Loyola of Los Angeles Law Review

Volume 54 | Number 1 Article 4

Fall 11-1-2020

Forging a Path Towards Meaningful Digital Privacy: Data Monetization and the CCPA

Rebecca Harris

Forging a Path Towards Meaningful Digital Privacy: Data Monetization and the CCPA

Cover Page Footnote

J.D. Candidate, May 2021, Loyola Law School, Los Angeles; B.S., Biology, University of California, Santa Cruz, June 2011. Many thanks to Professor John T. Nockleby for his guidance and advice. Thanks also to the editors and staff of the Loyola of Los Angeles Law Review for their endless support and for always inspiring me to reach higher. Lastly, thanks to my parents, John and Joanne Harris, to whom I owe it all.

FORGING A PATH TOWARDS MEANINGFUL DIGITAL PRIVACY: DATA MONETIZATION AND THE CCPA

*Rebecca Harris**

The California Consumer Privacy Act (CCPA) was passed in response to a number of newsworthy data breaches with widespread impacts, and which revealed how little digital privacy consumers actually have. Despite the large market for consumer data, individual consumers generally do not earn money when their personal data are sold. Further, consumers have very little control over who collects their data, what information is collected, and with whom it is shared. To place control back in the hands of the consumer, affirmative consent should be required to collect and sell consumer's data, and consumers should have the ability to sell these data themselves.

The CCPA provides a mechanism for consumers to monetize their own data, but it does not go far enough. The CCPA allows consumers to "opt-out" of sharing their data, but an "opt-in" framework would offer increased privacy and greater incentives for companies to pay consumers for their data. Despite these and many other issues, the CCPA represents a step towards improved digital privacy. However, it remains to be seen whether the CCPA will result in any meaningful change to consumer data monetization and digital privacy protection more broadly.

* J.D. Candidate, May 2021, Loyola Law School, Los Angeles; B.S., Biology, University of California, Santa Cruz, June 2011. Many thanks to Professor John T. Nockleby for his guidance and advice. Thanks also to the editors and staff of the *Loyola of Los Angeles Law Review* for their endless support and for always inspiring me to reach higher. Lastly, thanks to my parents, John and Joanne Harris, to whom I owe it all.

TABLE OF CONTENTS

I. INTRODUCTION

Everyday interactions with technology generate valuable consumer data, which are sold to be used in advertising, analytics, and for many other purposes. The demand for consumer data has driven the growth of the data economy, which in 2018, had an estimated value exceeding $200 billion.[1] Although consumer data drive the data economy, under the current infrastructure, individual users neither earn money from the data they generate, nor do they have meaningful control over how their data are used.[2] Further, those companies that collect and profit from consumer data often fail to exercise even the most basic cybersecurity measures that are necessary to keep consumer data safe.[3] As a result, consumer information is often poorly protected, even though it is a valuable commodity. These issues raise the question of whether consumers should be the ones profiting from the data they generate and whether this would improve or weaken consumer data privacy.

Before 2020, California consumers had little, if any, means to direct companies not to collect and sell their personal data.[4] Further, since there were very few avenues for consumers to sell their personal data, there was virtually no way for individual consumers to personally profit from the data marketplace. A new California law has the potential to address these issues—the California Consumer Privacy Act (CCPA) provides a mechanism for consumers to exercise greater control over how their data are used and, potentially, may even offer an avenue for consumers to monetize their own data.[5]

The CCPA came into effect on January 1, 2020, and became the first major data privacy law in the United States.[6] The CCPA was first

1. Florian Gröne et al., *Tomorrow's Data Heroes*, STRATEGY & BUS. (Feb. 19, 2019), https://www.strategy-business.com/article/Tomorrows-Data-Heroes.

2. *Id.*

3. *See, e.g.*, Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017, 1:27 PM), https://www.wired.com/story/equifax-breach-no-excuse/ (reporting that hackers exploited a known vulnerability in Equifax's systems because the company failed to patch and update its software, despite Equifax's awareness of its security weakness).

4. Geoffrey A. Fowler, *Don't Sell My Data! We Finally Have a Law for That*, WASH. POST (Feb. 19, 2020), https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/?arc404=true.

5. Joshua Gutter, *Show Me the Money: How the CCPA Provides a Mechanism for Consumers to Monetize Their Personal Data*, JD SUPRA (Aug. 9, 2019), https://www.jdsupra.com/legalnews/show-me-the-money-how-the-ccpa-provides-94557/.

6. Dimitri Sirota, *California's New Data Privacy Law Brings U.S. Closer to GDPR*, TECHCRUNCH (Nov. 14, 2019, 11:55 AM), https://techcrunch.com/2019/11/14/californias-new-data-privacy-law-brings-u-s-closer-to-gdpr/; *see* Eric Goldman, An Introduction to the California

enacted in 2018 as a direct legislative response to the Cambridge Analytica scandal, which revealed the degree to which consumers lacked digital privacy and how little control they had over their personal data.[7] As a result, the law was aimed at empowering consumers to "take back control of [their] personal information."[8] To accomplish this, the CCPA affords consumers with new rights by regulating how consumers' data are handled.[9] One of the most important of these new regulations is that companies must allow consumers to "opt-out" of selling their data.[10] Additionally, the CCPA quietly includes an option for companies to compensate consumers by offering financial incentives to sell the consumers' data.[11]

Although the CCPA imposes narrow regulations to provide consumers with greater digital privacy, the new law is expected to create significant compliance costs for businesses, as well as broad legal liability.[12] The additional expected costs due to the CCPA arise not only from consumer data handling requirements, but also because the CCPA creates a limited private cause of action for consumers whose personal information was exposed in a data breach.[13] In light of the CCPA's expected added cost to businesses, it is not clear whether companies will actually exercise the financial incentive section of the law and compensate consumers for their data.

Additionally, even if consumers have the option to monetize their own data, this option could be overlooked because consumers are decision averse and unfamiliar with the provided framework to exercise this option. Nevertheless, because the CCPA provides a mechanism for consumers to sell their own data, the CCPA necessarily affords consumers with some ownership and control over their data and how that data are used.[14] However, there is a possibility that such a structure, compensating consumers for their data, could actually

---

Consumer Privacy Act (CCPA) 1 (July 1, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013 (excerpted chapter from ERIC GOLDMAN, INTERNET LAW CASES & MATERIALS (2019 ed.)) (last updated July 7, 2020) [hereinafter Goldman, An Introduction to the CCPA].

7. S. JUDICIARY COMM., ANALYSIS OF ASSEMBLY BILL NO. 375, 2017–2018 Reg. Sess., at 1 (Cal. 2018).

8. *Id.* at 3.

9. *Id.* at 8–14.

10. *Id.* at 17.

11. CAL. CIV. CODE 1798.125(2)(b)(1) (Deering 2020); *see id.* § 1798.120.

12. Goldman, An Introduction to the CCPA, *supra* note 6, at 6.

13. *Id.*; CAL. CIV. CODE § 1798.150(b).

14. *See* CAL. CIV. CODE § 1798.125(2)(b)(1).

decrease consumer privacy and potentially frustrate the CCPA's overarching goals.[15]

This Note seeks to address the many uncertainties created by the CCPA and will explore the new law's potential impacts, including how it might lay the foundation for a dramatic change in the market for consumer data. Part I discusses the current state of data privacy, including the value of consumer data, data breaches, and a survey of existing privacy law in the United States and in Europe. Part I also introduces the CCPA and how it fits into the greater landscape of data privacy. Part II describes data monetization, how it may be performed, and how the CCPA creates a framework for consumer data monetization. This Part also details potential concerns with consumer data monetization, as well as the CCPA's general weaknesses. Part III will briefly conclude by proposing how the CCPA could be improved to both better facilitate consumers monetizing their own data, and strengthen consumer data privacy.

II. FACTUAL BACKGROUND

A. Overview of Personal Data Privacy

The internet is so deeply integrated into people's lives that in 2019, three in ten Americans reported that they go online daily, and nearly one-third of those internet users reported they are online "almost constantly."[16] Behind Americans' hyper-connectivity lies the constant collection of user data and personal information. Yet, most internet users do not know who is collecting their personal data, how their data are being used, what their data are worth, or even how to stop sharing them with third parties.[17]

The terms "personal data," "consumer data," and "personal information" are umbrella terms that can be used interchangeably. The CCPA broadly defines personal information as "information that identifies, relates to, describes, [and] is reasonably capable of being

15. Christopher Tonetti & Cameron F. Kerry, *Should Consumers Be Able to Sell Their Own Personal Data?*, WALL ST. J. (Oct. 13, 2019, 9:00 AM), https://www.wsj.com/articles/should-consumers-be-able-to-sell-their-own-personal-data-11570971600.

16. Andrew Perrin & Madhu Kumar, *About Three-in-Ten U.S. Adults Say They Are 'Almost Constantly' Online*, PEW RSCH. CTR. (July 25, 2019), https://pewrsr.ch/2Y5pwdX (reporting that 81% of Americans go online on a daily basis).

17. Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection.

associated with . . . a particular consumer or household."[18] This definition includes specific identifiers, such as name, address, email address, social security number, internet protocol address, and more.[19] For example, the CCPA's definition of personal information captures a broad range of commercial data points, including purchasing tendencies, biometric information, internet browsing history, geolocation data, and employment-related data.[20] The broad definition of personal information makes it a catch-all term that can be used to describe essentially any information which could be derived about a person.[21] The term is so broad that personal information even includes "inferences drawn from any of the information . . . to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, [etc.]"[22]

1. Personal Data Collection and Its Value

Internet users generate immense amounts of data in their everyday interactions with technology, but they typically do not know that these data are, in fact, a valuable commodity.[23] Routine activities, such as using a search engine or posting on social media, leave behind a paper trail that reveals intimate details about the user.[24] Although these data contain private details, they are nevertheless sold or collected by data brokers, who specialize in scraping, selling, and analyzing consumer data.[25]

Data brokers gather consumer data from both public and non-public sources.[26] Public sources of data can include property records, marriage licenses, and census data.[27] In contrast, private sources of data can include information purchased directly from companies that interface with consumers.[28] Data brokers also purchase consumer data from other companies, including consumers' social media

18. CAL. CIV. CODE § 1798.140(o)(1).
19. *Id.* § 1798.140(o)(1)(A).
20. *Id.* at § 1798.140(o)(1).
21. *See id.*
22. *Id.* at § 1798.140(o)(1)(K).
23. Matsakis, *supra* note 17.
24. Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, VICE (Mar. 27, 2018, 7:00 AM), https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.
25. *Id.*
26. Matsakis, *supra* note 17.
27. Grauer, *supra* note 24.
28. Matsakis, *supra* note 17.

connections, credit card transaction data, general web browsing activity, and geolocation.[29] Given that data brokers collect consumer information from a wide range of sources, they are able to profile consumers based on their individual demographic, socioeconomic, psychographic, and physiological data.[30] Accordingly, data brokers hold vast amounts of personal, and often sensitive, information.

Data brokers then sell consumers' personal information to advertisers and retailers who analyze the data to gain deeper insight into consumer habits and to better tailor their targeted advertising to the individual consumer.[31] Although data brokers disidentify consumer records before selling them to advertisers, reidentifying an individual from an anonymized data set is relatively straightforward and easy to accomplish.[32] This fact is particularly troubling when considering anonymized location data sets and the vast amount of geolocation data that are collected from consumers. Identifying an individual based on raw, anonymized location data can be quickly achieved by first looking to where an individual device spent the night and then cross-referencing this location with public records to reveal the registered occupant of that home.[33] Accordingly, data brokers are not able to fully mitigate the privacy risks of selling consumer location data, even if such data are anonymized before sold.

Despite this privacy risk, the market for location data is booming and sales for location-targeted advertising reached approximately $21 billion in 2018.[34] However, consumer data are used for more than just targeted advertising—retailers use location data to understand where consumers have been, where they are going, and to influence what consumers do next.[35] Financial firms are even able to use these location data to inform their investment decisions.[36] For example,

29. *Id.*

30. Anne Logsdon Smith, *Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data*, 27 CATH. U. J.L. & TECH. 187, 197 (2018).

31. Jennifer Valentino-DeVries et al., *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.

32. Sophie Bushwick, *"Anonymous" Data Won't Protect Your Identity*, SCI. AM. (July 23, 2019), https://www.scientificamerican.com/article/anonymous-data-wont-protect-your-identity/.

33. Valentino-DeVries et al., *supra* note 31.

34. *Id.*

35. *Id.*

36. *Id.*

location data can provide real-time insights into consumer behavior and show whether customers are visiting a particular retailer's stores.[37]

Although an entire industry was created from selling consumers' personal information, these consumers are largely left out of the data economy. Consumers' data are collected and sold without their knowledge or consent, and generally, consumers have no say in how their data are used or handled. Further, consumers are not paid when their personal information is sold. However, the sale of such data does return some non-monetary value to consumers in the form of free services.

This exchange—data for services—resulted from an expectation built by Silicon Valley that digital services should be free.[38] To monetize free services, companies, such as Google and Facebook, collect and sell consumers' personal information for use in targeted advertising.[39] Consumers do receive a benefit from this exchange because advertising sales allow these companies to provide free services, such as search, email, and social media platforms. Additionally, traditional advertising sales, as well as selling consumer data for use in targeted or "behavioral" advertising, fund much of the press and other channels of expression, which are struggling to survive in today's economy.[40]

In 2018, companies generated approximately $178 billion in revenue from collecting and selling their users' data to enable targeted advertising.[41] However, beyond the use of free services, few users earned any money from the sale of their personal information.[42] Additionally, large-scale leaks and hacks have exposed rampant privacy abuses—highlighting that the custodians of consumer data often fail to adequately secure these data, even though they earn money from selling them to data brokers and advertisers.[43] These

37. *Id.*

38. Imanol Arrieta-Ibarra et al., *Should We Treat Data as Labor? Moving Beyond "Free"*, 108 AM. ECON. 38, 40–41 (2018).

39. *Id.* at 41.

40. Jordan Abbott, *Time to Build a National Data Broker Registry*, N.Y. TIMES (Sept. 13, 2019), https://www.nytimes.com/2019/09/13/opinion/data-broker-registry-privacy.html.

41. Gröne et al., *supra* note 1.

42. Gregory Barber, *I Sold My Data for Crypto. Here's How Much I Made*, WIRED (Dec. 17, 2018, 6:00 AM), https://www.wired.com/story/i-sold-my-data-for-crypto/ (noting that a data marketplace app, which enables consumers to sell their data, only had 5,500 sellers).

43. Kari Paul, *Americans' Data Is Worth Billions—and You Soon Might Be Able to Get a Cut of It*, MARKETWATCH (Oct. 9, 2018, 3:05 PM), https://www.marketwatch.com/story/americans-data-is-worth-billions-and-you-soon-might-be-able-to-get-a-cut-of-it-2018-10-09.

privacy issues raise the question of whether consumers would achieve greater digital privacy if they owned their own data, with the ability to sell or restrict their use as they see fit.[44]

2. Overview of Data Breaches

Consumers are particularly vulnerable to security breaches due to the immense volume of personal data that are collected and held by companies.[45] Data breaches are the inadvertent or unauthorized exposure of an organization's sensitive information.[46] Sensitive information can include the personally identifying details of that organization's customers or users, such as customers' social security number, date of birth, or financial account information.[47] These data can be misused in a number of ways: to file a fraudulent tax return; to fraudulently redirect a beneficiary's direct deposit benefits; to apply for employment; or to rent a home and more.[48] However, one of the most common misuses of personal information is financial fraud in the form of identity theft.[49]

New-account fraud is a type of identity theft that occurs when a fraudster uses someone else's personally identifiable information to open new financial accounts without that person's knowledge.[50] However, existing-account fraud is the more frequent type of identity theft and it involves unauthorized charges or withdrawals of money.[51] Identity theft, both as existing and new-account fraud, can continue for years following a breach because many pieces of identifying

44. Tonetti & Kerry, *supra* note 15.

45. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-230, DATA BREACHES: RANGE OF CONSUMER RISKS HIGHLIGHTS LIMITATIONS OF IDENTITY THEFT SERVICES 1 (2019) [hereinafter DATA BREACHES REPORT].

46. *Id.* at 1 n.1.

47. *Id.* at 1.

48. *Id.* at 4–5.

49. FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK 4 (2020), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf [hereinafter CONSUMER SENTINEL NETWORK REPORT].

50. DATA BREACHES REPORT, *supra* note 45, at 5.

51. *Id.*; CONSUMER SENTINEL NETWORK REPORT, *supra* note 49, at 4 ("Credit card fraud tops the list of identity theft reports in 2019. The FTC received more than 271,000 reports from people who said their information was misused on an existing account or to open a new credit card account.").

information, such as social security numbers, cannot be changed and thus can be used repeatedly.[52]

a. Frequency and consumer impacts

Due to a number of massive and highly publicized data breaches, consumers are more aware of data privacy than ever before.[53] In 2019, the Pew Research Center reported that approximately 30 percent of Americans had experienced a data breach in the past twelve months.[54] Most Americans also reported concern over how their personal information is collected and used by companies, likely in part due to high frequency and wide reach of data breaches.[55] Additionally, these data breaches have caused consumers to lose confidence in an institution's ability to protect their data, and in 2019, most Americans reported that they believed their personal information was less secure than it was five years prior.[56]

It is not surprising that Americans lack confidence in their digital privacy. Given the depth of sensitive information that companies collect, consumers are especially vulnerable to identity theft when companies fail to adequately secure these data and are hacked as a result.[57] For example, in 2017, the behemoth credit reporting agency, Equifax, announced that a breach of their database exposed the personal data of 143 million American consumers.[58] Equifax has access to the personal financial data of nearly every American adult because it is one of the three main agencies that calculate consumers' credit scores.[59] As a result of this breach, hackers were able to access

52. KAMALA D. HARRIS, ATT'Y GEN., CAL. DEP'T OF JUST., CALIFORNIA DATA BREACH REPORT 2012–2015 at 15–16 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

53. BROOKE AUXIER ET AL., PEW RSCH. CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED, AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 15, 17 (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf [PEW RSCH. CTR. REPORT].

54. *Id.* at 18.

55. *Id.* at 20.

56. *Id.* at 15.

57. Rani Molla, *Why Your Free Software Is Never Free*, VOX (Jan. 29, 2020, 12:00 PM), https://www.vox.com/recode/2020/1/29/21111848/free-software-privacy-alternative-data.

58. Lily Hay Newman, *How to Protect Yourself from That Massive Equifax Breach*, WIRED (Sept. 7, 2017, 7:34 PM), https://www.wired.com/story/how-to-protect-yourself-from-that-massive-equifax-breach.

59. *Id.*

the social security numbers, birth dates, addresses, and other personal data of nearly 44 percent of the U.S. population.[60]

b. Causes

Data breaches occur in nearly every industry and, although they can be caused by sophisticated cyber-attacks, data breaches are often due to a business's failure to follow basic cybersecurity practices.[61] For example, malicious cyber-attacks were responsible for nearly half of the 1,473 data breaches in 2019.[62] Data thieves accomplished this by using malware or hacking to exploit existing security weaknesses in the targets' systems in order to gain access to sensitive consumer records.[63] However, the remainder of 2019's data breaches were not caused by hackers or malware, but rather, were due to human error and system glitches.[64]

Although system glitches and human error are not sophisticated causes of data breaches, the consequences can be just as significant as those performed by hackers.[65] For example, in May of 2019, a journalist discovered that the large real estate and title insurance firm, First American, failed to employ basic and essential security measures to secure consumer data.[66] As a result, the sensitive financial records of over 885 million consumers were accessible to anyone using the First American website.[67] This gap in security provided easy access to users' social security numbers, driver's license images, bank account numbers, mortgage and tax receipts, and more.[68] Although it is unknown whether the exposed data were accessed and used for malicious purposes, it would have been extremely easy to do so and

60. *Id.*

61. *See* HARRIS, *supra* note 52, at iii, 28; Newman, *Equifax Officially Has No Excuse*, *supra* note 3.

62. *Identity Theft Resource Center's Annual End-of-Year Data Breach Report Reveals 17 Percent Increase in Breaches over 2018*, IDENTITY THEFT RES. CTR.: BLOG—LATEST NEWS (Jan. 28, 2020), https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/; Larry Ponemon, *What's New in the 2019 Cost of a Data Breach Report*, SEC. INTEL. (July 23, 2019), https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/.

63. *See* HARRIS, *supra* note 52, at iii.

64. Ponemon, *supra* note 62.

65. *Id. See generally* HARRIS, *supra* note 52, at 10, 38 (discussing sophisticated cyber criminals as the perpetrators of malware and hacking).

66. *See* Lily Hay Newman, *The Biggest Cybersecurity Crises of 2019 So Far*, WIRED (July 5, 2019, 7:00 AM), https://www.wired.com/story/biggest-cybersecurity-crises-2019-so-far/.

67. *Id.*

68. *Id.*

provided open-access to all of the information necessary to commit identity theft and fraud.[69]

Regardless of root cause, most data breaches were relatively preventable.[70] This is because companies frequently employ weak or insecure software and utilize insufficient access controls.[71] A company's failure to update its software on a regular basis can seriously compromise cybersecurity because updates are often issued to patch security vulnerabilities.[72] Such careless information technology practices have serious consequences.[73] Equifax, for example, had known for months that a software update was required to patch a security vulnerability, but nevertheless failed to take this simple, but necessary, step to bolster its security.[74] As a result, the company left millions of individuals' data exposed for hackers to access.[75]

c. Loss following a breach

Although some sensitive information, such as passwords, can be updated once accessed in a breach, many forms of personally identifying information, such as social security numbers, are not as easily altered.[76] Consequently, attackers typically use exposed information right away because credit card information can be changed soon after a breach.[77] As a result, personally identifying information that cannot be quickly changed is essentially a ticking

69. *Id.*

70. *See generally* ONLINE TR. ALL., 2018 CYBER INCIDENT & BREACH TRENDS REPORT 3 (2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf (95% of 2018 breaches could have been prevented).

71. *See FAQs*, HAVEIBEENPWNED.COM, https://haveibeenpwned.com/FAQs (last visited Oct. 4, 2020) (Have I Been Pwned aggregates data from large data breaches, allowing individuals to determine whether their email address and sensitive personal information were released in the breach). *See generally* Charlie Warzel, *How to Take Back Control from Facebook*, N.Y. TIMES (Apr. 30, 2019, 8:02 PM), https://www.nytimes.com/2019/04/30/opinion/facebook-ftc-privacy.html.

72. *See* Mike Hamilton, *Why Software Patches Don't Fix Everything*, FORBES (Aug. 6, 2019, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2019/08/06/why-software-patches-dont-fix-everything/#1db0a8b727d5.

73. *Id.*

74. *Id.*

75. *Id.*

76. HARRIS, *supra* note 52, at 15–16.

77. *See* Tom Groenfeldt, *Credit Card Fraud Is Down, but Account Fraud That Directly Hurts Consumers Remains High*, FORBES (Mar. 18, 2019, 8:05 AM), https://www.forbes.com/sites/tomgroenfeldt/2019/03/18/credit-card-fraud-is-down-but-account-fraud-which-directly-hurts-consumers-remains-high/#493dc7820bfc.

time bomb. This is because account information is often placed for sale on the dark web soon after it is stolen in a breach and as a result, is available for criminals to use long after the initial breach.[78]

After consumers' personally identifying information is breached, fraudsters can easily locate all of the required information to perform new-account identity theft.[79] Additionally, fraudsters do not face significant barriers to committing identity theft because most organizations maintain basic, if not remedial, methods of verifying identity.[80] The extent of most identity verification involves reviewing just name, address, date of birth, and social security number—information which can be quickly obtained once a consumer's personal information has been breached.[81]

Additionally, most merchants rely on just a username and password to access accounts or to make online purchases and do not require any multi-factor authentication.[82] Data breaches often result in the release of credential lists, which are collections of email addresses and passwords.[83] Without multi-factor authentication, all fraudsters require is the information contained in credential lists, and, as a result, consumers are at a greater risk of having their accounts improperly accessed.[84] If the breached company did not strongly encrypt user credentials, criminals can fairly easily crack credential lists to pair the email address to its plain text password.[85] Criminals then take these password lists from breached merchants and test them against a different merchant to see if the password still provides criminals access to the consumer's account.[86] Thus, multi-factor authentication is important to preventing identity theft because a criminal can access

78. Kate O'Flaherty, *Another 127 Million Records Have Gone on Sale on the Dark Web—Here's What You Should Do*, FORBES (Feb. 15, 2019, 7:50 AM), https://www.forbes.com/sites/kateoflahertyuk/2019/02/15/another-127-million-records-have-gone-on-sale-on-the-dark-web-heres-what-you-should-do/#7e86e1612293.

79. Groenfeldt, *supra* note 77.

80. *See id.*

81. *Id.*

82. *Id.*

83. Troy Hunt, *Password Reuse, Credential Stuffing and Another Billion Records in Have I Been Pwned*, TROYHUNT.COM (May 5, 2017), https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned.

84. *See id.*

85. *See id.*

86. Groenfeldt, *supra* note 77.

accounts using credential lists obtained from a data breach, especially if users do not use unique passwords for each merchant website.[87]

Although identity theft and fraud are exceedingly prevalent, consumers do have some limited protections for when their data are breached.[88] Financial institutions frequently offer services such as real-time account notification[89] and implement "zero-fraud liability" policies.[90] Additionally, laws limiting consumer liability for existing-account fraud mitigate much of the harm that victims of identity theft face.[91] Nevertheless, non-reimbursable transactions and secondary fees, such as overdraft penalties, still place victims of identity theft at risk of a significant financial loss.[92]

However, identity theft causes more than financial loss.[93] The exposure of personally identifying information can result in significant amounts of lost time, emotional distress, and reputational harm.[94] This is because stolen data are often sold and then not used until long after the initial breach.[95] Accordingly, even if victims of data breaches do not suffer an immediate financial injury, the increased risk of identity theft results in victim's suffering opportunity costs due to time spent mitigating their potential harms.[96]

B. Existing Data Privacy Legislation and Enforcement

Technology has created a moving target for privacy law in California and the United States in general. Although there are some legal protections for citizens' personal information in very specific contexts, personal data are not considered an economic asset and thus, few protections exist.[97] Despite the large market for consumer data and the depth of information that companies collect on consumers, consumers do not *own* their own data.[98] Further, because the United

87. *Id.*
88. *See id.*
89. *See id.*
90. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 775 (2018).
91. DATA BREACHES REPORT, *supra* note 45, at 5 n.11.
92. GIACT, The Changing Landscape of Identity Fraud 3 (2019) (unpublished paper).
93. DATA BREACHES REPORT, *supra* note 45, at 6.
94. *Id.*
95. Solove & Citron, *supra* note 90, at 757.
96. *Id.* at 758–59.
97. *See* Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construction for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 227 (2018).
98. *Id.* at 246.

States lacks meaningful digital privacy legislation that provides consumers with agency and control over their own data, existing laws do not establish a framework that could viably support consumers monetizing their own data.

1. Federal Protections

a. Statutory protections

Prior to the enactment of the CCPA, the United States lacked comprehensive data privacy legislation, and because of this, "privacy law in the wider U.S. remain[ed] a complex patchwork of narrowly tailored federal and state laws."[99] U.S. federal privacy law focuses only on specific types of data, specific industries, or specific modes of transmitting such data.[100] The resulting body of commercial privacy law is rife with gaps and ultimately fails to provide meaningful checks on the collection and sale of consumer data.

Data-specific privacy laws include the Fair Credit Reporting Act (FCRA) and the Health Information Portability and Accountability Act (HIPAA).[101] The FRCA protects consumer credit information and limits the ways in which third parties may use this information.[102] HIPAA protects medical information and sets security standards, as well as standards on de-identifying protected data.[103]

A prominent industry-specific privacy law is the Gramm-Leach-Bliley Act (GLBA).[104] The GLBA is limited to the financial services industry and requires that such institutions disclose how they share and safeguard sensitive customer data.[105] Additionally, the GLBA requires that covered financial services entities secure customer data

99. Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 73 (2018).

100. *See* David A. Hyman & William E. Kovacic, *Implementing Privacy Policy: Who Should Do What?*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1117, 1128 (2019).

101. Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REGUL. 667, 676 (2017); *see also* 15 U.S.C. §§ 1681–1681x (2018) (FCRA); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26 U.S.C., 29 U.S.C., 42 U.S.C., and 45 C.F.R.).

102. Rostow, *supra* note 101, at 676; *see* 15 U.S.C. § 1681b.

103. *See* 45 C.F.R. § 164.514 (2019); Rostow, *supra* note 101, at 676–77.

104. Pardau, *supra* note 99, at 81; *see also* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

105. Pardau, *supra* note 99, at 81; *see* 15 U.S.C. § 6801 (2018); Privacy of Consumer Financial Information, 16 C.F.R. § 313 (2000).

and allow consumers to opt out of sharing their data with third parties.[106]

A significant law protecting the mode of transmitting data is the Stored Communications Act (SCA).[107] The SCA protects electronic communications by prohibiting electronic communications providers from disclosing such communications to nongovernmental third parties without consent.

Because federal privacy laws are limited in scope, third parties oftentimes use consumer data in unexpected and nonconsensual ways. For example, HIPAA does not protect user-generated health information, since it only applies to specific entities, such as hospitals or health insurance companies.[108] Accordingly, HIPAA does not protect medical information collected from a Fitbit or Apple Watch, since these data are generated by the user, rather than a medical provider, and are thus not subject to HIPAA protections.[109] Similarly, the SCA does not protect location data collected from cell phones, even though the SCA protects communications made from those same devices.[110] Further, the SCA does not cover posts or comments made on social media, despite these being a form of electronic communication.[111] Thus, this "patchwork" of federal privacy law leaves many gaps for consumers' data to be exploited.

b. Agency protections

The Federal Trade Commission (FTC) serves as the primary authority to regulate privacy and data security, but without any comprehensive federal privacy laws, its enforcement authority is limited.[112] Nevertheless, the FTC has a broad regulatory scope that

106. Rostow, *supra* note 101, at 677.

107. *See* 18 U.S.C. § 2701 (2018).

108. Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 788 (2016); 45 C.F.R. § 160.103(4)(iv).

109. Lipman, *supra* note 108, at 788.

110. *See generally* 18 U.S.C. § 2701; Valentino-DeVries et al., *supra* note 31 ("There is no federal law limiting the collection or use of [location] data.").

111. Rostow, *supra* note 101, at 678.

112. *See* Lipman, *supra* note 108, at 789, 792; *see also* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2231, 2236, 2273 (2015) ("The FTC's endorsement of a diluted version of [Fair Information Practices] is one reason that the Commission is not a good candidate to serve a larger role in privacy policy. The Commission's privacy vision is too limited." (alteration in original) (quoting Robert Gellman, *A Better Way to Approach Privacy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183, 1205 (2003)).

covers most industries that involve consumers and that handle consumers' personal data.[113] The FTC derives its authority from section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices."[114] Further, the legislative history of section 5 indicates an intent that the FTC's authority be evolutionary and wide-reaching,[115] which allows the agency to respond to cybercrime's constantly changing nature.

However, the FTC's authority is hindered by a number of judicial carve-outs, such as exemptions for banks, common carriers, and not-for-profit institutions.[116] These exemptions were created by Congress in 1914, before digital privacy was ever a concern. Although the FTC is a powerful agency, it has a limited ability to address such privacy concerns.[117] This is because the FTC regulates relationships between companies and the consumers with whom they interact.[118] Since third-party aggregators do not directly interact with consumers, they lack opportunity to deceive consumers, and thus are not subject to FTC regulation.[119] Additionally, there is also the risk that large, institutional companies may ignore FTC guidelines by flagrantly handling consumer data because they consider FTC fines to be simply the cost of doing business.[120]

2. Existing California Privacy Law

California has long been an established leader in online privacy and has passed legislation with nationwide impact.[121] For example, in 2003, California became the first state to enact a data breach notification law.[122] This law served as a model for the forty-six other states that have since enacted similar data breach notification laws.[123]

113. *See* Hartzog & Solove, *supra* note 112, at 2236.
114. 15 U.S.C. § 45(a)(2) (2018); Lipman, *supra* note 108, at 789.
115. Hartzog & Solove, *supra* note 112, at 2246.
116. *Id.* at 2236, 2289.
117. *See* Lipman, *supra* note 108, at 792.
118. *Id.* at 792–93.
119. *Id.* at 793.
120. *See* Emily Stewart, *A $5 Billion Fine from the FTC Is Huge—Unless You're Facebook*, VOX (Apr. 25, 2019, 2:20 PM), https://www.vox.com/2019/4/25/18516301/facebook-earnings-ftc-fine-mark-zuckerberg-stock.
121. Lipman, *supra* note 108, at 793; CAL. BUS. & PROF. CODE § 22575(a) (Deering 2020) (requiring that any website that collects personally identifiable information post a privacy policy on its website. Because this law applies to any website accessible to Californians, it effectively requires that any U.S. website post a privacy policy).
122. HARRIS, *supra* note 52, at 1, app. C.
123. *Id.*

Nevertheless, gaps in California law remain because, even though California has more than one hundred different privacy laws, the focus of these laws is limited to content, potential victims, and modality.[124]

3. European Union General Data Protection Regulation

In contrast to the United States, the European Union enacted a comprehensive privacy law in 2018—the General Data Protection Regulation (GDPR).[125] The GDPR considers individual privacy protection to be a basic human right, and, at the time it was enacted, the GDPR was the world's toughest data privacy law.[126] The GDPR allows citizens to request access to their online data and restricts how businesses can obtain and handle such data.[127] Further, the GDPR affords European citizens with the "Right to erasure" or the "right to be forgotten,"[128] meaning that individuals can demand that companies delete their personal data.[129]

The GDPR's scope is not limited to European businesses and applies to any "controller or processor" of personal data that offers goods or services to data subjects in the European Union, regardless of where the processing takes place.[130] This world-wide scope also encompasses businesses that monitor the behavior of Europeans, so long as the behavior takes place within the Union.[131] The wide-reaching GDPR served as the model for legislators when drafting the CCPA.[132]

---

124. Pardau, *supra* note 99, at 88–89.

125. *Id.* at 83–85; Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018),https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer; *see also* 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 [hereinafter GDPR].

126. Tony Raval, *Data Privacy as a Basic Human Right*, FORBES (Nov. 12, 2019, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2019/11/12/data-privacy-as-a-basic-human-right/?sh=cdd8b574cbf3.

127. Satariano, *supra* note 125.

128. GDPR, *supra* note 125, art. 17, at 43–44.

129. Satariano, *supra* note 125.

130. GDPR, *supra* note 125, art. 3, at 32–33.

131. *Id.*

132. Erin Winick, *California's New Online Privacy Law Could Be Huge for the US*, MIT TECH. REV. (June 29, 2018), https://www.technologyreview.com/f/611570/californias-new-online-privacy-law-could-be-huge-for-the-us/.

C. California Consumer Privacy Act

The CCPA has the potential to not only strengthen digital privacy rights—it may also change the marketplace for consumer data. The CCPA's purpose is to provide consumers with greater control over their personal information. This purpose reflects a critical step towards creating a framework in which consumer data have tangible monetary value, and a system where consumers have the ability to actually profit from their own personal data.[133] Despite these possibilities, the law contains a number of significant issues that could inhibit its potential impacts on digital privacy rights and data ownership. Even with these issues, the CCPA creates new consumer rights and could ultimately lead the way towards improved digital privacy.

1. History of the CCPA

a. Ballot initiative

In early 2018, the Californians for Consumer Privacy group garnered more than six hundred thousand signatures to support their proposed new privacy law, the Consumer Right to Privacy Act of 2018.[134] This group was founded by a Bay Area real estate developer, who was concerned about data privacy and spent approximately $3 million of his own money to fund the Californians for Consumer Privacy ballot initiative.[135] California lawmakers did not want to risk voters passing that ballot initiative because, once passed into law, it would be extremely difficult for the legislature to change it.[136] This is because, once a ballot initiative is passed into law, amendments may only be made through additional ballot initiatives.[137] In a rushed effort to prevent the initiative from making it to the November ballot,

133. S. JUDICIARY COMM., ANALYSIS OF ASSEMBLY BILL NO. 375, 2017–2018 Reg. Sess., at 18–19 (Cal. 2018).

134. Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/.

135. Goldman, An Introduction to the CCPA, *supra* note 6, at 1.

136. Kristen J. Mathews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER ROSE LLP: PRIV. L. BLOG (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

137. *Id.*

California lawmakers unanimously passed a substitute bill, the California Consumer Privacy Act of 2018 (AB 375).[138]

b. Legislative history and intent

The legislative history of the CCPA notes that "[t]he world's most valuable resource is no longer oil, but data."[139] The Senate Judiciary Committee for the CCPA realized the value of data after the Cambridge Analytica scandal, which was the impetus for passing the law.[140] The Cambridge Analytica scandal revealed that a political consulting firm had harvested data on fifty million Facebook users, without those users' knowledge or consent.[141] Aside from the political implications of that scandal, it exposed technology companies' widespread collection of user data and raised the public's awareness of consumer privacy.[142]

In addition to the Cambridge Analytica scandal, the growing public demand for online privacy was also stoked by "surreptitious surveillance" of civilians.[143] As of 2019, most Americans felt that it was impossible to "go through daily life without being tracked" or having their data collected.[144] With the Internet of Things (IoT)[145] becoming a greater part of daily life, technology manufacturers and service providers are able to track, store, and sell data covering a wide variety of formerly private consumer behavior.[146] IoT products create "a network of connected devices" and include items such as "smart" thermostats, security cameras, internet-enabled washing machines, and more.[147] Further, in 2019, most Americans reported feeling that they have little to no control over how companies use their personal

138. John Stephens, *California Consumer Privacy Act*, A.B.A. (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/; Lapowsky, *supra* note 134.

139. S. JUDICIARY COMM., ANALYSIS OF ASSEMBLY BILL NO. 375, 2017–2018 Reg. Sess., at 1 (Cal. 2018).

140. *Id.*

141. Issie Lapowsky, *Cambridge Analytica Took 50M Facebook Users' Data—and Both Companies Owe Answers*, WIRED (Mar. 17, 2018), https://www.wired.com/story/cambridge-analytica-50m-facebook-users-data/.

142. ANALYSIS OF ASSEMBLY BILL NO. 375, at 1.

143. *Id.*; Lapowsky, *supra* note 134.

144. PEW RSCH. CTR. REPORT, *supra* note 53, at 2.

145. Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1372 (2017).

146. *Id.* at 1372–73.

147. *Id.* at 1372.

information.[148] The CCPA was a direct response to these concerns and was intended to provide consumers with new privacy rights, so that they can to take back control over their personal information.[149]

2. New Consumer Rights

The CCPA affords consumers new statutory rights to control their personal information, and in 2020, it is considered the toughest data privacy law in the United States.[150] New consumer rights under the CCPA fit primarily within three main categories: the right to know; the right to delete; and the right to opt out.[151] First, under the "right to know," consumers may request that a business disclose details about what personal information is collected—specifically, what categories of personal information, what sources were used to collect the information, for what purpose, and with whom the information is shared.[152] Second, under the "right to delete," businesses must delete any personal information collected from that consumer upon a verified consumer request.[153] Third, under the "right to opt-out," consumers have the right to direct a business not to sell their personal information.[154] Additionally, businesses must notify consumers of this right by including a "Do Not Sell My Personal Information" link on their homepage.[155]

Further, the CCPA offers a potential mechanism for consumers to make money from selling their personal data. Under section 1798.125, the financial incentive section of the CCPA, consumers can actually participate in the sale of their own data because a "business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information."[156]

148. PEW RSCH. CTR. REPORT, *supra* note 53, at 2.

149. *See* Lapowsky, *supra* note 134.

150. *E.g.*, Stephens, *supra* note 138.

151. *See* Fact Sheet, Att'y Gen., Cal. Dep't of Just., California Consumer Privacy Act (CCPA): Fact Sheet 1 (Oct. 10, 2019), https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf (also including the right to non-discrimination, which prohibits companies from discriminating against consumers that exercise their right to opt-out).

152. CAL. CIV. CODE § 1798.110(a) (Deering 2020).

153. *Id.* § 1798.105(a).

154. *Id.* § 1798.120(a).

155. *Id.* §§ 1798.135, .120.

156. *Id.* § 1798.125(b)(1); Assemb. B. 1355, 2019–2020 Reg. Sess. (Cal. 2019).

In addition to these new rights, the CCPA creates a private right of action, by which consumers can seek damages if their personal information is exposed due to a business's failure to "implement and maintain reasonable security procedures and practices."[157] However, prior to bringing suit for statutory damages, a consumer must first notify the business in writing of the violation and provide for a thirty-day cure period.[158]

3. Business Obligations

The CCPA imposes new obligations upon any company doing business in California that collects consumer information and that meets any one of the following requirements: (1) company's gross annual revenues are greater than $25 million; or (2) if the company "annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices"; or (3) if 50 percent or greater of company's annual revenues are derived from selling consumers' personal information.[159] Although the CCPA was born from internet-based data breaches, it applies equally to both online and offline businesses.[160] The CCPA is so wide-reaching that essentially all businesses will fall within its regulation.[161] Although not all businesses generate annual revenues greater than $25 million, most businesses, even small business, receive the personal information of more than 50 thousand consumers.[162] This is a low threshold, since a business would only need to process 137 unique credit card sales per day in order to receive the personal information of 50 thousand consumers annually.[163]

The CCPA's expansive application is the source of much criticism because it will likely impact small businesses disproportionately, even though the law was intended to address the abusive privacy practices of large technology companies, such as Facebook and Google.[164] The California Department of Justice's

157. CAL. CIV. CODE § 1798.150(a)(1).
158. *Id.* § 1798.150(b).
159. *Id.* § 1798.140(c)(1).
160. *Id.* § 1798.145; Goldman, An Introduction to the CCPA, *supra* note 6, at 2.
161. *See* Goldman, An Introduction to the CCPA, *supra* note 6, at 2.
162. *Id.*
163. *Id.*
164. Eric Goldman, *The California Consumer Privacy Act Should Be Condemned, Not Celebrated (Cross-Post)*, TECH. & MKTG. L. BLOG (Aug. 9, 2018),

Standardized Regulatory Impact Assessment estimated that CCPA compliance costs will range between $467 million and almost $16.5 billion between 2020 and 2030.[165] These initial compliance costs are primarily attributable to operational costs required to establish compliance plans, and costs to develop technological systems that respond to the CCPA and consumer requests to delete or stop selling their personal information.[166]

Smaller companies, with fewer than twenty employees, are expected to incur $50,000 in initial compliance costs, not including any costs associated with anticipated litigation.[167] Companies with more than 500 employees are expected to incur an initial cost of $2 million.[168] However, large technology companies are likely better equipped to handle the cost of CCPA compliance and anticipated litigation, whereas small businesses may not be able to shoulder such costs.[169] As a result, small businesses may be required to either stop offering "free" services or find other ways to pass along compliance costs.[170]

Further, the CCPA contains a number of issues and unclear definitions that could be exploited and ultimately undermine the law's overall purpose. For example, Facebook publicly stated in 2019 that it will not need to change its web-tracking services to comply with the CCPA since it does not fit the definition of "selling" data.[171] The CCPA's definition of "sell" contains an exception for when personal information is shared with a third-party "service provider" and is "necessary to perform a business purpose."[172] Facebook's web tracker, Pixel, tracks users' activity across the internet and then utilizes these

---

https://blog.ericgoldman.org/archives/2018/08/the-california-consumer-privacy-act-should-be-condemned-not-celebrated-cross-post.htm.

165. DAVID ROLAND-HOLST ET AL., BERKELEY ECON. ADVISING & RSCH., LLC, STANDARDIZED REGULATORY IMPACT ASSESSMENT: CALIFORNIA CONSUMER PRIVACY ACT OF 2018 REGULATIONS 8 (2019), http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

166. *Id.* at 24–25.

167. *Id.* at 11.

168. *Id.*

169. Goldman, *The California Consumer Privacy Act Should Be Condemned, Not Celebrated (Cross-Post)*, *supra* note 164.

170. *Id.*

171. Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019, 1:29 PM), https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345.

172. CAL. CIV. CODE § 1798.140(t)(2)(C) (Deering 2020).

data for targeted advertising.[173] Although privacy experts dispute Facebook's interpretation of the CCPA, Facebook's argument nevertheless illustrates how the CCPA's unclear definitions can be exploited by the very companies the law was directed at.[174]

III. ANALYSIS

Existing data privacy law does little to balance the scales of power, in that consumers have little control over their personal data and the companies collecting, profiting from, and holding these data, may govern the terms of this relationship as they wish.[175] Although the CCPA makes strides in data privacy, it mostly stays within the "control-based regime of 'notice and choice,'" where users are presented with long, unreadable disclosures and given the option to opt out of sharing personal data.[176] Such an arrangement imposes onerous obligations on businesses and does little to promote a mutually beneficial relationship between businesses and the consumers who provide valuable personal data.

To strengthen data privacy and reform the relationship between custodians of data and those who produce it, some legal scholars have proposed that companies who collect, analyze, and sell personal data for profit be considered "information fiduciaries."[177] Other models propose regulating data as property or even as labor.[178]

Although the CCPA does not create a framework to accommodate these proposed models, it does assign monetary value to consumer data and contains language that could facilitate compensating users for collection and sale of their data. It remains to be seen whether this feature of the CCPA will be utilized and whether it will have a material impact on consumer data privacy. Additionally, the CCPA is not clearly written and generally creates much uncertainty for businesses.

---

173. Sara Morrison, *Facebook Is Gearing Up for a Battle with California's New Data Privacy Law*, VOX (Dec. 17, 2019, 5:00 PM), https://www.vox.com/recode/2019/12/17/21024366/facebook-ccpa-pixel-web-tracker.

174. *Id.*

175. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016) (noting that "modern American privacy law encourages companies to profit in short-sighted ways by extracting as much value as possible from personal data in the short term").

176. *Id.*

177. Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 499 (2019).

178. Ritter & Mayer, *supra* note 97, at 227; Eric Posner & Glen Weyl, *Data Workers of the World, Unite!*, PROMARKET (Apr. 25, 2018), https://promarket.org/data-workers-world-unite/.

Ultimately, the CCPA's issues risk overshadowing the law's ability to facilitate consumer data monetization. The ability for consumers to profit from their own data is critical to disrupting the existing paradigm. So, despite its flaws and many issues, the CCPA is an important step towards creating a system in which consumers truly control their own data.

A. Beyond Privacy and Valuing Personal Data: Monetizing Personal Data

Public recognition concerning the large-scale collection and monetization of personal data has generated interest in policy reforms and new paradigms for data exchange.[179] Companies earn enormous amounts of money from using and selling consumer data, which were freely provided by consumers, yet these companies fail to serve as responsible custodians of such data. Additionally, consumers are not compensated for the valuable resource that they generate, nor are they paid for the near-constant surveillance that such pervasive data collection imposes.[180]

If consumers were able to earn money by selling their own data, rather than the technology companies collecting and selling it without user consent, the power dynamic of the existing digital advertising ecosystem would dramatically change. If consumers were able to control and sell their own data, they would have a vested financial interest in the protection of their personal information. For that reason, consumers would be financially invested in the safekeeping of their data. Thus, consumer data monetization could increase the stakes of data collection and incentivize companies to exercise greater security practices.

Millions of people use services such as Facebook and Google each day, generating data about their behavior that can be sold to be used in advertising and to train artificial intelligence (AI) programs.[181] Yet, consumers are not getting paid for this contribution and have very little control over its use. Further, data privacy legislation does not

179. *See* Dylan Walsh, *How Much Is Your Private Data Worth—and Who Should Own It?*, STAN. GRADUATE SCH. BUS. (Sept. 19, 2018), https://www.gsb.stanford.edu/insights/how-much-your-private-data-worth-who-should-own-it.

180. *See* Valentino-DeVries et al., *supra* note 31.

181. Eric A. Posner & E. Glen Weyl, *Want Our Personal Data? Pay for It*, WALL ST. J. (Apr. 20, 2018, 11:19 AM), https://www.wsj.com/articles/want-our-personal-data-pay-for-it-1524237577.

clarify who actually owns consumer data, even though such legislation endeavors to improve consumer digital privacy and discourage exploitative data collection practices.[182] Moreover, data privacy legislation does not outline a clear way in which consumers can earn a slice of the profits made from selling their personal data.

1. Data as Property

Proponents of granting consumers ownership over their data, with "the right to sell it or restrict its use," say that such a model would benefit society as a whole by encouraging innovation and improving digital privacy.[183] Data are different from other commodities in that data do not diminish with use and can be used by different companies or systems simultaneously.[184] For example, an individuals' personal data can be used by different companies at the same time without being depleted.[185] This quality of being "infinitely usable" makes the prospect of paying consumers for their data even more attractive.[186] Additionally, because data are an "infinitely usable" resource, consumers could be incentivized to maximize profits by sharing and selling their data more broadly, thereby improving data sets for AI and other uses.[187] Thus, granting consumers an ownership interest in their data could lead to greater societal gains.[188]

However, while consumer data possesses significant value on a mass-scale, there is the question of whether individuals would profit in a meaningful way from selling their own data. There are significant concerns with disrupting the data marketplace and how this could impact the way in which we use the internet.[189] Currently, consumers provide their data in exchange for free access to services.[190] Even if this is an imbalanced exchange, studies show that the public is generally unwilling to pay for services that they currently get for

182. Ritter & Mayer, *supra* note 97, at 226–27.
183. Tonetti & Kerry, *supra* note 15.
184. *Id.*
185. *Id.*
186. *Id.*
187. *Id.*
188. *Id.*
189. *See id.*
190. *Id.*

free.[191] Critics also note that owning data will "do little to help consumers' privacy—and may well leave them worse off."[192]

Additionally, granting consumers a property interest in their own data could create substantial difficulty for companies that use personal information for basic business purposes. For example, this "data as a property right" model could pose particular difficulty for businesses that may not even sell consumer data, but must store them for purposes such as providing customer service, complying with legal requirements, and countless other legitimate business uses.[193] Critics predict that such a marketplace would disrupt the current free flow of information and create substantial, if not insurmountable, technical and logistical costs that would likely not be worth the small amount of money that consumers could earn.[194]

Additionally, critics of the "data as property" model note that it could actually make consumer privacy worse because consumers would be incentivized to "click away rights to data in exchange for convenience, free services . . . or other motivations."[195] Critics also doubt the logistical feasibility of such a model, noting that any increases in data exchange could be easily stymied by companies that demand exclusive rights to the consumer data that they purchase.[196]

However, if an individual wishes to "click away [his or her] rights," that choice, to sell their data, should belong to the consumer.[197] Additionally, proponents of the data as property model point out that any practical difficulties of changing the data marketplace would be mitigated by innovation required to overcome these challenges.[198] Ultimately however, this model could lead to a fairer economy and distribution of income, because more individuals would have access to the same source of income—selling their own data.[199]

191. Magali Eben, *Market Definition and Free Online Services: The Prospect of Personal Data as Price*, 14 I/S: J.L. & POL'Y INFO. SOC'Y 227, 257 (2018).
192. Tonetti & Kerry, *supra* note 15.
193. *Id.*
194. *Id.*
195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.*
199. *See id.*

2. Data as Labor

The question of whether consumers should be able to control and sell their own data is not necessarily a binary inquiry. Consumers should be able to profit from their own data without destroying the entire data marketplace as we know it, while still increasing privacy and shifting towards "data dignity."[200] Rather than considering personal data a property right in all contexts, consumers could be paid when such data are used for specific, defined purposes.

For example, when users interact with the internet, payment could be required when their data are used as input for targeted advertising and when it is used "as a means of building better algorithms to target ads to others."[201] A number of startups are currently working towards accomplishing this by creating a mechanism for consumers to reclaim and secure their information, and then sell it to advertisers if they wish.[202] One program allows users to scrape their own data from third-party sources, such as from the health tracker Fitbit, anonymize these data, and then sell them to third-party advertisers.[203] Such information can be used by retailers and marketing companies to target consumers more efficiently and accurately, and match consumers with the best promotion for each particular individual.[204]

This model is more consistent with the "data as labor" theory, where consumers are encouraged to increase the quality and quantity of data.[205] The data as labor theory suggests that users or "data laborers" organize into "data labor union[s]" in order to negotiate contract terms and prices with the companies purchasing consumer data.[206] Such data unions could help to avoid potential issues seen with the "data as property" model. This is because data unions would increase consumers' bargaining power and make companies less able

200. Jaron Lanier, *You Should Get Paid for Your Data*, N.Y. TIMES (Sept. 23, 2019), https://www.nytimes.com/video/opinion/100000006678020/data-privacy-jaron-lanier-2.html (describing the concept of data dignity: "You should have the moral rights to every bit of data that exists because you exist, now and forever.").

201. Joshua Gans, *Paying for Data*, DIGITOPOLY (Sept. 23, 2019), https://digitopoly.org/2019/09/23/paying-for-data/ (discussing Jaron Lanier's video opinion piece with the *New York Times*, *Jaron Lanier Fixes the Internet*).

202. Paul, *supra* note 43.

203. *Id.*

204. *Id.*

205. Arrieta-Ibarra et al., *supra* note 38, at 38, 40, 41; Tonetti & Kerry, *supra* note 15.

206. Arrieta-Ibarra et al., *supra* note 38, at 41; Posner & Weyl, *Want Our Personal Data? Pay for It*, *supra* note 181.

to demand strict data-exchange terms, such as exclusive rights to data they purchased, which was a concern for the "data as property" model.[207] Given the interconnected objectives of the data as labor theory, this model would likely be best accomplished by utilizing decentralized networks and blockchain technology.

3. Blockchain's Role in Data Monetization

Applications that collect users' data use blockchain to store the data in an encrypted, decentralized network, only sharing such data with explicit user consent.[208] Advertisers can purchase a key to decrypt the individual's data and use these data to target specific users, either the individual user or others.[209] Such blockchain technology places greater control in the hands of consumers "by removing the middleman from facilitating transactions."[210] Accordingly, blockchain has "the potential to democratize the sharing and monetization of data and analytics" because it empowers consumers to truly control their own data.[211]

Many data marketplace startups are already using blockchain technology, which may be integral to consumers truly gaining control over their own data. Blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way."[212] Storing data in decentralized servers by using blockchain models puts consumers in control over their own data, since no single company or other individual would have sole license to it.[213] Rather, consumers literally hold the keys to unlock their personal data and thus maintain control over their use.[214] Additionally, the decentralized nature of blockchain offers improved cybersecurity and helps to ensure that user data remains confidential.[215]

---

207. Tonetti & Kerry, *supra* note 15.

208. Paul, *supra* note 43.

209. *Id.*

210. Chris Neimeth, *What Can Be Uncovered When Big Data Meets the Blockchain*, INFOWORLD (June 29, 2017, 9:27 AM), https://www.infoworld.com/article/3203748/what-can-be-uncovered-when-big-data-meets-the-blockchain.html.

211. *Id.*

212. Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV. (Jan.–Feb. 2017), https://hbr.org/2017/01/the-truth-about-blockchain.

213. Paul, *supra* note 43.

214. *Id.*

215. *See* Phillip Shaverdian, Comment, *Start with Trust: Utilizing Blockchain to Resolve the Third-Party Data Breach Problem*, 66 UCLA L. REV. 1242, 1275–76 (2019).

However, the use of blockchain technology is not entirely without issue. There is no legislation that currently regulates blockchain technology, nor are there commonly adopted standards for writing transactions in blockchain.[216] Blockchain technology could also fundamentally conflict with the CCPA, which requires that user data be deleted on request, since blockchain ledgers are immutable by nature.[217] Additionally, there is a concern regarding the scalability of blockchain, given that it is a relatively new technology.[218] Nevertheless, the cybersecurity benefits of blockchain technology and its ability to provide users with greater agency and control over their own data likely outweigh its potential issues.

B. The CCPA and Data Monetization: Facilitating Data Monetization

The CCPA is a landmark law for consumer rights and could represent a step towards disrupting the existing data-exchange model of providing data for free services.[219] Although the CCPA does not provide consumers with absolute ownership over their own data, it nevertheless provides consumers with significantly greater control over how their personal information is collected and used.[220] In doing so, the CCPA also creates a mechanism for consumers to monetize their personal information.

Unlike prior privacy legislation in the United States, the CCPA acknowledges the monetary value of user data. The CCPA does not only enable consumers to determine whether their data are sold to third parties, but it also permits companies to compensate consumers for the collection and sale of personal information.[221] It remains to be seen whether companies will actually offer financial incentives to consumers to collect and sell the consumers' personal information. Nevertheless, the CCPA is a step towards consumers having the ability

216. Peter Bendor-Samuel, *The Primary Challenge to Blockchain Technology*, FORBES (May 23, 2017, 10:59 AM), https://www.forbes.com/sites/peterbendorsamuel/2017/05/23/the-primary-challenge-to-blockchain-technology/#1a5a8ef32aba.

217. *See* CAL. CIV. CODE § 1798.105(a) (Deering 2020); Shaverdian, *supra* note 215, at 1287 (noting that blockchain technology could conflict with the GDPR).

218. Bendor-Samuel, *supra* note 216.

219. *See* Khan & Pozen, *supra* note 177, at 503.

220. *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, 4:44 PM), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/.

221. CAL. CIV. CODE §§ 1798.100, .125.

to profit from their digital labor and towards consumers gaining greater agency and ownership over their personal information.

The CCPA acknowledges the monetary value of personal data in two ways: by assigning a specific dollar amount to personal identifying information when it is exposed in a breach; and by authorizing a scheme by which businesses can pay consumers for the right to collect and sell their personal information.[222]

1. Private Right of Action

A significant feature of the CCPA is that it allows consumers to recover following a data breach, even if the exposure of their data did not result in financial harm.[223] Despite the increasing frequency of large data breaches, consumers have generally faced a number of legal hurdles when bringing suit after a breach.[224] Much of this difficulty is because plaintiffs must establish Article III standing in order to litigate in federal court.[225]

To establish Article III standing, plaintiffs must demonstrate that they have suffered an "injury in fact," which is "concrete and particularized," "actual or imminent," and that is fairly traceable to the actions of the defendant and redressable by a favorable judgment of a federal court.[226] However, data breaches often do not result in an immediate financial harm, which makes it difficult to demonstrate that an injury is "actual or imminent."[227] Consequently, consumers face a considerable barrier to recovery if their data was exposed in a breach, because without a legally recognizable harm, they lack Article III standing.[228]

The CCPA addresses this issue and affirmatively provides consumers with the right to sue following a data breach, regardless of whether they suffered a financial harm as a result.[229] Thus, consumers need not wait to recover until a third party uses their illicitly accessed

222. *Id.* §§ 1798.125(b)(1), .150(a)(1)(A); Assemb. B. 1355, 2019–2020 Reg. Sess. (Cal. 2019).

223. *See* CAL. CIV. CODE § 1798.150(a)(1).

224. Gregory S. Gaglione, Jr., Comment, *The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America*, 67 BUFF. L. REV. 1133, 1134 (2019).

225. Clara Kim, Note, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2016 COLUM. BUS. L. REV. 544, 557.

226. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).

227. Solove & Citron, *supra* note 90, at 752.

228. Kim, *supra* note 225, at 557–58.

229. *See* CAL. CIV. CODE § 1798.150(a)(1) (Deering 2020).

data to commit financial fraud.[230] The law provides that "[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices" may bring suit to recover damages no less than $100, but no more than $750.[231]

In providing statutory damages, regardless of financial injury, the CCPA recognizes that data exposure *is* the harm.[232] Further, providing statutory damages in the absence of financial injury acknowledges that consumer data are inherently valuable. However, the CCPA does not assign a high value to these data, since consumers may only recover between $100 and $750 without proving actual damages.[233]

Additionally, the inherent value of data is weakened by the CCPA's cure period.[234] The CCPA requires that, "prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provide[] a business [with] 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated."[235] If a company cures the violation within thirty days, then an individual or class of consumers may no longer bring suit.[236]

However, a cure period may not offer an adequate solution, since data illicitly accessed via a breach can be "replicated and transmitted instantaneously and without limit."[237] In fact, a failed amendment to the CCPA, Senate Bill 561, proposed eliminating the cure period entirely because it "incentivizes companies to break the law as a business decision, on the theory that fixing a violation will cost less than complying with the law in the first instance."[238] Further, the language of the cure period suggests that a company would only need

230. *See id.*

231. *Id.* § 1798.150(a)(1)(A); Assemb. B. 1355, 2019–2020 Reg. Sess. (Cal. 2019).

232. *See* CAL. CIV. CODE § 1798.150.

233. *Id.* § 1798.150(a)(1)(A).

234. S. JUDICIARY COMM., ANALYSIS OF SENATE BILL NO. 561, 2019–2020 Reg. Sess., at 3 (Cal. 2019).

235. CAL. CIV. CODE § 1798.150(b).

236. *Id.*

237. Will Oremus, *Why Facebook Isn't Helping Its Users Who Got Hacked*, SLATE (Oct. 24, 2018, 3:42 PM), https://slate.com/technology/2018/10/facebook-data-breach-2018-victims-cybersecurity.html.

238. ANALYSIS OF SENATE BILL NO. 561, at 7.

to cure the individual violation, rather than provide a cure to all affected individuals.[239] The law also does not define "cure," which makes it difficult to determine what would be considered a solution sufficient to bar future lawsuits.[240]

Despite the low statutory damages and the potentially problematic cure period, the CCPA nevertheless acknowledges that a breach is a harm in and of itself.[241] In order for consumers to monetize their personal data, the value of this personal information must be untangled from its utility to fraudsters, and such personal information must be considered inherently valuable, whether or not it is used to commit financial fraud. The CCPA does just this by providing statutory damages to victims of data breaches that expose nonencrypted and nonredacted personal information, even if this information is not later used to commit identity theft.[242]

2. Financial Incentives for Personal Data

The CCPA further acknowledges that personal data have value beyond providing a means for criminals to access consumers' bank accounts for identity theft. The CCPA notes that a "business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information."[243]

Despite existing privacy legislation, consumers still have very little ownership over their own data. The patchwork of existing privacy laws is unable to keep pace with technological developments and emerging risks, and also does not provide any framework for consumers to actually earn money from the immense amount of data that are collected from their normal internet usage. Although the CCPA provides a mechanism through which consumers can profit from their own data, it fails to define a clear structure for them to do so.

239. Lukas Sosnicki & Ashley R. Fickel, *February 27, 2019, CCPA Webinar Q&As: Private Claims Under the CCPA*, THE FIREWALL: BLOG (Feb. 27, 2019), https://www.thefirewall-blog.com/2019/07/february-27-2019-ccpa-webinar-qas-private-claims-under-the-ccpa/.

240. *See* CAL. CIV. CODE § 1798.150.

241. *See id.*

242. *Id.* § 1798.150(a)(1)(A); Assemb. B. 1355, 2019–2020 Reg. Sess. (Cal. 2019).

243. CAL. CIV. CODE § 1798.125(b)(1); Assemb. B. 1355.

C. Alternative Framework

The CCPA gives a consumer the ability to direct businesses to both delete any personal information the business has collected on that consumer and to stop selling these data to a third party.[244] However, rather than create a presumption of digital privacy, the CCPA "opt-out" paradigm is entirely reliant on individuals' "privacy self-management."[245] Further, this opt-out structure diminishes any incentive for companies to pay consumers for their data, and thus, reduces the likelihood that consumers will monetize their own data in a meaningful way.

Previously, consumers had little control over how their data were used. Although the CCPA is a large improvement for digital privacy rights, the practical realities of an opt-out framework may prevent these rights from being widely exercised.[246] This is because the process for opting-out is cumbersome and time consuming, such that it could critically undermine the ultimate goal of the CCPA, which is to improve digital privacy.

For example, if a consumer does not want his or her personal information sold to third parties, that consumer would first need to contact at least 150 data brokers individually to request that the data brokers delete their personal information.[247] Then, the consumer would need to contact any website or digital service that he or she had previously used to individually opt out of selling his or her personal data. The number of steps consumers must take to opt out of having their data sold is deeply problematic. Although consumers want greater digital privacy, they are generally averse to managing it themselves and "have a strong preference to avoid thinking about privacy in the first place."[248]

---

244. CAL. CIV. CODE §§ 1798.105, 1798.120.

245. Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. (forthcoming 2021).

246. *See id.* (while discussing the scalability of the CCPA, Solove compares the opting-out process to being "like trying to empty the ocean by taking out a few cups of water").

247. *See Sure, You Can Have Your Data . . . After Reaching Out to 150 Brokers*, MARKETPLACE (Jan. 27, 2020), https://www.marketplace.org/shows/marketplace-tech/sure-you-can-have-your-data-after-reaching-out-to-150-brokers/.

248. Charlie Warzel, *You Care More About Your Privacy Than You Think*, N.Y. TIMES (June 11, 2019), https://www.nytimes.com/2019/06/11/opinion/privacy-facebook-sexting.html; Dan Svirsky, Why Are Privacy Preferences Inconsistent? 14–15 (June 26, 2018) (unpublished paper), http://www.law.harvard.edu/programs/olin_center/fellows_papers/pdf/Svirsky_81_revision.pdf.

Under the CCPA, consumers, by default, consent to the sale of their personal information if they do not affirmatively opt out.[249] Companies that sell consumer information benefit from the opt-out framework, because very few consumers may actually exercise the option to opt out due to inconvenience or unawareness of this option. Thus, if few consumers actually opt out of selling their data, companies have little reason to offer financial incentives to those consumers who *do* consent to having their data sold.

Alternatively, an "opt-*in*" framework could improve consumers digital privacy and improve the likelihood that businesses would exercise their option to offer financial incentives to consumers to sell their personal information. An opt-in paradigm requires that a consumer affirmatively provide consent before businesses may sell that consumer's personal information.[250] Such a mechanism could help shift the balance of power from companies to the individuals and potentially incentivize businesses to create data sharing practices that consumers would want to consent to.[251]

By shifting the power dynamic and incentivizing companies to compensate consumers for their data, an opt-in framework could greatly improve the likelihood that consumers could actually earn meaningful money from selling their own data. If companies, by default, could not sell users' personal information, those companies would be incentivized to offer financial benefits to consumers that opt in to selling their data.

However, such an opt-in system is still not without its potential downsides. An opt-in paradigm could upset the data marketplace and have serious economic impacts.[252] Critics of an opt-in framework argue that requiring consent for data collection would hinder innovation by reducing the size and diversity of available data sets.[253] Additionally, an opt-in structure would impact advertising-based

249. CAL. CIV. CODE §§ 1798.115(d), .120, .135; Brian Barrett, *Hey, Apple! 'Opt Out' Is Useless. Let People Opt In*, WIRED (Aug. 2, 2019), https://www.wired.com/story/hey-apple-opt-out-is-useless/.

250. Barrett, *supra* note 249.

251. *Id.*

252. *See* Daniel Castro, *How an "Opt-In" Privacy Regime Would Undermine the Internet Ecosystem*, INFO. TECH. & INNOVATION FOUND. (May 26, 2017), https://itif.org/publications/2017/05/26/how-opt-in-privacy-regime-would-undermine-internet-ecosystem.

253. Polina Arsentyeva, *It's 2019, So Why Are We Still Talking About Opt-In Consent?*, INT'L ASS'N OF PRIV. PROS. (Nov. 12, 2019), https://iapp.org/news/a/its-2019-so-why-are-we-still-talking-about-opt-in-consent/.

online business models, particularly those businesses that fund "free" online services by selling consumer data for targeted advertising.[254]

However, these concerns may be exaggerated. Even if the CCPA was modified such that consumers would consent to having their data sold rather than opt out, as it is currently, websites could still use digital advertising to fund free services, just not targeted or behavioral advertising. An opt-in framework would not preclude businesses from selling general advertising space on their websites but would require user consent for targeted behavioral advertising.[255] Although the market for targeted advertising exceeds $20 billion, there is limited support that targeted advertising is actually more effective than non-targeted advertising.[256] The GDPR utilizes an opt-in structure and illustrates that requiring consumers to opt in to sharing and selling their data does not necessarily lead to catastrophic economic results.[257]

IV. CONCLUSION

The CCPA has created an immense amount of uncertainty and excitement, and its impacts may be felt across the entire California economy.[258] However, structural issues with the CCPA may result in low consumer engagement and undermine material improvements to consumer cybersecurity. The new law, although targeted at data brokers and large technology companies, is written in such a way that it will apply to almost all industries.[259] Further, due to the law's cumbersome opt-out framework, the benefits of the CCPA—to provide a means by which consumers can monetize their own data—may not be realized and may ultimately be overlooked. These issues

254. ALAN MCQUINN & DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., A GRAND BARGAIN ON DATA PRIVACY LEGISLATION IN AMERICA 5 (2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf.

255. *See* Jessica Davies, *After GDPR, the New York Times Cut Off Ad Exchanges in Europe—and Kept Growing Ad Revenue*, DIGIDAY (Jan. 16, 2019), https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/ (discussing the impacts of the GDPR, which reduced behavioral targeted advertising).

256. Valentino-DeVries et al., *supra* note 31; Natasha Lomas, *Targeted Ads Offer Little Extra Value for Online Publishers, Study Suggests*, TECHCRUNCH (May 31, 2019, 9:09 AM), https://techcrunch.com/2019/05/31/targeted-ads-offer-little-extra-value-for-online-publishers-study-suggests.

257. *See, e.g.*, Davies, *supra* note 255.

258. Eric Goldman, *Some Lessons Learned from the California Consumer Privacy Act (CCPA), 18 Months in (Part 2 of 3)*, TECH. & MKTG. L. BLOG (Dec. 17, 2019), https://blog.ericgoldman.org/archives/2019/12/some-lessons-learned-from-the-california-consumer-privacy-act-ccpa-18-months-in-part-2-of-3.htm.

259. *Id.*

have not been addressed via any of the recent amendments to the CCPA, which have mostly failed to make any significant changes to the law.[260]

Nevertheless, the law is not beyond repair and because the CCPA assigns value to consumer data, it signals a tide change in consumer privacy. The CCPA helps to create a system that places consumers in greater control of their own data, such that "[n]o company is entitled to data; they are entrusted with it."[261] By requiring that companies disclose how consumer data are used and with whom such data are shared, the CCPA helps to provide consumers with the information necessary to make informed choices and to hold companies accountable.[262] Further, enabling consumers to sell their own data increases the likelihood that consumers will, in fact, hold companies accountable, since these data will have actual monetary value. Thus, while imperfect, the CCPA may indicate momentum towards a paradigm where companies are merely the custodians, not the owners, of consumer data.

260. Tanya Forsheit, *And at the End of the Day, the CCPA Remains Very Much the Same (Guest Blog Post)*, TECH. & MKTG. L. BLOG (Sept. 16, 2019), https://blog.ericgoldman.org/archives/2019/09/and-at-the-end-of-the-day-the-ccpa-remains-very-much-the-same-guest-blog-post.htm.

261. Fredrick Lee, *CCPA Won't Be Enough to Fix Tech's Data Entitlement Problem*, TECHCRUNCH (Feb. 7, 2020, 12:09 PM), https://techcrunch.com/2020/02/07/ccpa-wont-be-enough-to-fix-techs-data-entitlement-problem/.

262. *Id.*; CAL. CIV. CODE § 1798.100 (Deering 2020).