.klri.re.kr/kor_service/lawView.do?hseq=38482&lang=ENG [https://perma.cc/E2M7-EARX] (last visited Jan. 20, 2020) ("A data subject has . . . [t]he right to . . . request access . . . to such personal information . . . ."); see also Alex Wall, GDPR Matchup: South Korea's Personal Information Protection Act, Int'l Ass'n of Privacy Prof'ls

companies to give users access to personally identifying data upon request, with limited exceptions.[26]

b. *California Inspires a Wave of State Efforts.* — As California's law forms much of the basis of this Note, it is necessary to review the law's unique background. Disturbed by the scope of the personal data economy, California real estate developer Alastair Mactaggart and finance executive Rick Arney teamed up to research the issue.[27] They eventually proposed a statewide ballot initiative in 2018 advocating for more consumer privacy rights.[28] Facebook and Google donated hundreds of thousands of dollars to defeat the measure.[29] Despite strong polling, Mactaggart and Arney recognized the risk of losing to the companies at the ballot box, so they negotiated a robust privacy bill with the California legislature and withdrew the initiative.[30]

As of January 1, 2020, the statute allows California consumers to request that a private company disclose the personal information it has collected on that consumer.[31] Absent federal preemption in the near future, the CCPA will continue to have a nationwide impact.[32]

(Jan. 8, 2018), https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act [https://perma.cc/Y589-DBXS] (noting that, like the EU's GDPR, South Korea's analogous law "protects privacy rights from the perspective of the data subject and . . . is comprehensive, applying to most organizations, even government entities").

26. Kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information], Law No. 57 of 2003, art. 28 (Japan), translated in Act on the Protection of Personal Information, Japanese Law Translation, http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&vm=2&re=02 [https://perma.cc/WTL6-PJ8J] (last visited Mar. 22, 2020); see also Data Protection in Japan to Align with GDPR, Skadden, Arps, Slate, Meagher & Flom LLP (Sept. 24, 2018), https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr [https://perma.cc/XJY9-SUPJ] (discussing the reciprocal recognition between Japan's and the EU's data protection regimes).

27. Confessore, Unlikely Activists, supra note 11.

28. Id.

29. Id.

30. Id.

31. Cal. Civ. Code § 1798.100(a) (2018). The disclosure right enables the consumer to move their data to another entity and/or request the deletion of their personal information. Id. § 1798.100(d), § 1798.105(a).

32. See Aaron Mak, The Big Change Coming to Just About Every Website on New Year's Day, Slate (Dec. 30, 2019), https://slate.com/technology/2019/12/california-data-privacy-law-ccpa-do-not-sell-changes.html [https://perma.cc/JTP2-S2UG] ("Since it's a lot more work to create a separate infrastructure just for California residents to opt out of the data collection industry, these requirements will transform the internet for everyone."); see also Julie Brill, Microsoft Will Honor California's New Privacy Rights Throughout the United States, Microsoft (Nov. 11, 2019), https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights [https://perma.cc/2MKJ-YC2T]; Sam Dean, California Is Rewriting the Rules of the Internet. Businesses Are Scrambling to Keep Up, L.A. Times (Dec. 26, 2019), https://www.latimes.com/business/technology/story/2019-12-26/california-internet-data-privacy-law (on file with the *Columbia Law Review*) ("Most businesses with a website and customers in California—which is to say most large businesses in the nation—must follow the new rules . . . ."). CCPA initiative coauthor Alastair Mactaggart expressly contemplated the likelihood that the CCPA transforms the rule-creating and rule-enforcing California Attorney General into "the chief privacy officer of the United States." Confessore,

Unlikely Activists, supra note 11. A 2018 PwC survey found that over 225 of 300 major, qualifying American companies collected information on California residents. Many US Businesses Doubt They Will Meet California Privacy Law Deadline, pwc (Oct. 9, 2018), https://www.pwc.com/us/en/services/consulting/cybersecurity/pulse-survey-ccpa.html [https://perma.cc/3H4Z-3XJY]; see also Samuel Cullari & Alexis Cocco, California Enacted a Data Privacy Law. Why Should Pa. Companies Care?, Legal Intelligencer (Apr. 3, 2019), https://www.law.com/thelegalintelligencer/2019/04/03/california-enacted-a-data-privacy-law-why-should-pa-companies-care (on file with the *Columbia Law Review*) (describing the broad application of the CCPA to companies outside California).

The law applies regardless of whether a company's website actively targets Californians, so industry professionals believe that passive access to out-of-state blogs or small business sites may result in them coming within the law's ambit. See, e.g., Determann, supra note 19. And within California, "most retailers, fitness studios, music venues and other businesses" will likely meet the criteria. Id.

At one point before the CCPA's 2020 effective date, there seemed to be a real risk that Congress might pass a federal law to explicitly preempt it. See John Thune, Protect and Innovate Online Privacy, Hill (Sept. 25, 2018), https://thehill.com/blogs/congress-blog/technology/408335-protect-and-innovate-online-privacy [https://perma.cc/PPD7-SDD7] ("The question is no longer whether we need a national law to protect consumers' privacy. The question is what shape that law should take."). Yet, at the time of this writing, Congress has not and significant hurdles remain, including the politicization of the issue. See Ali Breland, Dems Seek to Seize on Data Privacy as Midterm Issue, Hill (June 17, 2018), https://thehill.com/policy/technology/392575-dems-seek-to-seize-on-data-privacy-as-midterm-issue [https://perma.cc/24H3-BPYT]; Marguerite Reardon, Democrats Push for 'Internet Bill of Rights' to Protect Your Privacy, CNET (Oct. 5, 2018), https://www.cnet.com/news/democrats-push-for-an-internet-bill-of-rights-to-protect-consumer-privacy [https://perma.cc/6HUL-GFHC] (detailing the Democrats' post-2018 midterm election plans for "sweeping consumer privacy protections"); see also Allison Grande & Ben Kochman, Federal Privacy Law May Need Bigger Boost than Midterms, Law360 (Nov. 2, 2018), https://www.law360.com/publicpolicy/articles/1098125/federal-privacy-law-may-need-bigger-boost-than-midterms (on file with the *Columbia Law Review*) (describing "the path to consensus" on a federal privacy law as "a long haul"). In 2019, there was some renewed energy, as Democrats and Republicans each proposed separate bills, the Senate held a hearing, and the House Energy and Commerce Committee negotiated a bipartisan draft of a bill; however, "[N]one of . . . [the bills] seem[ed] to have gained significant traction." Wendy Zhang, United States: Comprehensive Federal Privacy Law Still Pending, Mondaq (Jan. 24, 2020), http://www.mondaq.com/unitedstates/x/886488/Data+Protection+Privacy/Comprehensive+Federal+Privacy+Law+Still+Pending [https://perma.cc/L483-5DQ5]; see also Lauren Feiner, A Federal Privacy Law Is Starting to Crystallize, but Democrats and Republicans Can't Agree on How to Do It, CNBC (Dec. 4, 2019), https://www.cnbc.com/2019/12/04/a-federal-privacy-law-is-starting-to-crystallize-senators-remain-divided-over-details.html [https://perma.cc/ZY2T-RR2P]. Commentators predict any "push to enact federal privacy legislation . . . to face many of the same hurdles as long-running efforts to establish national data breach notification and security standards." Grande & Kochman, supra. While drafts of those bills have been proposed in every session of Congress for a decade or more, "[N]one have even come close to reaching a floor vote." Id.

The CCPA inspired other activists, state attorneys general, and legislators.[33] Proposals modeled off the CCPA were introduced in eleven additional states during their respective 2019 legislative sessions,[34] and over half of all fifty states have considered some form of consumer data privacy legislation.[35] The seismic impact of the CCPA can be seen in the facts that Maine and Nevada have enacted similar laws, and the Connecticut, North Dakota, Louisiana, and Texas legislatures have authorized task forces to further study them.[36]

c. *Federal Law May Supplant State Efforts.* — There is currently no comprehensive federal data privacy law. After the CCPA's passage, however, tech companies began to lobby for federal legislation that would preempt it.[37] The Senate Commerce Committee held a series of hearings in the fall of 2018 during which tech company representatives requested preemptive federal legislation,[38] and privacy advocates, including Mactaggart, testified instead that federal legislation should leave the California law as a floor.[39]

---

33. Telephone Interview with Rick Arney, Coauthor, CCPA Initiative (Dec. 6, 2018) (on file with the *Columbia Law Review*) (detailing conversations with groups in Wyoming, Vermont, and Illinois about replicating California's model).

34. See Emily Tabatabai, Heather Egan Sussman, Nicholas Farnsworth & Sulina Gabale, State Legislators Joining the Consumer Privacy Protection Party: Introduced CCPA-Like Bills, Orrick (Mar. 18, 2019), https://blogs.orrick.com/trustanchor/2019/03/18/state-legislators-joining-the-consumer-privacy-protection-party-introduced-ccpa-like-bills [https://perma.cc/Y49E-B7LM] (detailing proposals under consideration in Hawaii, Maryland, Massachusetts, Nevada, New Mexico, New York, Rhode Island, and Washington, in addition to failed efforts in Mississippi and North Dakota); Texas Legislators Propose New State Data Privacy Laws, ACA Int'l (May 10, 2019), https://www.acainternational.org/news/texas-legislators-propose-new-state-data-privacy-laws [https://perma.cc/2BUR-X9A4] (detailing two CCPA-like bills proposed in the Texas state legislature).

35. Pam Greenberg, States Break New Ground on Consumer Data Privacy Legislation, Nat'l Conf. of State Legislatures (June 19, 2019), https://www.ncsl.org/blog/2019/06/19/states-break-newground-on-consumer-privacy-regulation.aspx [https://perma.cc/5YEE-MBDK].

36. Id.

37. Cecilia Kang, Tech Industry Pursues a Federal Privacy Law, On Its Own Terms, N.Y. Times (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html (on file with the *Columbia Law Review*).

38. See generally Examining Safeguards for Consumer Data Privacy: Hearing Before the S. Comm. on Commerce, Sci. & Transp., 115th Cong. (2018) (statement of Andrew DeVore, Vice President and Associate General Counsel, Amazon, Inc.) https://www.commerce.senate.gov/services/files/0F58A430-2037-4884-9B98-5FB3CA977838 [https://perma.cc/DGV7-DBRC]; see also Zack Whittaker, In Senate Hearing, Tech Giants Push Lawmakers for Federal Privacy Rules, TechCrunch (Sept. 26, 2018), https://techcrunch.com/2018/09/26/in-senate-hearing-tech-giants-push-lawmakers-for-federal-privacy-rules [https://perma.cc/S4KV-JNU2].

39. See Consumer Data Privacy: Examining Lessons from the European Union's General Data Protection Regulation and the California Consumer Privacy Act: Hearing Before the S. Comm. on Commerce, Sci. & Transp., 115th Cong. (2018) (testimony of Alastair Mactaggart, Chair, Californians for Consumer Privacy), https://www.commerce.senate.gov/services/files/9CC53419-6E09-4075-98BA-4C4F2D46A686 [https://perma.cc/H7BV-N9CW].

The Senate Democrats released a bill that does exactly that,[40] while the Senate Republicans have drafted a bill that would preempt state laws like the CCPA.[41] Both bills, however, include request-and-respond provisions.[42]

Other federal proposals in various stages of development do provide a right of data access.[43] In April 2018, Senators Amy Klobuchar and David Kennedy released a draft bipartisan bill that includes a right to access data as one of its privacy protections.[44] Senator Ron Wyden's Mind Your Own Business Act, introduced in October of 2019, includes a right of data access after a company receives a "written request from a verified consumer."[45] A list compiled by Congressman Ro Khanna, deemed the Internet Bill of Rights, included as its first right "to have access to and knowledge of all collection and uses of personal data by companies."[46] Before news of Cambridge Analytica broke, Congresswoman Janice Schkowsky proposed the Secure and Protect Americans' Data Act, which included a consumer right of data access under a request-and-respond model for data held by third-party data brokers.[47] And in 2015, the Obama Administration produced a draft Consumer Privacy Bill of Rights Act that included a request-and-respond right of data access.[48] Other bills, proposals, and frameworks either lack a data access right or do not explicitly do so using a request-and-respond

---

40. See Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 302(c) (2019).

41. See S. Comm. on Commerce, Sci. & Transp., United States Consumer Data Privacy Act of 2019 Discussion Draft 24 (2019), https://aboutblaw.com/NaZ [https://perma.cc/ZBG3-VBAB] [hereinafter Consumer Data Privacy Act Draft].

42. See S. 2968 § 102(a); Consumer Data Privacy Act Draft, supra note 41, at 8.

43. See Allie Bohm, How Well Do the Current Federal Privacy Proposals Protect Your Privacy?, Pub. Knowledge (Dec. 21, 2018), https://www.publicknowledge.org/news-blog/blogs/how-well-do-the-current-federal-privacy-proposals-protect-your-privacy [https://perma.cc/4JNG-GUY5] (recapping drafts of nine proposed federal bills seeking to regulate consumer data privacy).

44. See Social Media Privacy Protection and Consumer Rights Act of 2018, S. 2728, 115th Cong. § 3(b) (2018). Specifically, the bill entitles a user to "a copy of the personal data of the user that the operator has processed, free of charge and in an electronic and easily accessible format, including a list of each person that received the personal data from the operator for business purposes, whether through sale or other means." Id.; see also April Glaser, There's a New Bill to Regulate Facebook and Google's Data Collection, Slate (Apr. 24, 2018), https://slate.com/technology/2018/04/the-new-bill-to-regulate-facebook-and-googles-data-might-actually-do-the-trick.html [https://perma.cc/SJU9-YQCF].

45. Mind Your Own Business Act, S. 2637, 116th Cong. § 7(b)(1)(D) (2019).

46. Kara Swisher, Introducing the Internet Bill of Rights, N.Y. Times (Oct. 4, 2018), https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html (on file with the *Columbia Law Review*). Khanna's list is given further teeth by virtue of the fact that it was compiled on the orders of then-Democratic Minority Leader (and now Speaker) Nancy Pelosi. Id.

47. Secure and Protect Americans' Data Act, H.R. 3896, 115th Cong. § 2(b)(2)(B) (2017); see also id. at § 5(5)(A) (defining "information broker" as a "commercial entity" that collects information on noncustomers and provides it to third parties).

48. Administration Discussion Draft: Consumer Privacy Bill of Rights Act, § 106(a) (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/TM7R-JN6J].

model.[49] The above section makes clear, however, that request-and-respond data access rights have gained traction internationally, and will likely continue to have a major impact domestically, be it through the CCPA and other state laws or federal legislation. The next subsection details why consumers care about personal data.

2. *Concerns Over the Personalization of Data.* — There are many different definitions of what constitutes personal data.[50] As discussed below, data is a real economic asset that consumers routinely trade to quickly find information online, to network socially or professionally, and to pay for goods or services without money.[51] This Note does not require a single, exact definition of personal data, but worthwhile regulatory definitions encompass "our identity (demographics), our behavior (psychographics—our interests, attitudes, and opinions) and our purchases."[52]

Data is critically important because it is one of the key economic engines of the unfolding Information Age.[53] The data-driven economy has

---

49. For example, the CONSENT Act proposed by Senators Ed Markey and Richard Blumenthal neither explicitly preempts the CCPA nor provides a data access right. S. 2639, 115th Cong. (2018). And Senator Mark Warner's white paper does the same. Mark Warner, Potential Policy Proposals for Regulation of Social Media and Technology Firms, https://www.scribd.com/document/385137394/MRW-Social-Media-Regulation-Proposals-Developed [https://perma.cc/8PT9-6W5W] (last visited Jan. 29, 2020).

50. See, e.g., General Data Protection Regulation, supra note 22, ¶ 26 (defining personal data as "any information concerning an identified or identifiable natural person"); Cal. Civ. Code § 1798.140(o)(1) (2018) (defining personal data as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household").

51. Michael Haupt, Introducing Personal Data Exchanges and the Personal Data Economy, Medium: Project 2030 (Dec. 7, 2016), https://medium.com/project-2030/what-is-a-personal-data-exchange-256bcd5bf447 [https://perma.cc/YY8P-YU2W].

52. Id. Behavior can be understood even more expansively to also include activities like how long a person looked at a web page and where their mouse went. See Antonio Villas-Boas, Passwords Are Incredibly Insecure, So Websites and Apps Are Quietly Tracking Your Mouse Movements and Smartphone Swipes Without You Knowing to Make Sure It's Really You, Bus. Insider (July 19, 2019), https://www.businessinsider.com/websites-apps-track-mouse-movements-screen-swipes-security-behavioral-biometrics-2019-7 [https://perma.cc/7FQ4-WRL4].

53. In 2012, site-specific user profiles retailed in bundles of at least 10,000 for $0.005 each. Alexis C. Madrigal, How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $1,200, Atlantic (Mar. 19, 2012), https://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730 (on file with the *Columbia Law Review*). But considering the entire digital advertising ecosystem, user data may be worth as much as $1,200 per personal profile. Id. More recently, the lower end of the estimation range has been set at $240 per user. Wibson, How Much Is >Your< Data Worth? At Least $240 per Year. Likely Much More., Medium (Jan. 19, 2018), https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa [https://perma.cc/L5EZ-JC79]. And one man monetized a week's worth of his own personal data for $2,733 on Kickstarter in 2013. Federico Zannier, A Bite of Me, Kickstarter, https://www.kickstarter.com/projects/1461902402/a-bit-e-of-me [https://perma.cc/TKY7-B5X6] (last updated Oct. 28, 2013).

been defined by numerous scholars as "informational capitalism" where the creation, sale, and exchange of data permeate nearly all economic sectors.[54] In a recent speech, Apple CEO Tim Cook traced the rise of a trade in data into a full-fledged "data industrial complex."[55]

While consumer data is clearly valued by companies, consumers have expressed increasing uneasiness with how their data is handled. Surveys indicate Americans are distrustful of how their data is used but feel trapped or compelled to remain online.[56] Despite valuing such control, over ninety

---

Companies profit handsomely off this data. In the fourth quarter of 2017, Facebook made $6 per user globally, but about $27 on users in the United States and Canada. Anita Balakrishnan, Facebook Made an Average of $6.18 off Each User in Q4, More than Double Three Years Ago, CNBC (Jan. 31, 2018), https://www.cnbc.com/2018/01/31/facebook-earnings-q4-2017-arpu.html [https://perma.cc/S6CT-ELM5]. Google made almost $13 per American and Canadian user back in 2016. Roger Entner, Digital Advertising Takes the Lead—Dominated by Google and Facebook, Recon Analytics (May 30, 2017), http://reconanalytics.com/2017/05/digital-advertising-takes-the-lead-dominated-by-google-and-facebook [https://perma.cc/D53F-8DCE].

54. See David E. Pozen & Jeremy Kessler, Introduction, The Search for an Egalitarian First Amendment, 118 Colum. L. Rev. 1953, 1972–73 (2018); see also Julie E. Cohen, The Regulatory State in the Information Age, 17 Theoretical Inquiries L. 369, 370–71, 414 (2016). But see Shoshana Zuboff, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, 30 J. Info. Tech. 75, 75 (2015) (defining the phenomenon instead as "surveillance capitalism").

55. Evans, supra note 32. Cook warned that "[o]ur own information, from the everyday to the deeply personal, is being weaponized against us with military efficiency . . . . These scraps of data . . . each one harmless enough on its own . . . are carefully assembled, synthesized, traded, and sold." Id.

Of course, for-profit Apple is hardly championing consumer data privacy regulation for purely altruistic reasons. Apple's business decisions have firmly situated it on the direct-to-consumer revenue model side of the great tech divide, with social media tech giants like Facebook, Twitter, and Snap on the opposite, ad-driven revenue side. Alex Eule & Jon Swartz, Facebook and Apple Embody New Tech Divide, Barron's (Apr. 21, 2018), https://www.barrons.com/articles/facebook-and-apple-embody-new-tech-divide-1524273880 [https://perma.cc/VFG9-XXHX]. Some speculate that Apple's embrace of privacy is a cynical ploy to justify high device sales prices. See id. ("Perhaps partially to justify its high prices, Apple has made privacy a sales pitch for its products."); see also Jon Markman, Apple's Superficial Jihad for Data Privacy Is a Cynical Joke, Jon Markman's Pivotal Point (Oct. 29, 2018), https://www.markmanspivotalpoint.com/artificial-intelligence/apples-superficial-jihad-data-privacy-cynical-joke [https://perma.cc/L3W3-SNFJ]. Facebook, on the other hand, is certain to balk at increasing regulation of consumer data as it presents a significant threat to its business model. See Eule & Swartz, supra (explaining that Facebook makes ninety-eight percent of its revenue from data-driven targeted ads). But see Antonio García Martínez, Why California's Privacy Law Won't Hurt Facebook or Google, WIRED (Aug. 31, 2018), https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google [https://perma.cc/5WAX-95CF] (arguing that the Californian and European privacy laws favor the direct, first-party types of relationships consumers maintain with Facebook and Google over third-party relationships with data brokers). The gap between ad-driven businesses and direct-to-consumer companies reflects a longtime division that explains differing responses to past privacy regulation proposals. For an example of one such response, see Kang, supra note 37.

56. Lee Rainie, Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns, Pew Res. Ctr. (Mar. 27, 2018), http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns [https:

percent of survey respondents felt that consumers had lost control over how companies use their data.[57] Over sixty percent of Americans want to do more to protect their information online,[58] and almost seventy percent believe current regulations are insufficient to help.[59] Another Pew Research Center study found that approximately four out of five consumers believe that the risks posed by collection of consumer data by corporations outweigh the benefits.[60]

Nevertheless, consumers continue to pay with their data and behave as though their data and privacy matter little[61]—requiring a deeper explanation for the need to regulate. Professor Omri Ben-Shahar reconciles the "universal anxiety among people over the power of data with the universal indifference to sharing their own private information" by arguing for the

---

//perma.cc/8SW7-D4CZ] ("[E]xperts believe that unplugging is hard because social media and other technology affordances make life convenient and because the platforms offer a very efficient, compelling way for users to stay connected to the people and organizations that matter to them."); see also April Glaser, The Problem With #DeleteFacebook, Slate (Mar. 21, 2018), https://slate.com/technology/2018/03/dont-deletefacebook-thats-not-good-enough.html [https://perma.cc/3FXC-T4KA] ("[F]or many people, Facebook is becoming the internet and the internet is becoming Facebook . . . . [I]f you want to be a part of any social life or local political conversations or want to promote your work, that simply means being on Facebook.").

57. Mary Madden, Public Perceptions of Privacy and Security in the Post-Snowden Era, Pew Res. Ctr. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions [https://perma.cc/XD66-MZM8]; see also Mary Madden & Lee Rainie, Americans' Views About Data Collection and Security, Pew Res. Ctr. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-views-about-data-collection-and-security [https://perma.cc/6XV8-PSVW].

58. Mary Madden, Most Would Like to Do More to Protect Their Personal Information Online, Pew Res. Ctr. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/most-would-like-to-do-more-to-protect-their-personal-information-online [https://perma.cc/94J2-CX4G].

59. Lee Rainie, Sara Kiesler, Ruogo Kang & Mary Madden, Anonymity, Privacy, and Security Online, Pew Res. Ctr. (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online [https://perma.cc/PU7S-DT4M]; see also Bree Fowler, Americans Want More Say in the Privacy of Personal Data, Consumer Rep. (May 18, 2017), http://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data [https://perma.cc/J7U2-7VW8] (reporting that seventy percent of Americans "lack confidence that their personal data is private and safe from distribution without their knowledge"); Aaron Smith, Public Attitudes Toward Technology Companies, Pew Res. Ctr. (June 28, 2018), http://www.pewinternet.org/2018/06/28/public-attitudes-toward-technology-companies [https://perma.cc/6DK6-WNU4] (reporting that fifty-one percent of U.S. adults believe tech companies "should be regulated more than they are now" and fifty-five percent say "technology companies have too much power and influence").

60. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information, Pew Res. 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/473A-CKYH].

61. Omri Ben-Shahar, Data Pollution, 10 J. Legal Analysis 104, 111 (2019) [hereinafter Ben-Shahar, Data Pollution] ("[People] say that they greatly value their personal data, but they turn around and give it up for meager quid pro quo.").

existence of public, external "data pollution" harms from mass data collection, retention, and analysis.[62] These are "harms to social environments, political environments, informational ecosystems,"[63] and the "private interests of other people."[64] The universal indifference can be further explained by the fact that "only a small fraction" of the significant economic costs of data breaches are borne by the individual whose data is stolen.[65]

Between private, individual consumer sentiment and the public-data pollution hypothesis, there are multiple justifications for increased regulation of corporate data collection and use. Considering the financial stakes involved in data-driven targeted advertising, however, companies have every financial incentive to thwart such regulation.

B. *The Request-and-Respond Provision's Ties to FOIA*

Despite their prevalence in the consumer data privacy sphere, request-and-respond provisions did not originate there. This section provides a background on this provision's roots in FOIA and the connection between FOIA and the CCPA. Section I.B.1 provides a background on FOIA and its request-and-respond provisions. Section I.B.2 links FOIA to the CCPA, and section I.B.3 acknowledges some key differences between the two laws, before concluding that their overarching similarities render FOIA a useful comparator for a private right of data access.

1. *FOIA Is the Original Request-and-Respond Law.* — In his history of political transparency, Professor Michael Schudson describes the request-and-respond provision as "the great originality of [FOIA]."[66] Congressman John Moss served as the law's key champion over the course of the 1950s and '60s and assembled a coalition of supportive journalists.[67] The request-

62. Id. at 112–13. Examples of these harms include the weaponization of political propaganda in Facebook's Cambridge Analytica scandal, the Strava fitness app's reveal of "secret geographic locations of U.S. military operations," discriminatory targeted advertising, and at-home DNA testing kits revealing an unexpected family secret. Id. at 112–16.

63. Omri Ben-Shahar, Professor, Univ. of Chi. Law Sch., Address at the Legal Challenges of the Data Economy Conference: Data Pollution (Mar. 22, 2019), https://www.law.uchicago.edu/recordings/omri-ben-shahar-data-pollution [https://perma.cc/VVG4-EHNR].

64. Id.

65. Ben-Shahar, Data Pollution, supra note 61, at 117.

66. Michael Schudson, The Rise of the Right to Know: Politics and the Culture of Transparency, 1945–1975, at 35 (2015).

67. See David E. Pozen, Transparency's Ideological Drift, 128 Yale L.J. 100, 118 (2018) [hereinafter Pozen, Drift]; Thomas Blanton, Freedom of Information at 40, Nat'l Sec. Archive (July 4, 2006), https://nsarchive2.gwu.edu//NSAEBB/NSAEBB194/index.htm [https://perma.cc/5DV2-VF82]. Journalists, seeing themselves as "guardians of democracy," had grown exasperated by the executive branch's tight control of information. Pozen, Drift, supra, at 118. The effort was prodded along by the American Society of News Editors and a book they commissioned by lawyer Harold Cross called *The People's Right to Know*, which became the scholarly foundation and bible of the nascent freedom of information movement. George Kennedy, How Americans Got Their Right to Know, John E. Moss Found.,

and-respond provision can be traced to testimony before Moss's Special Subcommittee on Government Information in 1955, which argued for "a right of inspection of public records."[68] This right was refined in a draft bill delineating individual requests and agency responses.[69]

2. *The CCPA Was Based on FOIA.* — FOIA served as the explicit inspiration for the backers of the California ballot initiative that ultimately resulted in the CCPA. On the website for the nonprofit that sponsored the initiative, initiative-funder Mactaggart described the initial idea behind the CCPA in the following way: "While it was then possible (and still is) to ask almost any level of government what it knows about someone or something via a Freedom of Information request, consumers had no such ability with respect to businesses. That was our first focus, giving consumers such an ability."[70] And initiative coauthor Rick Arney more succinctly described the CCPA as "a FOIA for corporations."[71] Arney explained his belief that "problems are solved with daylight often, and the Freedom of Information [Act] is kind of what [the CCPA] is modeled after . . . . And we know that a lot of policies spawn from that."[72]

3. *Despite Their Differences, FOIA Is a Useful Lens to Critique the CCPA.* — Still, it is important to acknowledge the material differences and distinctions between FOIA and the CCPA.[73] In many respects, the laws could not be more dissimilar: FOIA applies only to government,[74] while the CCPA applies to private companies.[75] FOIA's drafting history contemplates a journalist requesting records from a bloated, federal agency to report on

---

http://www.johnemossfoundation.org/foi/kennedy.htm [https://perma.cc/4QAU-YKML] (last visited Jan. 29, 2020).

68. Harold C. Relyea, Freedom of Information, Privacy, and Official Secrecy: The Evolution of Federal Government Information Policy Concepts, 7 Soc. Indicators Res. 137, 140 (1980). FOIA had been preceded by (and, in fact, amended) the Administrative Procedure Act (APA), which required the government to publicly disclose documents. Schudson, supra note 66, at 57–58. The APA came with enough exceptions and broad carveouts, however, to render the mandate a nullity. Id.

69. Relyea, supra note 68, at 141.

70. About Us: A Letter from Alastair Mactaggart, Board Chair, Californians for Consumer Privacy, https://web.archive.org/web/20181114134745/https://www.caprivacy.org/about-us [https://perma.cc/6585-Q4WU] [hereinafter Californians for Consumer Privacy, About Us] (last visited Feb. 4, 2020).

71. Telephone Interview with Rick Arney, supra note 33.

72. Id.

73. One senior staffer for a state legislator involved in the CCPA's passage went so far as to disclaim *any* connection between FOIA and the CCPA: "I worked closely on the CCPA and from the Senator's perspective, this was not a FOIA issue. I don't see how there's a connection and it did not come up in our conversations." Email from Senior Staffer, Cal. State Senate, to author (Oct. 18, 2018, 14:12 EST) (on file with the *Columbia Law Review*).

74. 5 U.S.C. § 552(a) (2018) (applying FOIA to federal agencies, but not to the legislative or judicial branches).

75. Cal. Civ. Code § 1798.140(c) (2018) (defining "business").

findings for the public interest.[76] The archetypal CCPA request, on the other hand, is that of a sole consumer petitioning a sleek tech start-up for a zip folder of their data so they can delete it or port it over to a competitor.[77] To those respective ends, FOIA allows "any person" to request government records,[78] while the CCPA limits access to the consumer whose data are at issue.[79] FOIA requests can be individually litigated all the way up to the Supreme Court,[80] while the CCPA offers no private right of action for an unanswered request or unresponsive reply.[81] Many of FOIA's key burdens, such as the long delays in receiving a response and the need to threaten litigation,[82] seem inapt when applied to the CCPA, where automated responses can be provided in days or even hours. As the CCPA only applies to an individual's records, it also largely avoids FOIA's catch-22 prerequisite knowledge problem, where a requester must know (and specify) enough about the government program they are requesting records about to get a response, but may not yet possess sufficient knowledge without initially accessing those records.[83]

---

76. Margaret B. Kwoka, FOIA, Inc., 65 Duke L.J. 1361, 1367–71 (2016) [hereinafter Kwoka, FOIA, Inc.] (reviewing the origins of FOIA).

77. See Confessore, Unlikely Activists, supra note 11.

78. 5 U.S.C. § 552(a)(3)(A) ("[M]ake the records promptly available to any person.").

79. Cal. Civ. Code § 1798.100(a) ("A consumer shall have the right to request that a business that collects a consumer's personal information disclose to *that consumer* . . . ." (emphasis added)).

80. See, e.g., FBI v. Abramson, 456 U.S. 615, 615 (1982) (holding that records compiled for law enforcement usages do not lose their law enforcement exemptions to the FOIA when compiled for non-law-enforcement purposes); Baldridge v. Shapiro, 455 U.S. 345, 346 (1982) (holding that sections of the Census Bureau Act qualify as exempted statutes under FOIA, preventing the Bureau from providing the respondent information); Chrysler Corp. v. Brown, 441 U.S. 281, 281–83 (1979) (holding that businesses who submit documents to the government can sue to challenge an agency's decision to release those documents under FOIA).

81. See Adam Schwartz, You Should Have the Right to Sue Companies that Violate Your Privacy, Elec. Frontier Found. (Jan. 7, 2019), https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy [https://perma.cc/VG7B-M34U] ("[W]hile there is a lot to like about the new California Consumer Privacy Act[,] . . . a significant flaw is its lack of a private right of action.").

82. See infra section I.C.1.

83. Seth F. Kreimer, The Freedom of Information Act and the Ecology of Transparency, 10 U. Pa. J. Const. L. 1011, 1025–27 ("[V]eiled initiatives [including CIA torture and NSA surveillance programs cannot be successfully FOIA'd] until requesters discerned their existence. Indeed, mere hints and suspicions were inadequate; until identified with sufficient specificity that they could be the subject of reasonably precise inquiry, FOIA requests regarding such programs were likely . . . fruitless."); see also Staff of H. Comm. on Oversight & Gov't Reform, 114th Cong., FOIA Is Broken: A Report 26–29 (Comm. Print 2016), https://republicans-oversight.house.gov/wp-content/uploads/2016/01/FINAL-FOIA-Report-January-2016.pdf [https://perma.cc/H3P4-ZHAQ] [hereinafter FOIA Is Broken] (listing examples of "unreasonable standards for a 'reasonable description'"). The CCPA only largely (rather than certainly) avoids this issue because a corporation could conceivably develop new methods or tools that allow for more intrusive data collection and a larger data haul that they keep consumers in the dark about.

Nevertheless, FOIA provides a useful comparator for the CCPA because of the degree to which it inspired the California law and the degree to which both laws share similar aims and operations. Despite the fact that a state legislative staffer disclaimed any connection between the laws,[84] the legislature's sole interest was finding a workable compromise to pull the restrictive initiative from the ballot.[85] Legislators had no particular policy preferences or goals,[86] so the focus of this analysis instead properly remains on Mactaggart and Arney, who took up "the [drafting] pen" during the final legislative negotiations.[87] Mactaggart and Arney were explicitly inspired by FOIA. They believed the CCPA would serve as a "FOIA for corporations"[88] and deliberately set out to make it so.[89] They drafted an initiative-turned-law with a similar request-and-response mechanism as FOIA.[90] They hoped the CCPA would shine a light in the same way that FOIA's drafters intended.[91] While comprehensive consumer data privacy regulation offers more limited practical experience, FOIA's rich history has spawned extensive research and literature, much of it relevant.

While the valid distinctions between FOIA and the CCPA mean that FOIA cannot serve as this Note's exclusive lens of analysis, the law remains tremendously useful. A proper analysis of the CCPA will therefore leverage FOIA without limiting all of its analysis and critiques to the FOIA paradigm. Nonetheless, it is first necessary to understand how request-and-respond provisions operate.

C. *How Request-and-Respond Provisions Operate*

This section provides necessary context to how request-and-respond provisions operate in both the public and the private spheres. Section I.C.1 illuminates the public right to know by examining FOIA. Section I.C.2 examines the early beginnings of CCPA and GDPR practice to glean insights into the private right to data access.

1. *FOIA's Deficiencies.* — Subject to some exceptions, the operative provision of FOIA provides that "each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person."[92] In practice, this means that, after determining what information a requester

84. See supra note 73.

85. Telephone Interview with Senior Staffer, Cal. State Senate (Nov. 16, 2018) (on file with the *Columbia Law Review*).

86. Id.

87. Confessore, Unlikely Activists, supra note 11.

88. Telephone Interview with Rick Arney, supra note 33.

89. Californians for Consumer Privacy, About Us, supra note 70.

90. See infra section I.C.

91. See supra notes 70–72 and accompanying text.

92. 5 U.S.C. § 552(a)(3)(A) (2018).

wants from the government, the requester must figure out which government agency is most likely to have the information.[93] Next, requesters write to the applicable agency and must "reasonably describe" the requested information, while also complying with any specified agency protocols or guidelines.[94] Agencies are required to respond within twenty working days of receiving such requests.[95] If an agency requires an extension, the agency must inform the requester that it will take no more than an additional ten working days to respond to the request.[96] Agencies can refuse to disclose requested information if it comes within nine specified exemptions.[97]

There are, however, enforcement mechanisms and recourse for the requester. If a request for information is denied, requesters can appeal to the agency.[98] That administrative appeal must receive a response within twenty business days of receipt.[99] If the agency denies the appeal, a requester can seek judicial review of the denial.[100]

In practice, scholars have found FOIA "deficient in significant respects."[101] Due, in part, to both expansive exemptions[102] and chronic underfunding,[103] government FOIA practice is frequently criticized for its long processing times and insufficient productions when responses finally arrive.[104] FOIA's administration is handicapped by decentralization across

---

93. Comm. on Gov't Operations, A Citizen's Guide on How to Use the Freedom of Information Act and the Privacy Act in Requesting Government Documents, H.R. Rep. No. 95-793, at 7 (1977). FOIA does not apply to the legislative or judicial branches of government, nor to presidential papers, so a record must be held by an executive administrative agency to be covered by FOIA. Id. at 6.

94. 5 U.S.C. § 552(a)(3)(A); see also How to File a FOIA Request: A Guide, Pub. Citizen, https://www.citizen.org/wp-content/uploads/how_to_file_a_foia_request.pdf [https://perma.cc/N7K7-7B2A] (last visited May 14, 2020).

95. 5 U.S.C. § 552(a)(6)(A).

96. Id. § 552(a)(6)(B)(i).

97. Id. § 552(b)(1)–(9).

98. Id. § 552(a)(6)(A)(i)(III)(aa).

99. Id. § 552(a)(6)(A)(ii).

100. Id. (describing the right to appeal); id. § 552(a)(4)(B) (describing appeal procedures).

101. See David E. Pozen, Freedom of Information Beyond the Freedom of Information Act, 165 U. Pa. L. Rev. 1097, 1099 (2017) [hereinafter Pozen, Beyond FOIA].

102. See FOIA Is Broken, supra note 83, at 8–22 (describing a number of examples "where federal agencies make repeated and extreme efforts to subvert the public's right to access records" by overexempting responses).

103. Charles J. Wichmann III, Note, Ridding FOIA of Those "Unanticipated Consequences": Repaving a Necessary Road to Freedom, 47 Duke L.J. 1213, 1248 (1998) (describing the "underlying cause of FOIA's problems" as "a lack of adequate funding and staffing for agencies' FOIA-processing divisions").

104. Justin Cox, Maximizing Information's Freedom: The Nuts, Bolts, and Levers of FOIA, 13 N.Y.C. L. Rev. 387, 394 (2010) [hereinafter Cox, Maximizing Information's Freedom]; see also Federal Government Sets New Record for Censoring, Withholding Files Under FOIA, CBS News (Mar. 12, 2018), https://www.cbsnews.com/news/foia-federal-government-sets-new-record-for-censoring-withholding-files-trump-administration [https://

the federal government's many component agencies, minimal oversight, institutional pressures, and understaffing.[105] Despite the fact that FOIA appeals are judicially reviewed under the aggressive de novo review standard,[106] courts affirm almost ninety percent of agency denials.[107] FOIA's request-and-response provision proves effective then for only "tenacious requesters who know [exactly] what to look for."[108]

2. *The CCPA Leaves Unanswered Questions.* — The CCPA has a statutorily prescribed data request process like FOIA; however, several operational questions remain after the law's first few months in effect. Under the CCPA, consumers are able to request disclosure of "[t]he categories of personal information" companies have collected, the "categories of sources from which the personal information is collected," the business's purpose in collecting (or selling) the information, the categories of third parties that the business shares personal data with, and the actual, "specific pieces of personal information [the business] has collected about that consumer."[109] Businesses must respond to the data request within forty-five days,[110] but they are not obligated to respond to more than two requests for personal data by an individual consumer in a year.[111] There is no private enforcement mechanism or right of action for a violation of a data access obligation.[112] Instead it appears that the California Attorney General must first notify a business of its noncompliance and give it thirty days to cure a violation.[113] If the business does not comply after thirty days, the state Attorney General may assess a $2,500 fine for each violation (and a $7,500 fine if the violation is deemed intentional).[114] Nothing in the California Attorney General's second proposal of regulations in February 2020 details how consumers can contact the Attorney General's office to report

---

perma.cc/AZ8W-ACL4] (finding that requesters received censored files or no response at all in seventy-eight percent of the 823,222 requests government-wide in 2017).

105. Cox, Maximizing Information's Freedom, supra note 104, at 398.

106. See 5 U.S.C. § 552(a)(4)(B) (2018).

107. Paul R. Verkuil, An Outcomes Analysis of Scope of Review Standards, 44 Wm. & Mary L. Rev. 679, 712–19 (2002) (finding that district courts reversed just ten percent of 3,600 FOIA cases between 1990 and 1999); see also Max Galka, FOIA Litigation: Considering Whether the Costs Are Worth Considering, FOIA Mapper (Sept. 16, 2016), https://foiamapper.com/foia-litigation [https://perma.cc/UN7G-TJKZ] (finding requesters substantially prevailed by gaining access to both the requested records and attorney's fees in only 112 of 1,672 FOIA suits between 2009 and 2014).

108. Pozen, Beyond FOIA, supra note 101, at 1099.

109. Cal. Civ. Code § 1798.110(a) (2018).

110. Id. § 1798.130(a)(2).

111. Id. § 1798.100(d).

112. While a senior staffer speculated that the initial CCPA left the door open to a potential private right of action for a data access violation, Telephone Interview with Senior Staffer, supra note 85, the CCPA clean-up bill, passed in late August 2018, explicitly foreclosed this possibility. S.B. 1121, 2018 Leg., Reg. Sess. (Cal. 2018); see also Cal. Civ. Code § 1798.150(c).

113. Cal. Civ. Code § 1798.155(b).

114. Id.

a violation, or how businesses will, in turn, be notified.[115] At the time of this writing, the Attorney General is not scheduled to begin enforcing the law until July of 2020.[116] The little that can be gleaned from the first few weeks of the CCPA's operation is largely from personal experience. Downloading personal data from some of these companies, such as Apple or Facebook, follows a similar pattern.[117] A user first logs in to the online service or product.[118] A user next navigates to the site's data portal (which Apple calls "Data & Privacy" and Facebook labels "Your Facebook Information").[119] Next, the user selects the specific categories of data in which they are interested (and potentially the timeframe, too) and requests a copy of the data.[120] In January and February 2020 trials, Apple's data took four days to download.[121] Google's data took five hours,[122] while Facebook's, which is also available for browsing through its portal, was ready in just over twenty minutes.[123] Legacy media outlets like *The Atlantic*, on the other hand, that may lack sign-on credentials, require requesters to

---

115. See generally Attorney General, Chapter 20. California Consumer Privacy Act Regulations, Proposed Text of Regulations: Text of Modified Regulations, https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf [https://perma.cc/CL8R-83SZ]; see also Press Release, Xavier Becerra, Att'y Gen., Attorney General Becerra to Hold Public Forums on California Consumer Privacy Act as Part of Rulemaking Process (Dec. 19, 2018), https://oag.ca.gov/news/press-releases/attorney-general-becerra-hold-public-forums-california-consumer-privacy-act-part [https://perma.cc/65ET-66YH].

116. Press Release, Xavier Becerra, Att'y Gen., supra note 115.

117. See Zach Whittaker, How to Download Your Data from Apple, TechCrunch (Oct. 17, 2018), https://techcrunch.com/2018/10/17/how-to-download-your-apple-data [https://perma.cc/9FUA-45YC] [hereinafter Whittaker, How to Download]; see also Accessing & Downloading Your Information, Facebook Help Ctr., https://www.facebook.com/help/1701730696756992?helpref=hc_global_nav [https://perma.cc/GFC9-JCGK] (last visited Jan. 28, 2020); How to Reclaim Your Data from Google, Facebook, Microsoft, Apple Under GDPR, IT Pro (June 20, 2018), https://www.itpro.co.uk/general-data-protection-regulation-gdpr/31330/how-to-reclaim-your-data-from-google-facebook [https://perma.cc/K5VA-3GPU].

118. Whittaker, How to Download, supra note 117.

119. See id.; see also IT Pro, supra note 117.

120. Whittaker, How to Download, supra note 117.

121. Email from Apple to author (Feb. 8, 2020) (on file with the *Columbia Law Review*) ("The data you requested on February 4, 2020 . . . is ready to download.").

122. Email from Google to author (Jan. 25, 2020) (on file with the *Columbia Law Review*).

123. Email from Facebook to author (Jan. 25, 2020) (on file with the *Columbia Law Review*). While Facebook is voluntarily increasing some measures of transparency by providing tools that let its users see for the first time which third-party websites and apps have provided information about the users to Facebook, Dami Lee, Facebook's Clear History Tool Is Now Available to Everyone, Verge (Jan. 28, 2020), https://www.theverge.com/2020/1/28/21111981/facebooks-clear-history-tool-now-available-to-everyone [https://perma.cc/B2TT-DTBD], the social networking giant, like Amazon and Google, is simultaneously claiming the CCPA's "do not sell" request is inapplicable to it because it does not sell user data. Geoffrey A. Fowler, Don't Sell My Data! We Finally Have a Law for That, Wash. Post (Feb. 12, 2020), https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq (on file with the *Columbia Law Review*) [hereinafter Fowler, Don't Sell My Data!]. It merely *shares* that data with advertisers looking to microtarget its users—for billions of dollars. Id.

complete a signed "Affidavit of Identity," have it notarized before a notary public, and then physically mail it.[124]

Turning across the Atlantic, there is minimal information to be gleaned from the few months of activity of GDPR's similar data request right.[125] With GDPR's enactment, some major, multinational companies have extended GDPR-mandated data access rights to their American customers, too.[126] GDPR compliance posed a trickier challenge for other businesses. Research by a cloud data company found that roughly seventy percent of 103 surveyed businesses failed to provide user data within the GDPR's prescribed month.[127] And over 1,000 U.S. news sites opted to block European access rather than adhere to GDPR.[128] There are otherwise limited results available describing how GDPR's data access has operated.

II. THE CCPA'S REQUEST-AND-RESPOND PROVISION IS A FALSE PROMISE OF CONSUMER EMPOWERMENT

Inspired by over fifty years of FOIA, Part II argues that a request-and-respond data access provision presents insurmountable organizational, user-based, and behavioral concerns. Even in conjunction with other reforms,

---

124. Email from Atlantic to author (Jan. 27, 2020) (on file with the *Columbia Law Review*). For fuller examinations of which companies are providing CCPA data access rights to consumers (either in California or nationwide), lists have been compiled by journalists, see Fowler, Don't Sell My Data!, supra note 123, by crowdsourcing websites, see California Privacy Directory, Github, https://caprivacy.github.io/caprivacy/full [https://perma.cc/WP49-4BAX] (last visited Feb. 16, 2020), and by advocacy groups, see CCPA: Use the California Consumer Privacy Act to Protect Your Personal Information, Common Sense, https://www.donotsell.org [https://perma.cc/WN3V-96E2] (last visited Mar. 2, 2020).

125. GDPR requires that companies collecting and processing data on consumers must provide that data, along with other information, when a data subject (or a consumer) requests it. General Data Protection Regulation, supra note 22, at 11. Otherwise, they are subject to a fine and potential criminal liability. See, e.g., Stephen Eckersley, Info. Comm'r Office, Enforcement Notice to Ainsworth Lord Estates Limited 5 (June 18, 2018), https://ico.org.uk/media/action-weve-taken/enforcement-notices/2259303/ainsworth-lord-estates-en-20180618.pdf [https://perma.cc/AM8F-CZNK].

126. See supra note 23 and accompanying text.

127. The Majority of Businesses Surveyed Are Failing to Comply with GDPR, According to New Talend Research, Talend (Sept. 13, 2018), https://www.talend.com/about-us/press-releases/the-majority-of-businesses-are-failing-to-comply-with-gdpr-according-to-new-talend-research [https://perma.cc/AP7U-PG2D]; see also Ponemon Inst., The Race to GDPR: A Study of Companies in the United States & Europe 1 (2018), https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf [https://perma.cc/AYV8-GETE] (finding that almost half of over 1,000 surveyed companies would not be ready to meet GDPR's requirements by its enactment date).

128. Jeff South, More than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months After GDPR Took Effect, NiemanLab (Aug. 7, 2018), http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect [https://perma.cc/S3PJ-DAGK]; see also Len De Groot (@lendegroot), Twitter (Dec. 22, 2018), https://twitter.com/lendegroot/status/1076509597253361664 [https://perma.cc/67UR-WFV2] (describing how seven months after GDPR's enactment date, "Finally, @latimes is visible in Europe").

these provisions represent a false promise of consumer empowerment that will fall short of mounting an effective lobby against problematic corporate data practices. Instead of empowering users, request-and-respond data access will burden them in a manner consistent with prior targeted transparency regulations; these burdens fall upon consumers in the data space where they are uniquely unsuited to the challenge of managing their own privacy. Critically, the law lacks any mechanism to move from thousands of disaggregated and decontextualized data disclosures to an effective lobby against problematic data practices, which may be either invisible from the data or only tangentially related. Section II.A demonstrates that an individual-dominated requester pool does not facilitate broader transparency aims. Section II.B argues that the request-and-respond data access provision's reliance on the individual represents another example of failed targeted transparency in consumer protection. Finally, section II.C steps outside of the FOIA context and applies a privacy self-management critique to explain how this transparency romanticism takes the exact *opposite* lessons from past privacy experience on how to achieve change.

A. *First-Person Requests Do Not Serve the CCPA's Transparency Aims*

After considering how FOIA is dominated by individual requesters, this section demonstrates how the CCPA's similar requester pool will lead the law to fall short of its aims. Section II.A.1 first reviews the shared transparency aims of FOIA and consumer data privacy reformers. Section II.A.2 examines how FOIA's individual, "first-person" requesters crowd out more public-facing requests. Finally, section II.A.3 illustrates how similar dominance of the CCPA by individual interests abandons a critical public orientation while failing to enhance transparency.

1. *FOIA and CCPA Reformers Shared High Hopes for Transparency.* — The reformers responsible for FOIA and the CCPA shared a strong belief in transparency as a tool for the press to highlight ills for subsequent regulation.[129] While FOIA's public orientation and the CCPA's private focus are distinguishable, there is still a clear through line in this great faith in transparency. In the Progressive Era, transparency was wedded to the vision of "a more vigorous and egalitarian regulatory state capable of taming private economic interests."[130] This was seen not only in the writings of Louis Brandeis but also in the muckraking journalists of the era[131] who believed

129. See supra notes 66–72 and accompanying text.

130. Pozen, Drift, supra note 67, at 108.

131. Charles Edward Russell, The Story of the Nonpartisan League: A Chapter in American Evolution 64 (1920) ("To right any wrong in the United States is, after all, a simple process. You have only to exhibit it where all the people can see it . . . ."); see also Doris Kearns Goodwin, The Bully Pulpit: Theodore Roosevelt, William Howard Taft, and the Golden Age of Journalism 324 (2013) ("[T]he 'groundbreaking trio' of [Ida] Tarbell, [Lincoln] Steffens, and [Ray] Baker produced three exhaustive, hard-hitting investigative pieces that ushered in the distinctive new period of journalism that would later be christened 'the muckraking era.'"). Tarbell's journalism focused on "the predatory, illegal

that "'shameful facts, spread out in all their shame,' would set fire to the American pride," leading citizens to seek solutions to "unchecked industrialism."[132]

Decades later, the "culture of transparency" in the 1960s and '70s led to a host of significant reforms focused largely on the rise of the sprawling, federal, administrative state.[133] These postwar transparency advocates shared with their Progressive progenitors a desire to create a more equitable playing field through responsive and effective regulation.[134] These activists spawned many significant reforms, the "crown jewel[]" of which was the Freedom of Information Act.[135] The House Report for FOIA stated that "[a] democratic society requires an informed, intelligent electorate."[136] To that end, FOIA was conceptualized "by journalists, for journalists," so they could use government information to inform the public and "facilitate [its] effective participation in democratic governance."[137]

Alastair Mactaggart and Rick Arney, the reformers responsible for the CCPA, expressed a similar faith that given increased transparency, the press could effectively inform the public about data issues. Arney explained that the CCPA's data access right arose from a belief that "transparency is really important as a first step, so people can understand where their information is going."[138] He expressed confidence that "the press will get on this" and "wake up" the public by producing articles that "chronicle the lifecycle of [consumers'] information" and explaining how their personal information has been diced, sliced, and sold.[139] While Mactaggart and Arney are not looking to "take down Google," they share an overriding Brandeisian belief that "[p]roblems are solved with daylight."[140]

---

practices of Standard Oil"; Steffens illuminated political corruption in Minneapolis; and Baker hammered manipulative and deceptive union practices. Id.

132. Goodwin, supra note 131, at 325.

133. See Schudson, supra note 66, at 10–25; Pozen, Drift, supra note 67, at 115–17. See generally Herbert N. Foerstel, Freedom of Information and the Right to Know: The Origins and Applications of the Freedom of Information Act (1999) (reviewing the shift towards transparency during the Kennedy Administration and the origins of the Freedom of Information Act).

134. See supra note 133 and accompanying text.

135. John Moon, The Freedom of Information Act: A Fundamental Contradiction, 34 Am. U. L. Rev. 1157, 1158 (1985); see also David E. Pozen, Deep Secrecy, 62 Stan. L. Rev. 257, 314 n.204 (2010) ("FOIA introduced a norm of open access to government documents that has commanded deep public loyalty, taken on a quasi-constitutional valence, and spawned a vast network of imitator laws at all levels of United States government and in democracies around the world.").

136. H.R. Rep. No. 89-1497, at 12 (1966), reprinted in 1966 U.S.C.C.A.N. 2418, 2429; S. Rep. No. 88-1219, at 8 (1964).

137. Kwoka, FOIA, Inc., supra note 76, at 1371 (reviewing the origins of FOIA).

138. Telephone Interview with Rick Arney, supra note 33.

139. Id.

140. Id.

2. *FOIA Falls Short Because Its Requester Pool Is Dominated by Individuals.* — Professor Margaret Kwoka has recently demonstrated that FOIA's requester pool is dominated by individuals who primarily use FOIA to secure their own benefits.[141] Kwoka has documented the prevalence of individual, "first-person" requests, where an individual requests records from a government agency about themselves.[142] After corporate entities, first-person requests predominate, constituting twenty percent of requests.[143] First-person requesters use FOIA to secure public or private benefits and documents of personal interest.[144]

Despite FOIA's aim of serving as a media-facilitated tool of government oversight, first-person FOIA requests "crowd[] out" media requesters leading to years-long delays.[145] These requesters "tax the system," degrading the service journalists receive from FOIA officials more accustomed to handling rote first-person requests than responding in a timely fashion to more complicated (and newsworthy) requests.[146] This is demonstrated by the fact that media organizations accounted for less than eight percent of requests over a recent three-year span.[147] Any nonmedia individuals who aspire to turn a first-person request into something more newsworthy are also liable to fall prey to what might be called FOIA's postrequisite knowledge problem[148]—the inability of nonexpert requesters to properly analyze and understand received records.[149] To rectify some of

---

141. Margaret B. Kwoka, First-Person FOIA, 127 Yale L.J. 2204, 2207–11 (2018) [hereinafter Kwoka, First-Person FOIA].

142. See id. at 2217 ("[W]hen John Doe requests from a particular agency all records about John Doe, that constitutes a first-person FOIA request.").

143. Max Galka, Who Uses FOIA?—An Analysis of 229,000 Requests to 85 Government Agencies, FOIA Mapper (Mar. 13, 2017), https://foiamapper.com/who-uses-foia [https://perma.cc/EM3W-NQ24] [hereinafter Galka, Who Uses FOIA?].

144. Kwoka, First-Person FOIA, supra note 141, at 2243.

145. Id. at 2253–54; see also Delayed, Denied, Dismissed: Failures on the FOIA Front, ProPublica (July 21, 2016), https://www.propublica.org/article/delayed-denied-dismissed-failures-on-the-foia-front [https://perma.cc/3T5S-5NNH].

146. Kwoka, First-Person FOIA, supra note 141, at 2254–55; see also, e.g., FOIA Is Broken, supra note 83, at 35 (documenting how a FOIA request for a list of all FOIA requests in a specified period of time was denied by the CIA because it would require an "unreasonable effort").

147. Galka, Who Uses FOIA?, supra note 143; see also Frequent Filers: Businesses Make FOIA Their Business, Soc'y of Prof. Journalists (July 3, 2006), https://web.archive.org/web/20171025232839/http://www.spj.org/rrr.asp?ref=31&t=foia [https://perma.cc/V2YN-W622] (finding news media made up only six percent of the 6,000-plus requests made to seventeen agencies in September 2005).

The mere number of media requests does not necessarily speak to their potential journalism impact. Yet the share of non-public-facing requests necessarily means that these agencies' FOIA officials are tasked primarily (if not exclusively) with instead serving these interests. Kwoka, FOIA, Inc., supra note 76, at 1381.

148. For a description of FOIA's prerequisite knowledge problem, see supra note 83 and accompanying text.

149. See Nadia Hilliard, Monitoring the U.S. Executive Branch Inside and Out: The Freedom of Information Act, Inspectors General, and the Paradoxes of Transparency, *in*

these issues, Kwoka has proposed affirmative, online access (with no need for a formal request) for repetitive individual requests.[150]

3. *The CCPA's Requester Pool Will Also Cause It to Fall Short.* — Individual domination of the CCPA undermines the law's broader goals in two key ways. First, this domination abandons the notion of a public data pollution problem in favor of individual interests. And it does so while burdening these same individuals with a transparency task they are wholly unsuited for. This subsection examines each in turn.

Despite the fact that a first-person requester pool is expressly contemplated by the CCPA's design,[151] individuals pursuing their own private interests are unlikely to spur the additional regulation that reformers like Arney expect and hope for.[152] Individual domination will allow consumers to access their data from a company to learn what a company has collected, where the company collected it, why the company collected it, and with whom the company shared it.[153] Purportedly.[154] Yet these individual, siloed data dumps for one-off users, alone, do not speak to the scope of the current collective data pollution problem,[155] nor are they able to overcome a status quo where users "are complicit in regimes of data-monitoring and data-mining that damage their individual personhood and the democratic system."[156]

Furthermore, as the privacy self-management discussion in section II.C helps elucidate further, consumers lack the ability to parse these data dumps[157] and glean the useful insights necessary to spur more collective action. A survey early this year revealed that nearly three quarters of users

---

Troubling Transparency: The History and Future of Freedom of Information 166, 172–77 (David E. Pozen & Michael Schudson eds., 2018) (describing the expertise paradox of FOIA).

150. Kwoka, First-Person FOIA, supra note 141, at 2262–65.

151. Cal. Civ. Code § 1798.140(g) (2018) (defining the "consumer" who can request their records as "a natural person who is a California resident"). This is another distinction from FOIA, whose requesting "person" includes not only natural persons, but also a "partnership, corporation, association, or public or private organization." 5 U.S.C. § 551(2) (2018).

152. Telephone Interview with Rick Arney, supra note 33 (explaining his hope that "a lot of policies [will] spawn from" the right of data access).

153. Cal. Civ. Code § 1798.110(a). Consumers may then use that data to exercise other CCPA rights, including restricting the sale or exchange of their data, id. § 1798.120, porting their data to a competitor, id. § 1798.100(d), or deleting it, id. § 1798.105(a).

154. See Greg Bensinger, So Far, Under California's New Privacy Law, Firms Are Disclosing Too Little Data—Or Far Too Much, Wash. Post (Jan. 21, 2020), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency (on file with the *Columbia Law Review*) (detailing how "requests under the new law reveal huge variance in the data the companies disclose").

155. See supra notes 61–65 and accompanying text.

156. David Pozen, Irresistible Surveillance?, Concurring Opinions (Mar. 14, 2016), https://web.archive.org/web/20190203232014/https://concurringopinions.com/archives/2016/03/irresistible-surveillance.html [https://perma.cc/BMP6-BGR4].

157. See Bensinger, supra note 154 (quoting a data scientist who collected data about himself via the CCPA as stating, "Either they give you a fire hose of information that is almost impossible to interpret . . . or they give you practically nothing").

did not know Facebook curated a list of their interests and traits to better target ads at them, and over half were uncomfortable with the social network doing so.[158] This information is accessible through a request-and-respond data provision, but it is unlikely that any consumer will find it. Facebook's data response consists of twenty-four folders with labels such as "messages," "photos-and-videos," "location history," and "search history."[159] Buried inside the "ads" folder lies a private site titled "ads_interests.html," which includes the curated list of traits and interests.[160] A user would only find this list if they knew both what they were looking for and where to find it.[161] And even then, the list does not reveal which advertisers Facebook has shared that data with.[162]

Given the complexity of the data they receive, consumers' first-person data access requests will not serve the broader public's interest in learning more about corporate data practices. While these individual requesters are

158. Paul Hitlin & Lee Rainie, Facebook Algorithms and Personal Data, Pew Res. Ctr. (Jan. 16, 2019), www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data [https://perma.cc/TWS5-NZYH].

159. David Alpert, Access Your Information, Facebook (on file with the *Columbia Law Review*) [hereinafter Alpert's Data] (last modified Jan. 25, 2020).

160. Id. Ad targeting is not the only part of the data trove that would benefit from further explanation and context; "comments" provides a decontextualized stream of all comments a user has posted throughout their time on Facebook, stripped of everything but the name of the other user whose page the comment appeared on and the date and time. Id. This includes all the times a user has typed "hahaha" into the void, which is rather stark to find on a site whose core mission is connecting people. See Mark Zuckerberg, Bringing the World Closer Together, Facebook (June 22, 2017), https://www.facebook.com/zuck/posts/10154944663901634 [jttps://perma.cc/FM28-AFSA]. The "about_you" folder's initially ominous "face_recognition.html" closed site instead offers a field with a completely unintelligible string of nearly a thousand letters and numbers. Alpert's Data, supra note 159 ("Raw Data: Fu69lvYHGIAEG62eOdG00buT . . . ."); see also Kate O'Neill, Facebook's '10 Year Challenge' Is Just a Harmless Meme—Right?, WIRED (Jan. 15, 2019), https://www.wired.com/story/facebook-10-year-meme-challenge [https://perma.cc/3Z2P-EPF5] (expressing concern that a recent Facebook meme could help "train a facial recognition algorithm on age-related characteristics and . . . age progression"). But see Alexis C. Madrigal, Go Ahead, Post the Stupid Photo of Yourself from 10 Years Ago, Atlantic (Jan. 16, 2019), https://www.theatlantic.com/technology/archive/2019/01/go-ahead-do-10yearschallenge/580624 (on file with the *Columbia Law Review*) (explaining that Facebook had fifteen billion photos ten years ago and has likely already built an "age-progression machine learning system").

161. Even then, the list is useless without additional context. Such context is available here, see, e.g., Louise Matsakis, Most Users Still Don't Know How Facebook Advertising Works, WIRED (Jan. 16, 2019), https://www.wired.com/story/facebook-ads-pew-survey [https://perma.cc/QU4P-R2RL], but it will not always be. As machine learning algorithms progress, many issues will be fundamentally inexplicable. Jordan Pearson, When AI Goes Wrong, We Won't Be Able to Ask It Why, Vice: Motherboard (July 6, 2016), https://motherboard.vice.com/en_us/article/vv7yd4/ai-deep-learning-ethics-right-to-explanation [https://perma.cc/RU2S-T4EV]; see also General Data Protection Regulation, supra note 22, at 71 (detailing the right to explain).

162. See Kurt Wagner, This Is How Facebook Uses Your Data for Ad Targeting, Vox: Recode (Apr. 11, 2018), https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg [https://perma.cc/4VR8-U344].

not likely to crowd out journalistic requesters,[163] they suffer from the same postrequisite knowledge problem as FOIA requesters and are completely unequipped to turn individual data access into anything meaningful for the public good. By way of comparison, reporting the Cambridge Analytica scandal required "an entire year's work, the resources of three news organisations across two continents . . . [,] [a whistleblower] and an undercover film, plus a sheaf of incriminating documents."[164]

First-person data requesters advancing their own private interests will not merely be unable to shed further light on some of these harmful data practices; they may, in fact, actually undermine the CCPA's transparency aims by creating the appearance of openness while stymieing more substantive change.[165] The next section demonstrates how burdening ill-equipped individual users reflects another doomed example of targeted transparency.

---

163. Unlike painstaking agency FOIA responses, however, tech-savvy companies like Facebook, Google, and Apple will likely automate compliance with data access requests. See Kate Conger, How to Download Your Data with All the Fancy New GDPR Tools, Gizmodo (May 25, 2018), https://gizmodo.com/how-to-download-your-data-with-all-the-fancy-new-gdpr-t-1826334079 [https://perma.cc/55NG-X46K].

164. Carole Cadwalladr, Our Cambridge Analytica Scoop Shocked the World. But the Whole Truth Remains Elusive, Guardian (Dec. 23, 2018), https://www.theguardian.com/uk-news/2018/dec/23/cambridge-analytica-facebook-scoop-carole-cadwalladr-shocked-world-truth-still-elusive [https://perma.cc/23TU-25KX].

165. The CCPA may also unintentionally exacerbate the existing class differential in privacy. See, e.g., Michele Estrin Gilman, The Class Differential in Privacy Law, 77 Brook. L. Rev. 1389, 1392, 1397 (2012) (describing intrusive data collection methods the poor are uniquely subjected to by both private employers and public welfare agencies). The CCPA, like FOIA, is nominally inexpensive. Compare Cal. Civ. Code § 1798.100(d) (2018) (barring companies from charging for data access requests), with 5 U.S.C. § 552(a)(4) (2018) (limiting costs to document duplication for noncommercial educational, scientific, or media requesters). But just as fully vindicating a FOIA request through litigation requires motivation, "time, money, and expertise," the real benefits of the CCPA will only be available for well-heeled requesters. Pozen, Beyond FOIA, supra note 101, at 1113 (citing Kreimer, supra note 83, at 1020).

A consumer fully exercising their CCPA rights with hundreds of online products and services requires an insurmountable amount of both time and expertise . . . or money. Arney spoke excitedly about the fact that, in drafting the CCPA initiative, he and Mactaggart specifically authorized selected third parties to act on the consumer's behalf, requesting the consumer's data and exercising the law's other privacy rights. Telephone Interview with Rick Arney, supra note 33 (anticipating that these third parties will find out what information companies have collected and bar that information's further sale). Companies that are building these capabilities have already approached Arney, id., and privacy-focused start-ups recorded a significant boost in funding the year the CCPA passed. AngelList Weekly, 2018: The Year Privacy-Focused Startups Took Off, Proshare (Dec. 28, 2018), https://www.proshareng.com/news/Tech-Start-Ups/2018–The-Year-Privacy-Focused-Startups/43314 [https://perma.cc/B8M5-9G6T].

However, since the CCPA sensibly prohibits these companies from letting consumers indirectly "pay" for their services with additional data, see Cal. Civ. Code § 1798.140(t)(2)(A), consumers will have to pay directly for privacy. See Stacy-Ann Elvy, Paying for Privacy and the Personal Data Economy, 117 Colum. L. Rev. 1369, 1384–1400 (2017) (reviewing the different business models under which consumers pay for privacy). While Arney is optimistic that this new CCPA privacy management industry will be largely automated and therefore

B. *Request-and-Response Data Access Exemplifies Failed Transparency-As-a-Substitute Regulation*

This section contextualizes the CCPA's individual burden as another example of targeted transparency replacing more meaningful and substantive consumer protection regulation. Section II.B.1 traces the ideological drift of transparency that spawned this trend. Section II.B.2 ties the CCPA's request-and-respond provision's "see-through" and "hollowed out" regulation to other unsuccessful examples of neoliberal, transparency-inspired consumer protection.[166]

1. *Defining and Tracing Transparency's Ideological Drift.* — Transparency began as a progressive ideology and drifted rightward over time.[167] Professor David Pozen has clarified the drift theory as an idea's shift over time from an association with a certain policy or reform agenda ("political orientation X") to a substantial association with reform goals of "political orientation not-X."[168] In the Progressive Era, transparency was bound "to a reform agenda that aimed to limit the influence of big business and to produce more efficient, scientific, and democratically accountable regulation."[169] Since then (and especially in the half century since FOIA's passage), transparency's status as a norm and virtue of good governance has grown,[170] while the ties "between open government and active government" have significantly frayed.[171] Transparency is now used to argue for minimizing the regulatory power of the state and maximizing the freedom

---

relatively inexpensive, Telephone Interview with Rick Arney, supra note 33, a struggling family may still be forced to pick between groceries and a monthly privacy management subscription. See Sandra Fulton, Pay-for-Privacy Schemes Put the Most Vulnerable Americans at Risk, Free Press (May 10, 2016), https://web.archive.org/web/20171122122756/https://www.freepress.net/blog/2016/05/10/pay-privacy-schemes-put-most-vulnerable-americans-risk [https://perma.cc/38D6-87YQ].

166. See Pozen, Drift, supra note 67, at 148 ("Several of the ways in which transparency's meaning has shifted—for instance, through the co-optation of open records and open meetings regimes by unanticipated users—arose in a decentralized manner and do not appear to reflect any coherent neoliberal plan.").

167. See id. at 102 ("[T]he pursuit of transparency has become increasingly unmoored from broader 'progressive' values such as egalitarianism, expertise, or social improvement through state action and increasingly tied to agendas that seek to reduce other forms of regulation and to enhance private choice.").

168. Id. at 106. Professor Jack Balkin initially conceptualized ideological drift, offering free speech and racial "colorblindness" as two preliminary examples. J.M. Balkin, Ideological Drift and the Struggle over Meaning, 25 Conn. L. Rev. 869, 871 (1993).

169. Pozen, Drift, supra note 67, at 108; see also supra notes 130–132 and accompanying text.

170. See Letter from Paul A. Miltich, Special Assistant to the President for Pub. Affairs, White House 1 (Oct. 25, 1974) (on file with the *Columbia Law Review*) ("Critics of [President Ford's veto of the 1974 FOIA amendments] have . . . [said] that rejection of the freedom of information bill is unthinkable . . . . [I]t's true that 'freedom of information' is a catch phrase. Who in a democracy is opposed to freedom of information? Better you should be against motherhood.").

171. Pozen, Drift, supra note 67, at 123.

of markets,[172] as demonstrated by regulated firms using FOIA to impede government oversight.[173]

2. *Targeted Transparency as a Substitute Will Fail to Fix Consumer Data Issues.* — Consumer protection transparency measures fail both because they do not improve consumer decision making and because they act as substitutes rather than complements to robust, substantive regulation.[174] Laws like the CCPA are a product of the drift that section II.C.1 describes, which launched targeted transparency to the exclusion of ex ante measures.[175] Targeted transparency laws were championed as some of the most tolerable forms of oversight because they "inform and educate rather than regulate."[176] Unlike more substantive regulation, targeted transparency obviates any need to identify specific harmful practices and behaviors in the first instance or consider meaningful possible negative externalities resulting from regulation.[177] In a distinctly neoliberal turn,[178] targeted transparency devolves the locus of decision making from a central government actor to

---

172. Id. Conservative and libertarian groups like the Federalist Society have also used transparency to spark conversations about regulatory excess. About the Project, Regulatory Transparency Project, https://regproject.org/about [https://perma.cc/J84V-DT4E] (last visited Jan. 28, 2020).

173. See Pozen, Beyond FOIA, supra note 101, at 1115–16, 1125–27.

174. Pozen, Drift, supra note 67, at 162–63.

175. The CCPA's backers explained that they were not out "to kill" any specific business model but instead sought to shed light on data practices that they found to be "out of control." Confessore, Unlikely Activists, supra note 11.

176. Paula J. Dalley, The Use and Misuse of Disclosure as a Regulatory System, 34 Fla. St. U. L. Rev. 1089, 1092 (2007). Examples of mandatory disclosure regimes include drinking water purity, nutritional content of food, lead paint in residences, SUV rollover rates, genetically modified foods, workplace safety hazards, and airline safety incidents. Mary Graham, Information as Risk Regulation: Lessons from Experience 1–4 (2001), https://ash.harvard.edu/files/information_as_risk_regulation.pdf [https://perma.cc/Q9YX-64YZ]; see also Schudson, supra note 66, at 93–97 (describing the rise of mandatory nutritional labeling in the United States).

177. See Dalley, supra note 176, at 1093.

178. Professors David Singh Grewal and Jedediah Purdy have explained that neoliberalism is a program of "market fundamentalism" that consistently promotes capitalist imperatives against contrary democratic priorities. David Singh Grewal & Jedediah Purdy, Introduction: Law and Neoliberalism, 77 L. & Contemp. Probs., no. 4, 2014, at 1, 6. According to neoliberal theory, robust private contracting rights, like tech users agreeing to terms and conditions under the "notice-and-consent" model, are best suited to promoting individual dignity, freedom, and welfare. See id. Neoliberalism focuses on consumer purchases and the sort of "unfettered consumer choice," id. at 13, that allowed frivolous Facebook apps to harvest user data. See Ian Bogost, My Cow Game Extracted Your Facebook Data, Atlantic (Mar. 22, 2018), https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214 (on file with the *Columbia Law Review*). This consumer choice presupposes a certain semblance of true consumer autonomy, which has been effectively destroyed by the use of consumer databases that can exploit consumers' most individual and idiosyncratic vulnerabilities through extensive behavior and profile modeling. Vincent Manzerolle & Sandra Smeltzer, Consumer Databases and the Commercial Mediation of Identity: A Medium Theory Analysis, 8 Surveillance & Soc'y 323, 323–24, 334 (2011).

a localized individual.[179] The early returns on the CCPA bear this out. Not only do they include some examples of companies providing data "that require[] a data science degree to understand," but those who are most engaged with the law are provided limited options for sparking a broader transformation; users are told to examine their data, keep an eye out for anything worrisome, request the company delete such data and/or stop doing business with a company that vacuums up either too much or the wrong sorts of data, and finally, inform the California Attorney General.[180]

Consistent with the prior discussion about how first-person requesters are ill-suited to the task of making sense of their data,[181] Professors Omri Ben-Shahar and Carl Schneider have documented mounting evidence that targeted transparency regimes fail.[182] Mandated responders fail to provide information or else the requesters fail to receive it; requesters do not follow through with reading the disclosed data, do not understand it if they do read it, and do not act on it if they read and understand it; and requested information fails to meaningfully improve the requesters' decisionmaking.[183] This compilation of failures was seen in the recent case of Amazon's Ring security cameras, which fully complied with a prior California transparency mandate to "conspicuously post its privacy policy" to potential users,[184] while it provided its Ukraine-based engineers "virtually unfettered access to . . . every video created by every Ring camera around the world."[185]

Apart from failing to meaningfully inform and educate its intended recipients, targeted transparency has also drifted rightward as it is increasingly used "to stave off" more robust and market-disruptive means of regulation.[186] Targeted transparency was never intended to be an end in itself: Instead, its proponents envisioned government actors willing to reengage with prophylactic methods of regulation where transparency proved it

179. Dalley, supra note 176, at 1092–93.

180. Fowler, supra note 123.

181. See supra section II.A.3.

182. Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 U. Pa. L. Rev. 647, 651 (2011).

183. Id. at 665; see also infra section II.C (describing the behavioral economics issues plaguing consumers in this arena).

184. See Cal. Bus. & Prof. Code § 22575 (2019); Privacy Notice, Ring, https://shop.ring.com/pages/privacy-notice [https://perma.cc/3F6H-L4HJ] ("If you choose to activate this [facial recognition] feature, we obtain certain facial feature information about the visitors you ask your Ring product to recognize.").

185. Sam Biddle, For Owners of Amazon's Ring Security Cameras, Strangers May Have Been Watching Too, Intercept (Jan. 10, 2019), https://theintercept.com/2019/01/10/amazon-ring-security-camera [https://perma.cc/PG9R-EY3L] (detailing how, using only the customer's email address, U.S.-based Ring executives and engineers could also access "unfiltered, round-the-clock [customer] live feeds," independent of any real task-related need).

186. Pozen, Drift, supra note 67, at 162.

necessary.[187] In other words, transparency's uncovering of "the inner workings of institutions" is not intended to function as a self-congratulatory dead-end but rather as an impetus for "new modes of responsive regulation and democratic action."[188] This transparency triumphalism "hurt[s] the people it purports to help" by crowding out more optimal, tailored regulation.[189] Meanwhile, industry groups have even begun challenging these quintessential light-touch mandatory disclosures as overly cumbersome or deceiving,[190] just as the tech industry endeavored to first kill and later preempt the CCPA.[191]

Mactaggart and Arney admitted to grander (and more concrete) ambitions than reining in data practices. They hoped the CCPA would end the use of the "notice and choice" consent model in tech, leading to more consumers opting out of data sharing, and the eventual end of the third-party data market.[192] Yet their regulation fails to accomplish this directly, instead putting the onus on individual users to act, and then hoping that they do so, in the desired fashion, en masse. The next section helps explain why requiring consumers to "privacy self-manage" to achieve this hope is bound to fail as a means of collective regulation.

---

187. Id. at 136. Examples of these sorts of regulations include Louis Brandeis's advocacy for a ban on large banks having overlapping directors, Louis D. Brandeis, Serve One Master Only!, Harper's Wkly., Dec. 13, 1913, at 10 [hereinafter Brandeis, Serve One Master Only!]; the Magnuson-Moss Warranty Act's prohibition on conditioning warranties on tie-in sales, 15 U.S.C. § 2302(c) (2018); and legendary consumer advocate Ralph Nader's push for airbags, Katharine Macdonald, Nader: Firms Push Seat Belts to Avoid Air Bags, Wash. Post (Mar. 1, 1985), https://www.washingtonpost.com/archive/business/1985/03/01/nader-firms-push-seat-belts-to-avoid-air-bags/652f8a11-8c73-4fe0-91e4-7d06726590d5 (on file with the *Columbia Law Review*).

188. Pozen, Drift, supra note 67, at 113–14. Louis Brandeis's famed admonition about the disinfecting value of sunlight did not stop him from advocating for more muscular regulation when it was needed. Louis D. Brandeis, What Publicity Can Do, Harper's Wkly., Dec. 20, 1913, at 10–13. In fact, he took the results of the congressional investigation that exposed the moneyed trusts as a jumping-off point to recommend a full suite of further, more prophylactic regulations. Brandeis, Serve One Master Only!, supra note 187, at 10–12.

189. Ben-Shahar & Schneider, supra note 182, at 651. Pozen pointed to how mandated disclosures on home loans shielded predatory lenders rather than assisting the intended low-income beneficiaries. Pozen, Drift, supra note 67, at 138–39.

190. See Amanda Shanor, The New *Lochner*, 2016 Wis. L. Rev. 133, 168–69 (recounting how the tobacco industry initially compromised on product warning labels, only to later turn around and challenge them on First Amendment grounds); see also Pozen, Drift, supra note 67, at 140 n.191 ("The deregulatory goalposts thus keep shifting.").

191. See Kang, Tech Industry, supra note 37; Colin Lecher, Amazon, Microsoft, and Uber Are Paying Big Money to Kill a California Privacy Initiative, Verge (June 15, 2018), https://www.theverge.com/2018/6/15/17468292/amazon-microsoft-uber-california-consumer-privacy-act [https://perma.cc/Z97E-P3N6].

192. See Confessore, Unlikely Activists, supra note 11 (quoting CCPA initiative backer Alastair Mactaggart as arguing that when people increasingly opted out of data sharing, "[t]hird-party tracking would essentially end. So when you log in to Spotify . . . [y]ou wouldn't have 75 percent of the websites in the world looking over your shoulder").

C. *Request-and-Response Exacerbates Flawed Privacy Self-Management*

This section leaves the FOIA literature and uses both behavioral economics principles and Professor Daniel Solove's privacy self-management critique to demonstrate how a request-and-respond data access right ignores critical lessons learned about privacy.[193] Section II.C.1 describes the issue of scale that individuals have managing their privacy and data with myriad entities. Section II.C.2 examines consumers' difficulty in assessing harm, given both individual and societal data aggregation.

1. *The Increasing Scale of Digital Life Makes Effective Management Impossible.* — Consumers will struggle to manage their privacy because doing so effectively requires evaluating and acting on data relationships with nearly countless corporate entities.[194] While consumers may remember to request their data from Facebook, they may not know (or remember) to also request their data from their cell service provider who is selling their real-time location data to companies who, in turn, resell it to bounty hunters.[195] Consumers must request their data, make sense of it after receiving it,[196] and then act on it. Doing so dozens of times for different troves of data in hopes of managing these relationships quickly becomes unwieldy.[197]

The difficulties of self-managing consumer privacy are further illustrated by behavioral economics. Consumers are only boundedly rational, meaning they misjudge or make mistakes in perception, and possess only bounded willpower, so even when they decide on a rational goal, consumers struggle to see it through.[198] While the CCPA's light-touch data access

---

193. See infra note 195.

194. Recent research found that consumers maintain, on average, 191 online accounts. Amber Gott, LastPass Reveals 8 Truths About Passwords in the New Password Exposé, LastPass (Nov. 1, 2017), https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose.html [https://perma.cc/AD32-LJ8H].

195. Joseph Cox, I Gave a Bounty Hunter $300. Then He Located Our Phone, Vice: Motherboard (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile [https://perma.cc/XBC8-CA9H] (detailing how third-party location aggregators resell locational information to groups "ranging from car salesmen and property managers to bail bondsmen and bounty hunters"); see also Danielle Keats Citron, Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age, 80 S. Cal. L. Rev. 241, 243–51 (2007); Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880, 1889 (2013) (detailing the many corporations collecting user data unbeknownst to the user).

196. See supra section II.A.3 (describing the trove of Facebook data).

197. Solove, supra note 195, at 1889; see also Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 564 (2008) (calculating the total cost of everyone reading every privacy policy they encountered in a year to be $781 billion).

198. Ryan Bubb & Richard H. Pildes, How Behavioral Economics Trims Its Sails and Why, 127 Harv. L. Rev. 1593, 1603 (2014). The combination of bounded rationality and willpower plague even the most tech savvy among us, as demonstrated by the 2019 release of romantic texts Amazon CEO Jeff Bezos sent to his lover. See Kara Swisher, Opinion, The Sexts of Jeff Bezos and the Death of Privacy, N.Y. Times (Jan. 18, 2019), https://www.nytimes

may correct some of the information asymmetries currently plaguing consumers[199] while functioning as the most "choice-preserving" regulation,[200] such choice is rendered effectively meaningless where behavioral economics demonstrates that consumers will either be unable to do the sophisticated valuation involved in determining the best course of action,[201] or, if such a course is known, be unwilling to see it through. Over and over, at scale.

2. *Data Aggregation Poses Another Threat.* — The harm assessment required by privacy self-management is rendered more difficult by the aggregation of both a single individual's data and all of society's data. While a person may rationally choose to share an individual piece of data in isolation, the cumulative effects of countless pieces of the individual's data can be hard to anticipate or fully understand. The *New York Times* acutely demonstrated this in a 2018 article, tracking a specific woman to an overnight stay at an ex-boyfriend's house and a Weight Watchers meeting through a combination of technically anonymized app locational data and publicly available information.[202] Consumers' bounded rationality leads them to ignore these sorts of privacy risks, or miscalculate their odds and potential magnitude.[203] Consumers also overvalue short-term gains and undervalue long-term consequences.[204] They are likely, therefore, to give up locational information for the immediate payoff of access to a free app, even where there is known damage in the long run.[205] Request-and-respond data access will

---

.com/2019/01/18/opinion/amazon-jeff-bezos-affair.html (on file with the *Columbia Law Review*) ("If the man who wants to put listening devices [Amazon Echo smart speakers] in everyone's home doesn't always know that everyone's always watching, I don't know who will.").

199. See Telephone Interview with Rick Arney, supra note 33 (describing Arney's optimism about consumers learning more about the lifecycle of their data).

200. See Bubb & Pildes, supra note 198, at 1597.

201. Consumers also do not make transactional decisions in a privacy-specific vacuum: Privacy is most often a by-product rather than *the* core good or service, and consumers are even worse at evaluating trade-offs in these combinatorial transactions. See Alessandro Acquisti & Jens Grossklags, What Can Behavioral Economics Teach Us About Privacy?, *in* Digital Privacy: Theory, Technologies, and Practice 363, 368 (Alesssandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis & Sabrina De Capitani di Vimercati eds., 2008).

202. Jason Koebler, Delete All Your Apps, Vice: Motherboard (Dec. 10, 2018), https://motherboard.vice.com/en_us/article/j5zap3/delete-all-your-apps [https://perma.cc/UE9V-4T5M] ("The apps on your smartphone are tracking you . . . . [F]or all the talk about 'anonymization' and claims that the data is collected only in aggregate, our habits are so specific—and often unique . . . so that anonymized identifiers can often be reverse engineered and used to track individual people."); Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (on file with the *Columbia Law Review*); see also Solove, supra note 195, at 1889 (describing how sophisticated entities combine and analyze data to reveal sensitive or harmful information never intended for disclosure).

203. Acquisti & Grossklags, supra note 201, at 368.

204. See id. at 370–72.

205. Id. at 373.

allow users to know more about the totality of locational information surrendered, but users are unlikely to be able to meaningfully evaluate this information without technical expertise or a team of investigative journalists.[206]

Aggregation is further complicated by the data disclosures made by people other than the user in question. Privacy is a public good that can be enjoyed by everyone equally, no matter their respective contributions.[207] Privacy risks not being "produced" on a societal level in certain situations when it actually serves each individual's respective self-interest to trade away some modicum of their personal privacy for a good or service.[208] This, in turn, leads to everyone's privacy being eroded through the aggregation of large data sets that allow data brokers to unleash predatory marketing efforts on the poor[209] and Facebook to predict users' future locations, even when they are offline.[210] This phenomenon has led Professors Joshua Fairfield and Christoph Engel to observe that "[i]ndividual control of data is a fundamentally flawed concept because individuals cannot know what the data they reveal means when aggregated."[211] Data access fails because the production of one individual's data is necessarily divorced from the context of a broader dataset where the key threats to privacy and broader society lie.

III. CONSUMERS AND POLICYMAKERS NEED COMMAND-AND-CONTROL REGULATION

Part II explains how decentralized, decontextualized, and atomized request-and-respond data access will fail to effectively promote future substantive regulation. This Part examines two alternative solutions: a system of tailored affirmative disclosure and preventative, command-and-control regulation. This Part settles on the latter as the more effective means to

---

206. See supra note 165 and accompanying text.

207. Joshua A.T. Fairfield & Christoph Engel, Privacy as a Public Good, 65 Duke L.J. 385, 387 (2015).

208. Id. at 425.

209. Elvy, supra note 165, at 1423. Data brokers have used labels like "Rolling the Dice," "Fragile Families," "Ethnic Second-City Strugglers," or "Rural and Barely Making It." Staff of S. Comm. on Commerce, Sci. & Transp., 113th Cong., A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes 24 tbl.1 (Comm. Print 2013), https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577 [https://perma.cc/6EEB-ADHT].

210. Nicole Nguyen, Facebook Filed a Patent to Calculate Your Future Location, Buzzfeed (Dec. 10, 2018), https://www.buzzfeednews.com/article/nicolenguyen/facebook-location-data-prediction-patent [https://perma.cc/4J9V-9VQ4] ("[T]he technology . . . use[s] the data of other people you know, as well as that of strangers, to make predictions."); see also Fairfield & Engel, supra note 207, at 388–91.

211. Fairfield & Engel, supra note 207, at 390 ("[P]eople who buy felt pads for furniture are more likely to [return] loans . . . ; people who log into their credit-card accounts at 1:00 a.m. may . . . [have] financial anxiety; and people who use credit cards at [bars] are more likely to default on loans than people who use [them] at . . . dentist[s].").

ameliorate both the private and societal harms from the data industrial complex. Section III.A examines affirmative disclosure systems, and section III.B considers ex ante, preventative regulation.

A. *Affirmative Disclosure Ameliorates Some Concerns, but Leaves Most Unaddressed*

This section considers the merits of a tailored affirmative disclosure regime. Section III.A.1 examines how affirmative disclosure may be tailored to fit the consumer data privacy context. Section III.A.2 concludes that despite its potential benefits, affirmative disclosure is ultimately insufficient to resolve the request-and-respond provision's fundamental mismatch with the scope of the current consumer data problem.

1. *Affirmative Disclosure Can Be Tailored to the Consumer Data Privacy Context.* — Affirmative disclosure is a legislative mandate requiring a public or private body to publish "certain categories of information in a certain manner and pursuant to a certain timeline."[212] Unlike the CCPA's request-and-respond provision, an affirmative disclosure regime might immediately provide an accessible privacy portal once a user verified her identity through a standard username and password.[213] The disclosure could display some of the same key insights that the CCPA contemplates, including the personal information the company has collected on a user, when and why it was collected, and with whom the company has shared the data or sold it to.[214]

Affirmative disclosure can be further tailored to the consumer data privacy space. Companies could be compelled to disclose not only the personal information itself, but what exactly that personal data is worth to them.[215] Companies might be mandated to disclose both what the "average" consumer chooses to do with this information (and their data) and what the company does with consumers' data once they get a hold of it.[216] Affirmative disclosure could also require divulging the categories of information collected with specific, intelligible examples to the broader public, with an eye aimed at interested journalists and government regulators.

---

212. Pozen, Beyond FOIA, supra note 101, at 1107.

213. This helps counter Professor Kwoka's concerns about affirmative disclosure being ill-suited to private or personal information. Kwoka, First-Person FOIA, supra note 141, at 2262.

214. Washington state at one point was considering such a regime in its "GDPR-lite" bill. Telephone Interview with Alex Alben, Chief Privacy Officer, Wash. State (Dec. 25, 2018).

215. This, in some respects, seems to be a policy innovation contemplated by the CCPA's nondiscrimination provisions. See Cal. Civ. Code § 1798.125(b)(1) (2018) (allowing companies to offer differential prices to consumers, but only if based on the value of the data).

216. See Oren Bar-Gill, Seduction by Contract: Law, Economics, and Psychology in Consumer Markets 33–39 (2012).

2. *Even Tailored Affirmative Disclosure Ultimately Fails.* — There are significant benefits to this manner of tailored, affirmative disclosure regime. First, by eliminating requester pools and providing the means for regulators and muckraking journalists to access the information they need upfront, the overarching transparency aims of the law will be better attended to.[217] And behaviorally, designing these privacy portals to contain helpful "nudge"-like information such as the average consumer's choice can help overcome some of consumers' bounded rationality limitations.

Affirmative disclosure will nevertheless fail both individuals and society. Boosting transparency is still no end in itself, and disclosure may crowd out more substantive regulations.[218] Behaviorally, affirmative disclosure does not speak to bounded consumer willpower and will fail because it "offers no real commitment device."[219] It also does not help individuals who are unable to make sense of the vast quantity of data.[220] Instead, proper regulation will require limits on certain behaviors that prohibit the consumer from making a data transaction that they may otherwise desire, whether or not the consumer is fully informed of the risks and costs, because society has deemed these transactions too costly.[221]

B. *More Prophylactic, Preventative Regulation Is Needed*

This section explains why more prophylactic, command-and-control regulation is needed and what such regulation might look like. Section III.B.1 lays out the case for more stringent, preventative measures. Section III.B.2 explores the possibility of multiple such regulations, eventually settling on a Pigouvian tax as the most promising.

---

217. This will keep big tech companies consistently in the disinfecting sunlight to allow for future, flexible regulation as the industry continues to change, innovate, and grow.

218. See supra notes 186–191 and accompanying text (describing substitute transparency regulation).

219. Bubb & Pildes, supra note 198, at 1649. Behavioral economics literature explains that mandatory, affirmative disclosures fail to significantly improve outcomes in situations in which the complexity remains acute and firms have strong incentives to undermine consumer choice. Id. at 1638; see also Andrew Hasty, Treating Consumer Data Like Oil: How Re-Framing Digital Interactions Might Bolster the Federal Trade Commission's New Privacy Framework, 67 Fed. Comm. L.J. 293, 304 (2015) (detailing how companies hide their privacy practices). And by better highlighting the need for services like third-party privacy managers, affirmative disclosure may actually exacerbate the distributional concerns of a class differential in privacy.

220. See Bensinger, supra note 154.

221. Consumer privacy activist and former FTC technologist Ashkani Soltani recently characterized Silicon Valley's business model as akin to "selling you coffee and making it your job to decide if the coffee has lead in it . . . . [W]e have no baseline law that says you can't put lead in coffee." Confessore, Unlikely Activists, supra note 11. That, ultimately, is the issue with data access even in the affirmative disclosure form: While mandated access may empower a knowledgeable and sophisticated subset of consumers to learn that their coffee contains lead, it does not remove it or otherwise save those who may already be addicted to their caffeine fix.

1. *Preventive Regulation Is Needed to Curb Unrestrained Data Collection.* — Ex ante, command-and-control regulation is necessary because the CCPA's promise of consumer empowerment is bound to fail. Data access, be it through a request-and-respond or affirmative disclosure model, prizes individuals' interests over the public's.[222] These individuals fail to enhance a form of transparency[223] that is itself a poor substitute for substantive regulation.[224] And consumers need such regulation because of their inability to effectively manage their own data and privacy.[225]

Substantive regulation must replace the disaggregated, decontextualized, and atomized data dumps if society is to assert more democratic control over the "common good" of personal data.[226] And society must do so to encourage the production of a privacy public good[227] and ameliorate the negative externalities that result from public, data pollution harms.[228] Transparency efforts may preserve consumer choice, but they are "particularly weak medicine" when, as here, firms seek to undermine consumer autonomy.[229] When even third-party data brokers express an openness to transparency-focused consumer data privacy measures,[230] it becomes necessary to consider the regulatory alternatives transparency may be concealing.[231] Once consumer data has been collected, society is exposed "to stochastic and largely unbounded harms," indicating, as Professor Ian

---

222. See supra notes 151–158 and accompanying text.

223. See supra notes 163–164 and accompanying text.

224. See supra notes 186–191 and accompanying text.

225. Then-Judge Stephen Breyer previously encapsulated one of the key tensions between increased information and more substantive regulation: "Those who favor warnings argue in favor of consumer choice and claim that warnings are adequate to overcome the informational defects in the marketplace . . . . Those who favor banning a [practice] often argue there is no way to convey a meaningful warning." Stephen Breyer, Regulation and Its Reform 163 (1982).

226. See Ben Tarnoff, Silicon Valley Siphons Our Data like Oil. But the Deepest Drilling Has Just Begun, Guardian (Aug. 23, 2017), https://www.theguardian.com/world/2017/aug/23/silicon-valley-big-data-extraction-amazon-whole-foods-facebook [https://perma.cc/4PLC-JDED] ("[W]e make [data] *meaningful* together, since useful patterns only emerge from collecting and analyzing large quantities of it.").

227. See Fairfield & Engel, supra note 207.

228. See supra notes 61–65 and accompanying text.

229. Bubb & Pildes, supra note 198, at 1600. Meaningful choice has been effectively destroyed by the use of consumer databases that can exploit consumers' most individual and idiosyncratic vulnerabilities through extensive behavior and profile modeling. Manzerolle & Smeltzer, supra note 178, at 323; see also Paul M. Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 Iowa L. Rev. 553, 560 (1995) (describing how corporate surveillance is fundamentally geared to shaping and pushing consumers towards revenue-maximizing choices).

230. Becky Peterson, Acxiom, a Huge Ad Data Broker, Comes Out in Favor of Apple CEO Tim Cook's Quest to Bring GDPR-like Regulation to the United States, Bus. Insider (Jan. 21, 2019), https://www.businessinsider.com/acxiom-supports-apple-ceo-tim-cooks-call-for-data-regulation-2019-1 [https://perma.cc/8CLK-BY26].

231. See Marilyn Strathern, The Tyranny of Transparency, 26 Brit. Educ. Res. J. 309, 310 (2000).

Samuel argues, that we have reached "the final nail in the coffin for an ex post resistance strategy."[232] The personal data economy, therefore, must be regulated as the extractive industry it has become.[233] There are a variety of possibilities for command-and-control regulation, but the optimal choice is the one that directly internalizes the costs of data collection by firms.

2. *Taxing Data and Other Modes of Ex Ante Regulation.* — The CCPA's drafters hoped that their transparency efforts would eventually lead to the end of the third-party data economy.[234] Banning the third-party data market may come with significant costs, however, and will not operate as a panacea. Data can create enormous "positive externalities,"[235] so cutting off an entire avenue for companies to profit from consumer data will almost certainly reduce, if not eliminate, many of these externalities. Shutting down the third-party data market will significantly curtail the profits of (if not totally end) the data broker industry; thus, proposals to do so will likely meet strong political resistance. Ending the third-party data market will also hamstring the tailoring and targeting efforts of advertisers that lead to the personalization that some users enjoy.[236] While, in this Note's view, the benefits of a direct ban on third-party data collection outweigh its costs,[237]

---

232. Ian Samuel, The New Writs of Assistance, 86 Fordham L. Rev. 2873, 2910–11 (2018).

233. Confessore, Unlikely Activists, supra note 11 ("To Silicon Valley, personal information had become a . . . limitless natural deposit, formed in the digital ether by ordinary people as they browsed, used apps and messaged . . . . Like the oil barons before . . . , they had collected and refined that resource to build some of the most valuable companies in the world . . . ."); see also Tarnoff, supra note 226 ("A company that yanks copper out of an earth that belongs to everyone should be governed in everyone's interest. So should a company that yanks data out of every crevice of our collective lives.").

234. Confessore, Unlikely Activists, supra note 11.

235. Ben-Shahar, Data Pollution, supra note 61, at 134 ("For example, Google Trends—a service that uses Google's search data for purposes different than those for which it was collected and stored—provides valuable clues about social phenomena such as the spread of medical and social ills.").

236. See Widening Gap Between Consumer Expectations and Reality in Personalization Signals Warning for Brands, Accenture Interactive Research Finds, Accenture (May 3, 2018), https://newsroom.accenture.com/news/widening-gap-between-consumer-expectations-and-reality-in-personalization-signals-warning-for-brands-accenture-interactive-research-finds.htm [https://perma.cc/8RWT-ZBQ3] (detailing the degree to which consumers value data-facilitated personalization). But see Alexis C. Madrigal, If It Wasn't the Pregnancy Tests, Why *Did* Baby Catalogs Start Arriving at Our House?, Atlantic (Apr. 18, 2013), https://www.theatlantic.com/technology/archive/2013/04/if-it-wasnt-the-pregnancy-tests-why-did-baby-catalogs-start-arriving-at-our-house/275072 (on file with the *Columbia Law Review*) (expressing concern about predictive marketing).

237. A direct ban would provide a number of positive benefits. Limiting the market for consumer data would decrease the value of such data in nonbrokers' hands (and limit the incentive to collect in the first place). It would limit the amount of aggregating, processing, and targeting firms can undertake, which would decrease the scope of the privacy intrusion facilitated by current data aggregation practices. Consumer-facing services' data collection and processing would be limited to the extent of their direct capabilities to do so. Indirectly, the incentives for internal data collection would decrease to the amount such activities directly increase businesses' revenues from the core services or products they offer to

the current infeasibility of such an aggressive proposal renders it fatally flawed. Billion-dollar industries with positive externalities have not historically disappeared overnight.[238] Reformers are better off pushing for incremental, substantive reforms that can help break the entrenched power of industry. Policymakers have many options to better regulate mass data collection, retention, aggregation, and analysis; this subsection focuses on restricting the third-party data economy by considering some plausible, alternative solutions.

These incremental reforms, or other entirely different alternatives, may still make a positive impact. These might include limiting the quantity of data that can be collected, devising some sort of licensing scheme to institute better, "safer" data collection, and prescribing specific technology requirements for data collectors.[239]

These solutions all have significant drawbacks. Limiting data quantity is too blunt a tool that ignores data's positive effects.[240] Creating a licensing or permitting scheme would be costly and lead to overprotection.[241] And specific technology prescriptions focused on transparency and security, on the other hand, would not be attentive enough to overcollection and retention of consumer data.

The most fruitful solution may be assessing a "Pigouvian tax" at the point of data collection, which, like mandated insurance, might function as a means of internalizing the externalities of consumer data transfers at the time and place of collection.[242] Such a tax would force firms to think more carefully about when, why, and how they collect consumer data. Unlike how polluting industry responds to the carbon taxes that serve as the

---

consumers in their trade or business. Facebook would still target advertisements at its users, but those ads would be less precisely targeted (and less valuable to Facebook's customer advertisers) without the augmentation of data from third-party brokers. Target may still be able to accurately forecast when customers are pregnant based off their in-store purchases, Charles Duhigg, How Companies Learn Your Secrets, N.Y. Times Mag. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (on file with the *Columbia Law Review*), but other big box stores would likely never again send a data broker-facilitated letter addressed to "Daughter Killed in Car Crash or Current Business." Kashmir Hill, OfficeMax Blames Data Broker for 'Daughter Killed in Car Crash' Letter, Forbes (Jan. 22, 2014), https://www.forbes.com/sites/kashmirhill/2014/01/22/officemax-blames-data-broker-for-daughter-killed-in-car-crash-letter [https://perma.cc/6K8W-RMZT].

238. See Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability 23 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/HT5G-VSDH] (calculating almost half a billion dollars in annual revenue for just nine data brokers).

239. See Ben-Shahar, Data Pollution, supra note 61, at 133.

240. See id. at 133–34 ("Data's externalities are . . . bi-directional. Even when emitted (and used for purposes beyond those for which they are primarily collected), data create benefits.").

241. Id. at 136.

242. Id. at 138–39, 147.

inspiration for a data tax,[243] tech firms have every incentive to capture, bundle, and sell the externalities produced by consumer data.[244] Therefore, where firms decide collecting data is in their interest, such costs would be absorbed by them and limit their reach and ability to perform unthinking, vast collection of data. Alternatively, these costs would be passed on to the consumer more directly, and firms would need to articulate and justify why such data collection would be in the consumer's direct interest or risk losing them to a noncollecting competitor. Over time, such a tax would likely lead to less (and more thoughtful) data collection in line with the principles the CCPA's backers set out to achieve.

CONCLUSION

In December 2018, the *New York Times* reported that Facebook had shared users' data with over 150 third-party companies to boost user growth on Facebook and facilitate partners' new features.[245] Facebook gave Spotify and Netflix the power to read its users' private messages, granted Microsoft's search engine the ability to see all of a user's friends, and gave the *Times* itself continuing access to user data even six years after the publication had shuttered the underlying application.[246] In response to this report, *Consumer Watchdog*'s Privacy and Technology Project Director John M. Simpson described the CCPA's request-and-respond data access provision as a "powerful tool to stop Facebook's ongoing privacy abuses. [Consumers] could ask what [Facebook] had and [tell the company] to stop sharing it."[247]

This author has asked Facebook what it has. Even with the story firmly in mind, it was impossible to find or see this privacy abuse, let alone do anything to stop it. Simpson exhibits the same transparency romanticism that plagues the CCPA. His analysis is grounded in the belief that once people learn a little bit more about a problematic practice, a solution will miraculously emerge. This unwavering faith in transparency abandons the hard-won lessons learned since the Progressive Era and fails to provide any

243. Id. at 139–40.

244. Id. at 140.

245. Gabriel J.X. Dance, Michael Laforgia & Nicholas Confessore, As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants, N.Y. Times (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (on file with the *Columbia Law Review*) (describing how these data sharing arrangements "underscore how personal data has become the most prized commodity of the digital age, traded on a vast scale by some of the most powerful companies in Silicon Valley and beyond").

246. Id.

247. John M. Simpson, Landmark California Consumer Privacy Act Would Have Let People Block Facebook's Sharing of Private Data, Consumer Watchdog Says, Consumer Watchdog (Dec. 20, 2018), https://www.consumerwatchdog.org/privacy-technology/landmark-california-consumer-privacy-act-would-have-let-people-block-facebooks [https://perma.cc/6VEF-DXFQ].

sort of roadmap for how to move from disclosure and knowledge to actual, substantive reform.

Simpson's analysis hints at other issues, both FOIA-related and FOIA-independent, with the CCPA's data access right. When corporations misuse consumers' data, the onus remains on individual, behaviorally-flawed users to self-manage their own privacy. And those individuals who do access their data and somehow restrict Facebook from sharing it promote their own interests but fail to address broader democratic transparency concerns. Some may instead call for a system of affirmative disclosure that shifts the burden to companies like Facebook to proactively share what data they have collected and how they use it with consumers. But this still presents a flawed example of targeted transparency. Proper consumer protection in this space requires more robust, preventative measures that better internalize certain methods of data collection, transfer, and analysis.