Putting the Price on Privacy: Decommodifying Data with the Fiduciary Model

Talia Bank
Macalester College
tbank@macalester.edu

Abstract: Engaging with the internet and digital technologies is more invasive than ever before and the platforms that make it so have weaponized the law to shield themselves from the consequences of their exploitative business models. Federal data privacy laws in the U.S. are woefully inadequate and no law currently regulates private sector data collection and commodification, a process that undermines transparency, privacy, autonomy, and democracy itself. But the information economy does not operate in a lawless space; rather, it is the product of legal innovations and political maneuvers on the part of platforms during the early development of the digital age. Data propertization as a tool for ensuring privacy protections, if enacted at the national level, would be a continuation of that harmful legacy. The information fiduciary model is a promising alternative and presents a real opportunity to not only protect user privacy, but to also restructure the information economy towards greater transparency and greater responsiveness to user interests.

Since the advent of computers in the 1950s and the creation of the World Wide Web in 1989, the internet has grown exponentially in terms of its reach and ability to affect life outside the digital realm. About 4.66 billion people are active users of the internet worldwide—nearly 60% of the world's population.[1] According to a 2021 Pew report, 93% of adults in the U.S. use the internet, up from just 52% in 2000, and 72% use at least one social media platform.[2] In a

---

[1]Statista. (2022, May 4). Worldwide Digital Population April 2022. www.statista.com.statistics/617136/digital-population-worldwide

[2] Perrin, A., & Atske, S. (2021, March 26). *About three-in-ten U.S. adults say they are 'almost constantly' online*. Pew Research Center. http://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online.
Pew Research Center. (2023, April 7). *Internet/broadband fact sheet*. Pew Research Center: Internet, Science & Tech. Retrieved from http://www.pewresearch.org/internet/fact-sheet/internet-broadband.
Auxier, B., & Anderson, M. (2021, April 7). *Social media use in 2021*. Pew Research Center: Internet, Science & Tech. http://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021.

country of 330 million, about 230 million have shopped for and purchased products online.[3] It is undoubtedly true that the internet is actively revolutionizing the way people interact with one another and the world. In just several decades, it has rapidly increased access to information, globalized commercial markets, and connected individuals and groups thousands of miles apart.

However, these arguably positive effects of digitalization towards greater connectivity and participation in the global economy can obscure a more sinister function: just as the internet broadens access to various commodities and social networks, so it serves as a vehicle through which the online behavior of its users, whether social, economic, or miscellaneous in nature, is itself commodified. With the emerging ubiquity of the internet and its ever-expanding number of users, platforms that enable online activity have become privy to massive amounts of information about people who visit their websites. Each search, click, like, share, and save serve as windows into the lives of internet users—indicators of their interests and attachments and predictors of their behavior as consumers. Tracking technologies such as cookies, Flash cookies, and web beacons facilitate mass data collection by enabling information-sharing between user devices and sites and servers; while they partly serve to enhance web services by, for example, allowing users to save passwords and usernames or items in a virtual shopping cart, their parallel purpose is that of allowing third parties such as advertisers and analytics companies to track online engagement and behavior.[4] This process often occurs without users' explicit and comprehensive knowledge. Notice of third-party tracking and data collection is often hidden in

---

[3] *U.S. and World Population Clock*. United States Census Bureau. (n.d.). Retrieved April 22, 2023, from https://www.census.gov/popclock/
Number of digital shoppers in the U.S. 2021. Statista. (2017, September). Retrieved from https://www.statista.com/statistics/183755/number-of-us-internet-shoppers-since-2009/

[4] Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of internet commerce*, *10*(1), 1-16.

terms of use agreements or privacy policies that over 90% of users do not bother to read or fail to comprehend when they do.[5] These documents tend to employ complex, legalistic language that can span hundreds to thousands of pages; privacy policies and terms of use agreements are overwhelmingly ineffective for *informed* consent.[6] While cookies are more visible to users since many websites offer some kind of consent to cookies banner on their pages and a significant number of users elect to delete their overall browser cookies periodically in any case, other technologies like Flash cookies and web beacons are designed to avoid detection and deletion; user knowledge of the ways in which these are used for advertising and other commercial activities remains obscure and inaccessible.[7]

Even when users are not actively browsing the internet, simply traveling with a smartphone produces detailed location data that apps can and do collect and sell to advertisers and commercial outlets.[8] Shopping at an in-person retailer while paying digitally for any purchases has a similar effect. Despite the fact that location data is typically anonymized, it can be easily linked to one's identity with publicly available residential and occupational records, as

---

[5] Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128-147.

[6] Bashir, M., Hayes, C., Lambert, A. D., & Kesan, J. P. (2015). Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, *52*(1), 1-10.

[7] Sipior, et al. (2011). 7-13.

[8] Valentino-DeVries, J., Singer, N., Keller, M. H., & Krolik, A. (2018, December 10). *Your apps know where you were Last night, and they're not keeping it secret*. The New York Times. Retrieved from https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

well as information from social media.[9] Besides, whether or not personal data can ever be truly anonymous, and many argue it cannot, it is nonetheless being commodified through a shadow economy of data brokerage that users do not engage with directly, cannot fully understand due to lack of transparency, and therefore cannot truly consent to. Anonymity ultimately means little if one's value as a consumer hinges less on their name and address and more on their interests, hobbies, and lifestyles. The breach of privacy exists regardless of how far platforms and companies go to either anonymize, or de-anonymize the data they collect; it is more so the practice of extracting data itself, rather than the process of anonymizing it, that defines information privacy or lack thereof.

Even when users are concerned about data privacy issues, and an overwhelming number of Americans are, it is unlikely that they will avoid using the internet and other technologies capable of personal data collection or change their behavior using these digital platforms in order to protect their privacy.[10] Initially coined by Hewlett Packard employee Barry Brown in 2001, scholars have continued terming this behavioral quirk "the privacy paradox"— a real and widespread worry over the pervasiveness of personal data collection and invasion of privacy coupled with little to no change in one's online activity and interactions with technology to protect privacy.[11] Notably, the prominent information privacy scholar Daniel Solove and others

---

[9] Hern, A. (2019, July 23). *'Anonymised' data can never be totally anonymous, says study*. The Guardian. https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds
De Montjoye, Y. A., Radaelli, L., Singh, V. K., & Pentland, A. S. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, *347*(6221), 536-539.
Kolata, G. (2019, July 23). *Your Data Were 'Anonymized'? These Scientists Can Still Identify You*. The New York Times. Retrieved from https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html

[10] Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and privacy: Concerned, confused and feeling lack of control over their personal information.

[11] Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*, *77*, 226-261.

have criticized the privacy paradox as a simplification of nuanced individual processes of weighing risks and rewards when it comes to behavior on the internet.[12] In Solove's telling, the privacy paradox falsely equates a series of specific choices on the part of individual users with a general failure to take action to protect their own privacy. The process of changing one's behavior to achieve a measure of information privacy is "a vast, complex, and never-ending project that does not scale" and therefore should not be the vehicle through which society pursues privacy protections. More broadly, scholars have critiqued approaches to data privacy that center individual users as agents of change, whether that be the option to opt-out of or opt-in to data collection, access to private browsers, or more simplified privacy policies and terms of use agreements.[13] While these strategies certainly offer some benefit, they also shift the onus of ensuring privacy from digital platforms to users and consumers. By proposing *user-led* efforts as primary strategies for information privacy, regulators and policymakers imply that platforms are off the hook and have little to no responsibility to change the commercial practices that undermine the privacy of their users and exploit their tendency to divulge vast troves of personal information. To heed Solove's warning then, it is imperative that the privacy paradox be

---

[12]Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, *89*, 1.

[13]Liu, Z., Sockin, M., & Xiong, W. (2020). *Data privacy and temptation* (No. w27653). National Bureau of Economic Research.
See Liu et al.'s discussion on opt-in/opt-out data privacy systems and the persistent threat to the privacy of users who opt-out by those who opt-in;
Lyons, K. (2021, March 13). *Judge rules Google has to face lawsuit that claims it tracks users even in Incognito mode*. The Verge. Retrieved from https://www.theverge.com/2021/3/13/22329240/judge-rules-google-5-billion-lawsuit-tracking-chrome-incognito-privacy
McDonald, A. M., & Cranor, L. (2008). The cost of reading privacy policies. *I/S: Journal of Law and Policy for the Information Society, 4(3),* 543-568.
Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.*, *10*, 273.

understood as representing the relative vulnerability and powerlessness of individual users in the face of hidden commercial mechanisms beyond their control and invisible to the untrained eye.

In today's interconnected and increasingly digitized world, it is also extremely difficult to avoid an online presence altogether if one is concerned about advancing their career, finding a job or recruiting for one, keeping up with current events, and connecting with loved ones across vast distances, among many other activities familiar to modern life for many Americans. Of course, it is not impossible to avoid the internet, but as more people adopt and integrate technology into their daily lives, it will become harder for the hold-outs as they inevitably miss out on the opportunities, conveniences, and livelihoods afforded by the digital age.[14] Moreover, the harms of using the internet and other technologies in terms of information privacy are not immediately apparent or felt, making digital platforms appear free, accessible, and relatively harmless. But while new technologies have surely benefited humanity in immeasurable ways, they have also allowed for mass data collection, a practice that has actively transformed people into products, commodifying their attention, emotions, hobbies, interests, and values.

Users tend not to divulge this information intentionally or explicitly, as one would do voluntarily by, for example, filling out a survey. Rather, information is extracted from data that users produce by simply using the internet, interacting with others online, or even moving physically with a device. In other words, data and information production is a *by-product* of internet use, which is itself a necessity in an interconnected and digitized economy. But for the information economy, this by-product is the main product, and integral for the multibillion dollar

---

[14] Silva, Christianna. (2017 June 6). *The Internet of Things Is Becoming More Difficult to Escape*. NPR. http://www.npr.org/sections/alltechconsidered/2017/06/06/531747037/the-internet-of-things-is-becoming-more-difficult-to-escape.

industries of targeted advertising, marketing, and data analytics.[15] With personal data, advertisers have the ability to target advertisements to the populations and subpopulations predicted most likely to purchase their products.[16] Likewise, creditors use detailed financial information gathered from all corners of the internet to determine people's financial capacity and creditworthiness.[17] Apps for tracking menstrual cycles have been found to share the personal, and extremely sensitive, data of their users with advertisers, tech companies, and insurers.[18] A shadow economy of data brokerage in which data is packaged and sold within a vast web of interested parties undergirds and facilitates these functions.[19] Regarding the commercial applications of personal data, the list goes on and its limits are indeterminate. Essentially, the collection and application of personal data allows for a more efficient and personalized market, but at the same time gives countless actors intimate glimpses into the lives of users, typically unbeknownst to them.

Moreover, the political implications of the information economy have become more

---

[15] (2022 May 4). *U.S. Digital Advertising Industry - Statistics and Facts*. Statista. www.statista.com/topics/1176/online-advertising/#dossierContents__outerWrapper.

[16] Boerman, Sophie C., et al. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363–76. https://doi.org/10.1080/00913367.2017.1339368.

[17](2022). *Privacy Policy Experian*. Experian. https://www.experian.com/privacy/.
(2021 August). *Equifax Privacy Statement*. Equifax. www.equifax.com/privacy/privacy-statement.
(2021 December 1). *Trans Union LLC Privacy Notice*. TransUnion. www.transunion.com/privacy/transunion.

[18] Gupta, Alisha Haridasani, & Singer, Natasha. (2021 January 28). *Your App Knows You Got Your Period. Guess Who It Told?*. The New York Times. www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html.
Wong, Emily, et al. (2022 January 18). *When Tracking Your Period Lets Companies Track You*. NPR. www.npr.org/2021/12/29/1068930998/when-tracking-your-period-lets-companies-track-you.

[19] Crain, Matthew. (2016). The Limits of Transparency: Data Brokers and Commodification. *New Media and Society*, 20(1), 88–104. Https://doi.org/10.1177/1461444816657096.

apparent and recognized as increasingly problematic for functional democracy.[20] The scandal surrounding the now-defunct analytics company Cambridge Analytica (CA), Facebook, and their role in the electoral victory of the Trump campaign in 2016 and the Vote Leave (Brexit) campaign in 2020 exemplifies the detrimental effects of targeted advertising and other targeted political content. The documentary *The Great Hack* details the ways in which CA's analysts scraped user data from Facebook, translated the behavioral information into predictors of political ideology and psychological vulnerability or predisposition to certain political ideas, and then used their results to target political ads and content and sway voters in a manner bordering on manipulation.[21] Invasion of privacy looms large in this particular scandal, as do issues of autonomy and democracy. CA's former business development director Britanny Kaiser, now a digital literacy and data rights advocate, described CA's operation as focused on "targeting those whose minds we thought we could change…We bombarded them through blogs, websites, articles, videos, ads, every platform you can imagine until they saw the world the way we wanted them to… Until they voted for our candidate."[22] While this paper does not attempt to comprehensively grapple with the effects and implications of targeting content in either commercial or political contexts, these practices are evidently problematic. It should be a goal of

---

[20] Heawood, Jonathan. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information Polity*, 23(4), 429-434.
Kozlowska, I. (2018). Facebook and data privacy in the age of Cambridge Analytica. *The Henry M. Jackson School of International Studies*, 1.
Giorno, Taylor. (2022 April 21). *The Third-Party Brokers Who Make Millions Selling Your Data to Political Groups*. Open Secrets News. www.opensecrets.org/news/2022/04/the-third-party-brokers-who-make-millions-selling-your-data-to-political-groups.

[21] Amer, Karim & Noujaim, Jehane. (2019). *The Great Hack*. USA:Netflix.
Rosenberg, Matthew, et al. (2018 March 17). *How Trump Consultants Exploited the Facebook Data of Millions*. The New York Times. www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[22] Ibid.

literature going forward to question the centrality of these commercial and marketing strategies and challenge their legitimacy in a democracy that purportedly values individual autonomy and freedom from coercion.

Whether oriented around selling products or selling candidates and ideas, the mass collection and commodification of personal information signals the arrival of a new chapter. Shoshana Zuboff's 2019 book, *The Age of Surveillance Capitalism*, popularized the notion that technology companies and other data collectors pose an existential threat to democracy, privacy, and human flourishing.[23] In her telling, the emergent digital economy is a kind of cancerous outgrowth of capitalism gone haywire and best described as a surveillance economy, where data produced by internet users is collected, analyzed, and made profitable by its value as a predictor of human behavior and, by extension, consumer behavior.[24] Zuboff presents "surveillance capitalism" as the resulting framework and dominant logic driving this transformation; a system that "unilaterally claims human experience as free raw material for translation into behavioral data" and represents "the darkening of the digital dream and its rapid mutation into a voracious and utterly novel commercial project…"[25] The result is not simply personalized browsing and advertising and an ever-improving internet experience fueled by machine-learning—even though these *are* products of surveillance capitalism and the information economy. Rather, the chief interest and primary profit-making apparatus of this economic model is the collection of data, the

---

[23]Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Apple books ed., PublicAffairs.

[24] Ibid. at 300, 384-390

[25]Ibid. at 21.

extraction of information, and the execution of commercial practices, like advertising, that capitalize on the observable and applicable behavioral patterns that emerge:

> "Real-world activity is continuously rendered from phones, cars, streets, homes, shops, etc…. back to the digital realm, where it finds new life as data ready for transformation into predictions. They produce a twenty-first-century 'means of behavioral modification'... not to impose behavioral norms, such as conformity or obedience, but rather to produce behavior that reliably, definitively, and certainly leads to desired commercial results."[26]

It is, therefore, the economic structure underlying commercial practices like targeted advertising that exploits the vulnerable position of internet users relative to online platforms and other technologies capable of surveillance. To users, the immense scale of data collection is indefinite, as are the processes by which their personal data is translated into commercially-valuable behavioral information. For platforms and surveillance technologies, whether that be a retailer, a mobile app, or even a personal fitness tracker, the precise contours of the transaction—free and accessible internet and technology usage in return for personal data—are known, understood, and manipulated towards financial gain.[27]

---

[26]Ibid. at 388.

[27]Paul, Kari. (2019 November 6). *'Tossed My Fitbit in the Trash': Users Fear for Privacy after Google Buys Company*. The Guardian. www.theguardian.com/technology/2019/nov/05/fitbit-google-acquisition-health-data.

Zuboff especially condemns Google, the company she claims pioneered the surveillance capitalism business model.[28] Google, and Zuboff's discussion of it, serves as a useful case study for understanding the development of data collection technologies and the profit motive behind their rise. As has been the case with many tracking technologies like cookies, Google initially used the data its users produced as a tool to 'clean up' search results and improve the accuracy and effectiveness of web services like Google translate, voice recognition, and spell check. That is to say, through machine learning, user data was originally used to optimize technology and web services and to offer a user experience that made platforms practical, accessible, and therefore attractive. In this early form, the practice of data collection therefore posed little threat to internet users in terms of privacy and related issues like targeted advertising and behavior modification.

2002 is the year Zuboff marks as the birth of 'surveillance capitalism' through Google's trailblazing use of personal data to not just optimize, but also curate user experience. Through a happy accident, Google found that the user-generated data it had been using to optimize its offerings was just a fraction of a much larger trove of information that could be used to personalize the internet for each and every user through targeted advertising.[29] As a company, Google grasped that what someone searches for and how they search for it, how long they spend interacting with certain content, what they click on, and the various other factors of internet engagement have immense predictive power; based on user-generated data, it's possible for corporate and political actors to surveill users like never before not just predict how they will

---

[28] Zuboff (2019), at 24.

[29] Ibid. At 133-160.

respond to certain content, but also *force* that exact reaction. In Zuboff's telling, Google pursued this strategy and raked in profit from targeted advertising, sparking a new era for capitalism, technology, and society.

Zuboff is effective at framing the issue of information privacy from a social, political, and moral perspective. Her work is a compelling appeal to reassert the centrality of an autonomous, uncoerced human experience in a digital age that values predictability and control over freedom and agency. However, when it comes to legal questions, Zuboff's account has some important limitations. She mentions that the information economy and its commercial stakeholders owe their success to "the neoliberal inheritance, and the realpolitik of surveillance exceptionalism—as well as by their own purpose-built fortifications designed to protect supply chain operations from scrutiny through political and cultural capture."[30] And yet, the majority of her book focuses on describing these "supply chain operations" in real-time, leaving the historical and legal contexts that allow for surveillance capitalism to thrive on the back-burner.

This paper attempts to center the legal history of the information economy in the U.S. and consider current innovations in the legal understandings of data privacy as products of specific socio-legal and political maneuvers and subsequent missed opportunities. The goal here is to build on the exhaustive literature criticizing the information economy, emphasize the legal structures that allow for its unregulated, *legally legitimized* existence, and offer an analysis of two emerging legal responses to the perils of the information economy and trace the ways in which they exacerbate or break with, respectively, the damaging legal and political failures of the past. Namely, this paper will show how viewing personal data as property, and thereby affording

---

[30] Ibid. At 247.

data-specific private property rights to users, further solidifies a legacy of legal immunity for information economy actors engaged in mass data collection and surveillance and offers an information fiduciary model as a promising alternative.

When considering the law of the information economy, Zuboff indicates that surveillance capitalism functions in a lawless space—a kind of digital Wild West.[31] Considering the lack of a federal data privacy statute in the U.S. as well as the Constitution's explicit silence on the issue, "lawless" may appear as an accurate way to describe the current information economy. This state of affairs presents a stark contrast to, for example, the European Union, where the General Data Protection Regulation, enacted in 2018, provides strong privacy protections focused more on reforming and restricting the design and architecture around data collection than individual action to protect privacy[32]. Even where there are legal privacy protections in the U.S., such as in state constitutions, many of these measures still place responsibility on users to take initiative and tend not to challenge the legitimacy of mass data collection itself.[33]

It is worth asking how the U.S. came to the point where data collection has been enshrined in commercial practices, seemingly to the point of no return. Julie Cohen offers a compelling answer through her exploration of the legal, economic, and sociopolitical processes and events that have historically legitimized data collection and surveillance in her book *Between Truth and Power* (2019). Cohen differs in her account from Zuboff in two main ways. Rather

---

[31]Ibid. At 203-206.

[32]Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 47-64.

[33] National Conference of State Legislatures. (2022 April 26). *State Laws Related to Digital Privacy*. *NCSL*. www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

than characterizing the data economy as lawless, she argues that the new business model is a purposeful product of existing legal structures and the pro-business, pro-innovation neoliberal ideology that fuels them. Furthermore, she suggests that while Zuboff's focus on surveillance, control, and behavior modification is more than merited given its pervasiveness, her 'surveillance capitalism' account overlooks the role of law and legal institutions in creating the very conditions necessary for an information economy to come into being, as well as the ways in which stakeholders co-opt legal understandings of concepts like property, speech, and trade secrets in order to enshrine its legality.

Faced with the challenge of responding to the threat of surveillance capitalism and the broader information economy it is situated within, Cohen argues that informational capitalists, or actors in the information economy, actively bend and contort legal frameworks and discourses in order to not only assert the legality of their enterprise, but also to establish its legitimacy through the logics of neoliberalism and innovation. Cohen urges an understanding of law and legal institutions as having a "facilitative role in these processes of economic and ideological transformation… [and are] not simply superstructure but rather the means through which expressions of economic rationality and governmentality become specific, detailed, and actionable."[34] Further,

> "Law for the information economy is emerging not via discrete purposive changes, but rather via the ordinary, uncoordinated but self-interested efforts of information-economy participants and the lawyers and lobbyists they employ…

[34] Cohen, Julie E. (2019). Between Truth and Power: The Legal Constructions of Informational Capitalism. New York: Oxford University Press. 8.

> Legal institutions are the mechanisms through which changes in governmentality assume concrete forms that shape the options available to social and economic participants, and those forms also impose limitations… the previous era's institutional settlements become the residue with which the next era's institutional entrepreneurs must contend."[35]

Cohen's response to Zuboff then is to situate surveillance capitalism as part of a broader information economy embedded within a legal system that stakeholders have intentionally shaped to accommodate the commodification of data and ensure a significant degree of legal immunity. They do so by invoking legal strategies and innovations during litigation such as equating data capture with speech and maintaining the secrecy of algorithms by presenting them as trade secrets, among others.[36] As Amy Kapczynski notes in her side-by-side review of Zuboff and Cohen, by spotlighting these legal developments, Cohen places "Zuboff's concerns in broader perspective: private control of platforms enables not merely behavioral surplus capture and behavioral modification but a host of other new forms of power subject to abuse."[37] But to go back to behavioral surplus capture, or personal data collection, Cohen's bird's eye view encourages a careful examination of history to inform present transformations in the legal world. In fact, if one traces the legal development of information privacy in the U.S., it becomes abundantly clear how the "self-interested efforts of information-economy

---

[35] Ibid. 9

[36] Kapczynski, A. (2020). The law of informational capitalism. *Yale law journal*, *129*(5), 1460-1515.

[37] Ibid. 1489.

participants," as Cohen puts it, have weaponized legal innovations and political ideology to produce not a digital Wild West, but a carefully legalized and legitimated information economy.

In his works *Big Iron and the Small Government* and *None of Your Damn Business*, Lawrence Capello describes this history in a coherent narrative that highlights the federal government's willingness and ability to regulate its own data collection but not that of the private sector.[38] In line with Cohen, he writes, "the current state of data collection was largely a product of political, social, and cultural developments that date back to the Eisenhower era."[39] Rather than being an "inevitable byproduct of technological evolution," mass data collection and the information privacy issues that accompany it are direct consequences of failure "to articulate an idea of privacy capable of formulating effective policies and protections" in the face of intense pressure for deregulation.[40]

Capello traces the development of data collection back to the intersection between the advent of main-frame computers in the 1950s, or "big iron," and the rise of the American welfare state with New Deal liberalism. Using emerging technologies, the U.S. Government acquired, stored, and shared information between agencies about its citizens in the effort to extend social and legal benefits. However, that information was scattered among various agencies, collected on

---

[38]Cappello, L. (2017). Big Iron and the Small Government: On the History of Data Collection and Privacy in the United States. *Journal of Policy History*, *29*(1), 177-196.

[39] Ibid. 178.

[40] Ibid. 179.

an inconsistent basis, and inaccessible to researchers; Big iron had allowed for collecting and storing data, but had not undergone centralization.[41]

Initial reactions to the inextricable relationship between data collection and welfare management were muted, but by the 1960s concerns over privacy became more widespread. A proposal to create a national data center in order to centralize the information the government collected and thus optimize the operations of federal agencies was met with fierce opposition and Congress promptly rejected the idea. At the same time, access to advancing technologies became increasingly democratized over the second half of the twentieth century. By the 1980s, owning and using technology capable of data collection (collecting data on users) such as personal computers became much more widespread.

The technological development and democratization of big iron introduced another dimension into the emerging debate over privacy. Capello points out that privacy advocates "came to face not just the government but a host of commercial entities with varying aims and practices that made the privacy problems they faced more confusing, harder to articulate, and more difficult to address with policy initiatives."[42] Credit bureaus, corporations, insurance companies, and other commercial entities pursued any and all available data to make informed assessments about clients and consumers without their knowledge. The information they gleaned guided decisions on, for example, who was creditworthy, who was more likely to cost insurers, who was a safer bet for a mortgage, and more importantly, who fell on the opposite side of that judgment. In other words, as mentioned previously, data, and the information about people that it

---

[41]Ibid. 182.

[42] Ibid. 180

communicates, has a *predictive capacity*—it is a tool through which commercial entities make profit by identifying consumers most likely to spend more on products and cost less in insurance terms.

Thus, with the increasing use of data collection and sharing among commercial entities, the debate over privacy shifted focus. Whereas with government-led data collection, privacy advocates sought decentralization, which they viewed as "privacy's strongest safeguard," and achieved it through successful resistance to the federal data center proposal, the emerging *commercialization* of information, or the channeling of data's predictive capacity towards commercial, profit-seeking ends, posed new challenges.[43] Rather than centralization, the biggest threat to privacy became the wider dissemination of data—and the shadow economy of data brokerage in which information moves from one entity to another.

Capello argues that privacy advocates failed to shift gears to account for this change and effectively frame the transforming threat to privacy. He describes increased public concern throughout the 1960s and into the 70s, fueled by a growing body of scholarship, journalism, and literature, which pressured Congress to act. In 1970, Congress passed the Fair Credit Reporting Act, the first information policy legislation in the U.S. While the Act provided some meaningful privacy protections—such as requiring credit agencies to disclose information to consumers looking to report any errors, correcting or deleting any inaccurate information, and refraining from reporting outdated information to third parties—it did *not* challenge or change the fundamental process at the root of privacy invasion concerns: data collection on a mass scale. Additionally, the Act only targeted credit reporting agencies, leaving aside a host of other entities

---

[43] Ibid. 183

engaged in data collection. Even then, despite the Act's passage, Capello notes, "Credit bureaus sought out every financial transaction made by their subjects. And sales divisions poured over data purchased by these organizations to better identify prospective buyers and so tailor their direct-marketing campaigns."[44] In practical terms, the Act did not protect consumers, but simply afforded them some additional rights that they could exercise—a user-led effort.

Capello traces the next key point in the development of data privacy to 1973, when the Department of Health, Education, and Welfare (HEW) published a report containing suggestions on how best to give individuals increased access to and control over the information collected, shared, and processed about them. Responding to the HEW report, Congress geared up to pass the Privacy Act of 1974 with various interests engaged in intense lobbying. Those who profited from information collection, such as insurance companies, banks, and even literary publishers, argued that data-related privacy invasions were too vaguely defined and that legislation that was too restrictive would unduly burden private businesses and stifle innovation.[45] These arguments struck a chord in Congress and the final version of the Privacy Act of 1974, while giving individuals access to their data files and placing restrictions on the collection, use, and dissemination of personal information by federal agencies, lacked any regulatory provisions for the private sector. In sum, "by 1974 privacy advocates were pushing against a much more varied array of interests comprised of multiple actors," writes Cohen. "The rhetoric employed by these interests, particularly their economic arguments, complicated the terms of the privacy debate."[46]

---

[44] Ibid. 185.

[45] Ibid. 187.

[46] Ibid. 189.

This rhetoric—the logic of neoliberalism and the worship of innovation, the argument that privacy protections unduly burden companies, and the claim that privacy itself is too vague to serve as a workable standard—holds immense influence over governing institutions to this day. As Cohen suggests, policy entrepreneurs must now contend with the centrality that these ideas have achieved in the legal and political discourses surrounding information privacy and technology more generally. They have defined the parameters of the debate and the feasibility of proposed regulations and most importantly, they have served to advance a legal environment in which information economy actors have carved out a safe haven through their own legal restructuring and retooling of concepts like trade secrets, copyright, patents, and speech.[47] In turn, federal policy has failed to catch up to and curb the ever-increasing power of digital platforms. Federal privacy statutes on the books today are narrowly tailored, pertaining only to certain sectors and only to specific entities within those sectors. For example, the Family Educational Rights and Privacy Act (FERPA) only regulates information collected by schools and education agencies that receive federal funding but overlooks testing companies, surveyors, and other entities.[48] The Genetic Information Nondiscrimination Act (GINA) only regulates the use of genetic information in employment and insurance decisions, overlooking consumer genetics companies.[49] The sector-specific HIPPA, COPPA, GLBA, and FCRA are riddled with similar loopholes; this patchwork approach to data privacy is a direct legacy of information economy actors preventing more robust and comprehensive private sector regulation in 1974.

---

[47] See Cohen, Kapczynski

[48] Barrett, L. (2018). Confiding in Con Men: US privacy law, the GDPR, and information fiduciaries. *Seattle UL Rev.*, *42*, 1057.

[49] Ibid. 1068.

In light of this, it is integral that proposals for data privacy regulation take the missed opportunity to question the legitimacy of mass data collection as a commercial practice inherently invasive of privacy. As Cohen and Capello show, current protections and legal understandings of data privacy are a product of a malleable legal system shaped by pressure from stakeholders in the information economy. While U.S. law now restricts data collection on the part of the government, the behemoth of private interest and what Cohen deems "platform power" has successfully carved out a place for itself in the gray areas between constitutional silence and illegality. Some scholars have sought to challenge the legal ambiguity surrounding data collection and information privacy by proposing to equate personal data with private property, thus extending user private property-like rights over their data. In contrast to data and information privacy, private property protections have long been a pillar of legal entitlement in the U.S. Alan Westin, considered a father of digital privacy scholarship and advocacy, supported the propertization of data in his 1967 book, *Privacy and Freedom*, writing, "personal information, thought of as the right of decision over one's private personality, should be defined as a property right, with all the restraints on interference by public or private authorities and due-process guarantees that our law of property has been so skillful in devising."[50] Since then, the data-as-property model has gained traction in both academic and political communities, in the U.S. and abroad. In their 2017 article advocating for data propertization Ritter and Mayer detail the merits of data-as-property proposals for ensuring privacy, using Estonia, Germany, the automotive industry, and others as case studies.[51] Their

---

[50]Westin, Alan. (1967). *Privacy and Freedom*. Ig Publishing. 222.

[51]Ritter, J., & Mayer, A. (2017). Regulating data as property: a new construct for moving forward. *Duke L. & Tech. Rev.*, *16*, 220.

argument hinges on the claim that data is a tangible asset and is therefore well suited for protection as property in a country that already has robust private property protections. Others have argued for data propertization as a means of legally recognizing user ownership of personal data, a concept undergirding many of the protections in the EU's GDPR as well as in some U.S. state information privacy laws such as California's Consumer Privacy Act.[52]

In the political realm, data privacy in general and data propertization in particular have received greater attention in recent years. In his 2020 campaign for president, Andrew Yang proposed data propertization through a data dividend, where users would be paid by companies for the use of their data.[53] California's governor, Gavin Newsom, has backed a similar payout plan.[54] Data propertization and monetary payment seem to go hand-in-hand, with dividend proposals functioning effectively as rental payments for access to personal information. It is worth examining data propertization and proposals for dividend payouts in light of the legal innovations and political maneuvers of information economy actors that Cohen and Capello have highlighted in their respective works.

While being paid for and enjoying clear ownership over one's personal data can seem not only appealing but also fair, it would also incentivize users to opt-in to data collection.

---

[52] Jurcys, P., Donewald, C., Fenwick, M., Lampinen, M., & Smaliukas, A. (2020). Ownership of user-held data: why property law is the right approach. *Harvard Journal of Law and Technology Digest [2021]*
Victor, J. M. (2013). The EU general data protection regulation: Toward a property regime for protecting data privacy. *Yale LJ*, *123*, 513.
European Union. (2018). *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/
California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. (2022). https://oag.ca.gov/privacy/ccpa

[53]Data Dividend Project. (2021) *Data Dividend Project*. www.datadividendproject.com.
Yang 2020 - Andrew Yang for President. *Data as a Property Right*. yang2020.com/policies/data-property-right.

[54] Ulloa, Jazmine. (2019 May 5). *Newsom Wants Companies Collecting Personal Data to Share the Wealth with Californians*. Los Angeles Times. www.latimes.com/politics/la-pol-ca-gavin-newsom-california-data-dividend-20190505-story.html.

Additionally, putting a price on data privacy would produce disappointingly low payouts; because individual user data is pretty much worthless for its predictive capacity unless it is aggregated with the data of other users, one user's data would yield very little ad revenue and thus a miniscule digital or data dividend.[55] On a political level, it also allows for politicians to claim that they are working to protect data privacy while what they would really be doing by advancing data propertization and dividend proposals is pricing privacy invasion and throwing money at an issue that payouts will *not* solve.

However, these critiques are not original and have been well-documented. And yet, there is a missing piece in the opposition to data propertization. Like the sector-specific federal privacy laws that fail to regulate most commercial actors, the trade secrets law that protects the secrecy of algorithms, and the logics of neoliberalism and innovation above all things, the data-as-property model is at its core a part of the legacy of the 1970s. More specifically, enshrining data as private property would likewise further establish the practice of mass data collection and permanently entrench invasion of privacy as a part of daily life in the digital era. By propertizing data, legal entrepreneurs and policymakers would be turning a page that will be very difficult to unturn.

Instead of propertizing data, institutional actors need a model that breaks with the tradition initiated by the 1974 Privacy Act and provides space for challenging the legitimacy of mass data collection itself rather than accepting it as inevitable. Here, an information fiduciary model emerges as a promising alternative to the flawed vision of data propertization. Developed

---

[55] Tsukayama, Hayley. (2020 October 26). *Why Getting Paid for Your Data Is a Bad Deal*. Electronic Frontier Foundation. www.eff.org/deeplinks/2020/10/why-getting-paid-your-data-bad-deal.
Herman, Sean. (2020 October 30). *Should Tech Companies Be Paying Us For Our Data?* Forbes. www.forbes.com/sites/forbestechcouncil/2020/10/30/should-tech-companies-be-paying-us-for-our-data/?sh=3464c7 c74147.

by Jack Balkin, the information fiduciary model seeks to apply the existing legal relationship of a fiduciary to platforms engaged in data collection. Generally, a fiduciary is a person or entity that enters into a legally binding relationship with a beneficiary in which they are bound to act in the best interests of the beneficiary and exercise care, loyalty, and good faith in whatever service they perform on behalf of the beneficiary.[56] Fiduciary relationships are typically based on trust and ensure that the fiduciary acts in a trustworthy manner when acting on behalf of or performing a service for a beneficiary that lacks similar skills or knowledge. Some examples of fiduciary relationships include doctors and patients, union leaders and the workers they represent, and boards of trustees and the organization they manage.

In a series of papers, Jack Balkin argues for platforms dealing in information and data collection to enter into fiduciary relationships with their users as a means of ensuring data privacy. He writes that because users trust platforms with their data, the relationship between users and platforms mirrors the types of trust-based relationships that are traditionally associated with fiduciaries: "In the midst of these asymmetries of knowledge, power, and control, digital companies hold themselves out as trustworthy enterprises; they in- sist that our data is safe with them and that our privacy and our safety is their central concern. They encourage us to trust them so that we will en- trust them with our data, indeed, with our digital lives."[57] Lindsey Barrett, another scholar writing in support of information fiduciaries notes, "Like traditional fiduciaries, companies that collect enormous amounts of data on individuals have as strategic advantage over their clients due to the fact that they are trusted with the user's sensitive information, in addition

---

[56]Miller, P. B. (2018). The identification of fiduciary relationships. The Oxford Handbook of Fiduciary Law (New York: Oxford University Press, 2019).

[57] Balkin, J. M. (2020). The fiduciary model of privacy. *Harv. L. Rev. F.*, *134*, 11.

to superior and specialized knowledge, lack of transparency, and the reliance of their users on the specialized services provided."[58] An information fiduciary relationship would impose upon digital platforms certain responsibilities towards protecting consumer privacy that they have been resistant to undertake.

Balkin's critiques of the current state of affairs center on the failure of many privacy approaches to ensuring that the architecture of the information economy is itself scrutinized. Recognizing that "digital companies create the environment in which end users operate," Balkin and fellow information fiduciary advocates propose an approach that may potentially ask whether the practice of data collection itself is a legitimate action for a fiduciary to engage in.[59] Unlike data propertization then, the information fiduciary model breaks with entrenched legal underpinnings of the information economy by seeking to fundamentally restructure the relationship between users and platforms. That said, the information fiduciary model *is* a developing idea and contains notable gaps when it comes to what defines information fiduciary responsibilities, who defines them, and who enforces them. Chair of the Federal Trade Commission Lina Khan has criticized information fiduciaries with David Pozen in a 2019 law review, arguing that information fiduciaries, because of the questions left unanswered about the specifics of their operation, are too vague to be of practical use and ill-fitting as a privacy model. They correctly note, "it is not hard to imagine how the interests of a social media company's stockholders and users could come apart," leading to an implausibility that companies will put

---

[58] Barrett, Confiding in Con Men

[59] Balkin, 16.

users first in matters of data collection.[60]Additionally, Khan and Pozen introduce a humorous yet eerily accurate portrayal of what an information fiduciary may look like for a digital platform:

> "To appreciate just how odd it is to think that a behavioral-advertising company could be a fiduciary for its users, imagine visiting a doctor — let's call her Marta Zuckerberg — whose main source of income is enabling third parties to market you goods and services. Instead of requesting monetary payment for services rendered, Dr. Zuckerberg floods you (and her two billion other patients) with ads for all manner of pills and procedures from the second you set foot in her office, and she gets paid every time you try to learn more about one of these ads or even look in their direction. In fact, this is just about the only way she gets paid — as her financial backers are apt to remind her."[61]

These critiques are strongly justified, but the efficacy of the information fiduciary model lies precisely in its current vagueness. The model's ability to encompass various kinds of platforms in a hypothetical fiduciary relationship translates into the possibility of fiduciary responsibilities that differ from one kind of platform to the next. While it is odd to imagine an information fiduciary model for Marta Zuckerberg and the companies she represents, the information fiduciary model is on the rise because it targets business

---

[60]Khan, L. M., & Pozen, D. E. (2019). A skeptical view of information fiduciaries. *Harvard Law Review*, *133*(2), 497-541, see 505-510.

[61] Ibid. 514.

models that are problematic to begin with. Why try to fit Marta Zukerberg into the information fiduciary model? Doing so would effectively be to subscribe to the idea that privacy protections are an undue burden on platforms. If Marta Zuckerberg does not fit neatly into the information fiduciary model and would have to dramatically change its operations in this new legal regime, then so be it. Information fiduciaries center the user over the company, offering an excellent vehicle for reversing the damaging legal developments of the 1970s. Through the information fiduciary model, the architecture of the information economy can be restructured and repurposed to prevent invasion of privacy by design and create a system that is at once less exploitative and more transparent.

In conclusion, mass data collection and the information economy pose a real challenge to the privacy, autonomy, and security of the billions of people who use the internet and digital technologies on a daily basis. Despite the lack of a federal data privacy policy, the information economy does not exist in a lawless space but rather in a legal environment designed to facilitate data extraction and commodification and shield the platforms that engage in these commercial practices from legal scrutiny. A legal approach to protecting privacy through the propertization of data would operate as a continuation of this legacy, entrenching data extraction and invasion of privacy as an inevitable part of the user experience. The information fiduciary model offers a promising alternative. While it is still a developing model, at its core it challenges the extractive architecture with which platforms exploit and commodify their users by asking whether platforms fail to uphold fiduciary responsibilities. In just a few decades, technology has

developed to such an extent that data commodification seems a permanent fixture of digital life, but it is never too late to begin asking whether platforms are serving users' best interests.