Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 15 | Issue 2 Article 8

5-18-2021

THE COMMODIFICATION OF PERSONAL DATA AND THE ROAD TO CONSUMER AUTONOMY THROUGH THE CCPA

Blaire Rose

THE COMMODIFICATION OF PERSONAL DATA AND THE ROAD TO CONSUMER AUTONOMY THROUGH THE CCPA

ABSTRACT

The internet has transformed into a museum of personal information collected through the digital footprint we leave behind after each act performed on the web. Businesses have monetized this collection of personal data in various ways. For instance, many companies analyze this information through predicting analytics and data profiling to identify consumer interests that they can exploit as a means to generate revenue. Though user data promotes many benefits for businesses and consumers alike, the recent data breaches of massive companies, coupled with hazy privacy disclosures that beget consent disputes, have left both users and businesses perturbed and exposed to various risks. The California Consumer Privacy Act (CCPA) attempts to regulate businesses' use of Californian consumer data and purports to be a promising solution to concerns regarding data privacy. However, its poor drafting and unintelligible requirements pose serious challenges such that the Act ultimately fails to provide consumers with primary control over their personal information that's collected online. This Note examines the "anti-discrimination" provision enumerated in section 1798.125 of the CCPA and addresses the ineffectual restraints placed on businesses that transact in personal data. To encourage transparency and enable informed consumer decision-making, this Note recommends that California should: 1) void the reasonable-relationship exception in section 1798.125(a)(2) since it undermines the provision, and the valuation of personal data across different industries is inconsistent and unmanageable; and 2) supplement the "financial incentives exception" in section 1798.125(b)(1) with additional restrictions on permissible practices that prioritize disclosure and foster consumer autonomy.

INTRODUCTION[1]

Data privacy regulations concern the legal restrictions and customs that "govern the use, transfer, and processing of personal data."[2] Increased

1. While writing this Note, California voters passed Proposition 24, the California Privacy Rights Act (CPRA) of 2020. The CPRA amends and expands numerous provisions within the existing CCPA and will become operative on January 1, 2023. However, this Note and statutory language quoted herein refers only to the existing language of the CCPA. *See* CPRA, CA Proposition 24 (2020), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf; *see also* Robert N. Famigletti & Christine E. Lyon, *CPRA Passes: California Voters Approve Proposition 24*, CLIENT ALERT (Nov. 4, 2020), https://www.mofo.com/resources/insights/201104-cpra-passes-california.html.

attention on infamous data breaches coupled with growing concerns over the security of personal information[3] has culminated in a widespread demand for data privacy legislation. Yet, the federal government has refrained from implementing a universal data privacy regime, which has resulted in a nationwide patchwork of nonuniform and unclear state laws and industry specific regulations.[4]

In 2018, California passed the California Consumer Privacy Act of 2018 (the Act or CCPA)—perhaps the most sweeping privacy legislation ever enacted in United States history.[5] The CCPA[6] establishes both privacy limits and obligations on businesses managing[7] data of Californian consumers.[8] Additionally, the Act provides California residents new rights for protecting and retaining authority over their personal information,[9] such as "the right to request that a business delete any personal information about the consumer which the business has collected,"[10] and the right "to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information."[11] Although the Act is a California statute, any business regardless of location is subject to the Act's provisions if it collects, or controls the collection of, personal

2. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2058 (2004) (citing Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1659–60 (1999)).

3. *See generally* Aaron Smith, *Americans and Cybersecurity*, PEW RES. CTR. (Jan. 26, 2017), https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

4. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection; *see also* STEPHEN P. MULLIGAN, WILSON C. FREEMAN, CHRIS D. LINEBAUGH, CONG. RES. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW (Mar. 25, 2019).

5. The Act was passed in 2018 but did not go into effect until January 1, 2020. *See* Purvi G. Patel, Nathan D. Taylor & Alexandra E. Laks, *The 2018 California Consumer Privacy Act*, MORRISON & FOERSTER (June 29, 2018), https://www.mofo.com/resources/publications/180629-california-consumer-privacy-act-2018.html#_ftn1.

6. The CCPA defines a "consumer" as any "natural person who is a California resident," which is defined in section 17014 of Title 18 of the California Code of Regulations. *See* CCPA, Cal. Civ. Code § 1798.140(g) (2018); *see also* 18 CCR § 17014(a)(1) (2018) ("Resident includes every individual who is in this state for other than a temporary or transitory purpose.").

7. The Act applies to businesses that either collect or control the collection of consumer personal information. *See generally* CCPA, Cal. Civ. Code § 1798.100 (2018).

8. Confusion over the definition of "Californian consumer" remains a point of notable concern since the breadth of the definition of "consumer" extends far beyond state borders and instigates other difficulties in interpretation. *See* Harriet Pearson, Fran Faircloth & Catherine Essig, *California Consumer Privacy Act: The Challenge Ahead – Key Terms in the CCPA*, CHRON. OF DATA PROTECTION 2 (Sept. 14, 2018), https://www.hldataprotection.com/2018/09/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-key-terms-in-the-ccpa/.

9. *See* Akin Gump Strauss Hauer & Feld LLP, *California Passes Landmark Consumer Privacy CCPA – What it Means for Businesses*, JD SUPRA (July 9, 2018), https://www.jdsupra.com/legalnews/california-passes-landmark-consumer-87324/.

10. CCPA, Cal. Civ. Code § 1798.105(a) (2018).

11. *Id.* § 1798.120(a).

information from a California resident [12] and meets other qualitative factors. [13] Thus, the Act's enactment prompted a majority of businesses throughout the United States to quickly adopt and amend practices to comply with the legislation before it took effect in 2020.[14] In fact, several states have initiated other legislative proposals to introduce their own rendition of privacy laws, remarkably similar to the CCPA.[15]

While the CCPA attempts to answer the call for data protection, the Act continues to be met with considerable criticism related to unclear definitions, [16] ambiguities within provisions, [17] and insufficient guidance concerning these issues from the California Attorney General.[18] Although amendments addressing these issues have been added,[19] questions regarding several of its provisions remain unanswered.[20]

In particular, the "anti-discrimination provision" documented in section 1798.125 of the CCPA [21] has generated notable controversy among businesses. [22] While this provision is intended to prevent and prohibit

12. *What Businesses Outside California Should Know About the California Consumer Privacy Act*, TANNENHAUM HELPERN SYRACUSE & HIRSCHTRITT LLP (Mar. 20, 2019), https://www.thsh.com/publications/what-businesses-outside-california-should-know-about-the-california-consumer-privacy-act.

13. Businesses must also satisfy one of the following thresholds: (1) annually earns gross revenues in excess of $25,000,000; (2) annually buys, sells, or receives or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or (3) derives at least 50% of its annual revenues from selling consumers' personal information. *See* CCPA, Cal. Civ. Code § 1798.140(c)(1).

14. Patel et al., *supra* note 5.

15. *See* Joseph J. Lazzarotti, Jason C. Gavejian & Maya Atrakchi, *State Law Developments in Consumer Privacy*, JACSKSONLEWIS (Mar. 15, 2019) https://www.workplaceprivacyreport.com/2019/03/articles/consumer-privacy/state-law-developments-in-consumer-privacy/.

16. *See* Letter from Eric Goldman on behalf of 41 California Privacy Experts to California Legislature (Jan. 17, 2019), TECH. & MKTG. L. BLOG, https://blog.ericgoldman.org/archives/2019/01/41-california-privacy-experts-urge-major-changes-to-the-california-consumer-privacy-act.htm.

17. *See* Ronald I. Raether, Sadia Mirza, *INSIGHT: So the CCPA is Ambiguous – Now What?*, BLOOMBERG L. (June 14, 2019, 4:00 AM), https://news.bloomberglaw.com/privacy-and-data-security/insight-so-the-ccpa-is-ambiguous-now-what.

18. *See* Sam Sabin, *Companies Know California Privacy Law Goes Into Effect by Jan. 1, but Little Else*, MORNING CONSULT: DATA PRIV. (Aug. 21, 2019, 11:31 AM), https://morningconsult.com/2019/08/21/companies-know-california-privacy-law-goes-into-effect-by-jan-1-but-little-else/.

19. *See* Jeewon Kim Serrato & Susan Ross, *And then there were five: CCPA amendments pass legislature*, DATA PROT. REP. (Sept. 17, 2019), https://www.dataprotectionreport.com/2019/09/and-then-there-were-five-ccpa-amendments-pass-legislature/.

20. *See* David Stauss, Bob Bowman, Marci Kawski & Tobias P. Moon, *CCPA Update: Analyzing the G's Proposed Regulations*, BYTE BACK (Oct. 10, 2019), https://www.bytebacklaw.com/2019/10/ccpa-update-analyzing-the-ags-proposed-regulations/#more-2508.

21. "Anti-discrimination provision" refers generally to CCPA, Cal. Civ. Code § 1798.125 (2018).

22. *See generally* Mark Brennan, James Denvil, Shee Shee Jin & Jonathan Hirsch, *California Consumer Privacy Act: The Challenge Ahead – The CCPA's Anti-Discrimination Clause*, CHRON. DATA PROT. 10th (Dec. 12, 2018), https://www.hldataprotection.com/2018/12/articles/consumer-

businesses from discriminating against consumers who exercise their newly obtained rights granted by the Act,[23] it also provides exceptions "to the general prohibition on discrimination."[24] These exceptions authorize businesses to create a tiered pricing structure to charge different prices for consumers who voluntarily provide their data[25] and permit businesses to offer "financial incentives" in exchange for personal information.[26] The plain language of section 1798.125, which allows a business to charge consumers who exercise their rights "a different price or rate"[27] or provide "a different level or quality of goods or services to the consumer,"[28] appears to contradict the provision[29] immediately preceding that authorization. This prefatory language explicitly forbids businesses from "[c]harging different prices or rates for goods or services," or "[p]roviding a different level or quality of goods or services" to consumers who exercise their rights.[30] Thus, although section 1798.125 may have been well-intended, the plain language[31] of the provision, without further clarification, instantiates the "contradictory and ambiguous"[32] nature of the Act.

Businesses have struggled to make sense of this paradox and are confused about how the provision would legally work.[33] The recurring questions and concerns echoed by these businesses illuminate the fundamental problems with this provision.[34] Specifically, the "reasonable relationship exception" in section 1798.125(a)(2),[35] which permits businesses to charge consumers who provide their data, as compared to those who do not, with enticing prices so long as that "difference [in price]

privacy/california-consumer-privacy-act-the-challenge-ahead-the-ccpas-anti-discrimination-clause/.

23. CCPA, Cal. Civ. Code § 1798.125 (2018).

24. *See generally* Brennan, et al., *supra* note 22.

25. CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018).

26. *Id.* § 1798.125(b)(1).

27. *Id.* § 1798.125(a)(2).

28. *Id.*

29. *See generally id.* § 1798.125(a)(1).

30. *Id.*

31. *Compare* CCPA, Cal. Civ. Code § 1798.125(a)(1) ("A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title . . . ."), *with* CCPA, Cal. Civ. Code § 1798.125(b)(1) ("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. A business may also offer a different price, rate, level, or quality of goods or services to the consumer . . . .").

32. *See* Anthony Dazhan, *CCPA compliance: A rocky road ahead?*, DATAGUISE BLOG (Mar. 28, 2019), https://www.dataguise.com/blog/ccpa-compliance-rocky-road-ahead.

33. *See id.*

34. *See* Grant Davis-Denny, *Confusion in Calif. Privacy Act's Anti-Discrimination Rule*, LAW 360 (Sept. 5, 2018, 1:49 PM), https://www.law360.com/articles/1079569/confusion-in-calif-privacy-act-s-anti-discrimination-rule.

35. "Reasonable relationship exception" refers generally to CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018).

is reasonably related to the value provided to the business,"[36] presents challenges in terms of calculating the value of that data to which the provision refers.[37] The "financial incentives exception" in section 1798.125(b)(1)[38] is also problematic since it fails to explicate allowable compensatory payments[39]—the only demarcation between permissible and impermissible incentives is the vague caveat outlined in section 1798.125(b)(4) which proscribes "incentive practices that are unjust, unreasonable, coercive, or usurious in nature."[40]

The unaddressed ambiguity and deficient language within the anti-discrimination provision leaves businesses to translate for themselves what the provision requires for compliance[41]—a precarious guessing game that affects unknowing consumers who transact with these players. Since there is little likelihood that the grey area will be clarified by further amendments,[42] businesses must look to the legislative intent[43] and common industry practices to formulate a uniform and appropriate interpretation of this provision.

Accordingly, Part I of this Note will recount the evolution of the internet and the development of the personal data marketplace, as well as the current data privacy regulations in the United Sates. Part II will discuss the creation of the CCPA and the legislative intent behind its implementation. Part III will illuminate the ambiguities and inadequacies of section 1798.125, the anti-discrimination provision, and consider the impending consequences that will likely result from its unintelligible

36. *See* CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018) ("Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.").

37. *See* Muge Fazlioglu, *Top 5 Operational Impacts of the CCPA: Part 4 – Rights of erasure, objection to sale, and nondiscrimination*, INT'L ASSOC. PRIVACY PROFS. (Aug. 14, 2018), https://iapp.org/news/a/top-5-operational-impacts-of-cacpa-part-4-rights-of-erasure-objection-to-sale-and-non-discrimination/#.

38. "Financial incentives exception" refers generally to CCPA, Cal. Civ. Code § 1798.125(b)(1) (2018).

39. CCPA, Cal. Civ. Code §1798.125(b)(1) states that "financial incentives, including payments to consumers as compensation" are permissible but does not provide any further detail defining what other incentives businesses may offer to induce consumers to relinquish their personal information. *See id*.

40. *Id.* § 1798.125(b)(4).

41. *See* Lydia F de la Torre, *Interpreting CCPA using the "Golden Rule": Purposes for processing, sales, and records threshold*, GOLDEN DATA BLOG (Sept. 7, 2019), https://medium.com/golden-data/interpreting-ccpa-using-the-golden-rule-6fcb1a8d03b5.

42. The end of the legislative session was September 13, 2019. Therefore the CCPA, once signed by the Governor, will take effect on January 1, 2020, as drafted, with few changes from amendments and regulations. *See* Deborah A. George, *California CCPA Amendment Update: Here's What Passed*, ROBINSON COLE (Sept. 19, 2019), https://www.dataprivacyandsecurityinsider.com/2019/09/california-ccpa-amendment-update-heres-what-passed/.

43. *See generally* Lauren Mattiuzzo, *Legislative Intent and Statutory Interpretation*, HEINONLINE BLOG (Mar. 22, 2018), https://home.heinonline.org/blog/2018/03/legislative-intent-and-statutory-interpretation/.

drafting. Finally, Part IV will offer a solution to the existing problems within section 1798.125 that protects both businesses and consumers by voiding the "reasonable relationship exception" provided in section 1798.125(a)(2), and amending the "financial incentives exception" authorized in section 1798.125(b)(1) to include additional regulations that refashion the restraints on businesses in a manner that advances the legislative intent behind the Act and provides value to consumers.

I. BACKGROUND

"*We are in a very interesting and, I would say, complicated period in the internet's history, on this planet anyway, of trying to figure out how to maximize its utility while minimizing some of the harmful aspects that are appearing*."[44]

A. EXPANSION OF THE INTERNET & THE UNDERGROUND DATA MARKETPLACE

As the computerization of information developed, concerns about privacy increased and Congress attempted to regulate information held by federal agencies.[45] Still, many legislative attempts to control government information systems fell short.[46] Amid the internet's evolution, personal information became a coveted target for commodification.[47]

"Commodified personal data is a discrete package of personal information that can be exchanged for something else."[48] The process of commodifying data into a profit generating asset involves four main stages: "(i) collection (ii) processing (iii) mining, and (iv) usage."[49] The internet

44. Vinton Cerf, *Future of the Internet with Vint Cerf*, CXO TALK #331 (Mar. 8, 2019), https://www.cxotalk.com/episode/future-internet-vint-cerf. Vinton Cerf, Chief Internet Evangelist, Google, is a computer scientist often referred to as the "Father of the Internet" for creating, with Robert Kahn, "the TCP/IP protocols and the architecture of the Internet." *See Vint Cerf*, INTERNET HALL FAME (last visited Oct. 11, 2019), https://internethalloffame.org/inductees/vint-cerf.

45. *See* Freedom of Information Act of 1966, 5 U.S.C. § 552(a)(3)(A); *see also* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (2000) (codified at 5 U.S.C. § 552a); *see also* Family Educational Rights and Privacy Act of 1974 (FERPA), Pub. L. No. 93-380, 88 Stat. 484, (codified at 20 U.S.C. § 1232g).

46. *See* Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE, PLI 1, 1–26 (Kristen J. Mathews ed., 2016) (2006), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

47. A "commodity" is a good "that is subject to ready exchange or exploitation within a market." *Commodity*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/commodity (last visited Mar. 30, 2021).

48. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2069 (2004).

49. *See* Emile Douilhet & Dr. Argyro Karanasiou, *Legal responses to the commodification of personal data in the era of big data: The paradigm shift from data protection towards data ownership*, INFORM. COMM. SOC., 2 (June 2012), https://www.researchgate.net/publication/

provides new methods for collecting information[50] through "clickstream data"[51] and "cookies,"[52] which allows websites to identify and aggregate user information through an individual's online activity.[53] Businesses use computer algorithms and analytics software to gather consumer data and help recognize behavioral patterns.[54] Consumer data tracking is then employed to increase sales[55] and generate revenue through numerous mechanisms[56] like creating targeted advertising[57] and trading information through data brokerage companies.[58] Data can also be rented to marketers as another source of income.[59]

This process precipitated the inception of a personal data trade market.[60] Data brokers[61] buy and sell personal data they have gathered through public records, commercial sources, and online activity, among

316878931_Legal_responses_to_the_commodification_of_personal_data_in_the_era_of_big_data_The_paradigm_shift_from_data_protection_towards_data_ownership.

50. *See* Solove, *supra* note 46, at 1–36.

51. "A clickstream is a record that contains data about a website user's clicks on a computer display screen . . . [which] provides a visual trail of user activity with detailed feedback. Such data . . . facilitate[s] market research. . . ." *Clickstream*, TECHOPEDIA, https://www.techopedia.com/definition/15403/clickstream (last visited Dec. 27, 2019); *see also* Solove, *supra* note 46, at 1–36

52. "A cookie is the term given to describe a type of message that is given to a web browser by a web server. The main purpose of a cookie is to identify users and possibly prepare customized Web pages or to save site login information for you. . . . [A] cookie will contain . . . information about the browser. . . . Some Web sites do use cookies to store more personal information about you." *See* Vangie Beal, *What are Cookies and What do Cookies Do?*, WEBOPEDIA (Sept. 4, 2008), https://www.webopedia.com/DidYouKnow/Internet/all_about_cookies.asp; *see also* Solove, *supra* note 46, at 1–36.

53. *See* Max Eddy, *How Companies Turn Your Data Into Money*, PCMAG: FEATURES (Oct. 10, 2018, 8:00 AM), https://www.pcmag.com/article/364152/how-companies-turn-your-data-into-money.

54. *See* Cindy Waxer, *How data mining can boost your revenue by 300%*, CNNMONEY (Oct. 28, 2013, 6:20 AM), https://money.cnn.com/2013/10/28/smallbusiness/data-mining/.

55. *Id.*

56. *See* Douilhet & Karanasious, *supra* note 49.

57. Eddy, *supra* note 53.

58. *See* Wibson, *What is a Decentralized, Privacy-Preserving Data Marketplace, and Why is it Important for You?*, MEDIUM (Dec. 1, 2017) https://medium.com/wibson/what-is-a-decentralized-privacy-preserving-data-marketplace-and-why-is-it-important-for-you-b49df43c213c.

59. *See* Solove, *supra* note 46, at 1-36 (citing Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN L. REV. 1393, 1407–09 (2001)).

60. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2069 (2004).

61. *See What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing on S. Hrg. 113-693 Before the S. Comm. on Commerce, Science, and Transportation*, 113th Cong. 7 (2015) (statement of Hon. John D. Rockefeller IV, U.S. Senator from West Virginia, citing Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, at 68 (Mar. 2012)) ("While there is no statutory definition for 'data brokers,' the Federal Trade Commission has defined this term to include 'companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud.'").

others.[62] Data brokers amass "categories of information about individuals" which provide insight into consumer behaviors, buying preferences, and even a consumer's location at the time the data is collected.[63] By merely using a smartphone or credit card in the current technology landscape, consumers unknowingly expose the most intimate details of their lives to companies, ranging from "if you've just gone through a break-up, if you're pregnant or trying to lose weight" to "what medicine you take, where you've been, and even how you swipe and tap on your smartphone."[64] Worst of all, consumers are usually unaware of this process or have not consented[65] to their information transmogrifying into a commodity used by a "faceless corporation."[66]

Despite industry-specific guidelines and privacy-related consumer protection laws that protect personal information, [67] there is still no comprehensive federal data privacy law in the United States.[68] The growth of the internet has also been accompanied by the rise in data breaches which "have become troublingly pervasive and continue to increase in prevalence,"[69] often affecting billions of consumers of some of the most prominent corporations throughout the United States.[70] Due to the increased severity and frequency of data breaches, as well as heightened consumer awareness and concern over how businesses use personal information,

62. *See* Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, MOTHERBOARD: TECH BY VICE (Mar. 27, 2018, 10:00 AM), https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.

63. *See What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing on S. Hrg. 113-693 Before the S. Comm. on Commerce, Science, and Transportation*, 113th Cong. 14 (2015) (statement of Hon. John D. Rockefeller IV, U.S. Senator from West Virginia) (identifying several examples of categories of information that data brokers collect from individuals).

64. Steven Melendez & Alex Pasternack, *Here are the data brokers quietly buying and selling your personal information*, FAST COMPANY (Mar. 02, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

65. *See* Wibson, *supra* note 58.

66. *See* Nate Cardozo, *Internet Companies: Confusing Consumers for Profit*, ELEC. FRONTIER FOUND. (Oct. 14, 2015), https://www.eff.org/deeplinks/2015/10/internet-companies-confusing-consumers-profit.

67. *See* Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45; *see also* Gramm-Leach-Bliley Act (GLBA) of 1999, Pub. L. No. 106-102, 113 Stat. 1338, (codified at 15 U.S.C. §§ 6801–09); *see also* Health Insurance Portability and Accountability Act (HIPPA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

68. *See generally* Ieuan Jolly, *Data Protection in the United States: Overview* (Oct. 1, 2018), https://1.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default.

69. *See* William Williams, *On the Clock, Best Bet to Draft Cyberdefensive Lineman: Federal Regulation of Sports Betting from a Cybersecurity Perspective*, 13 BROOK. J. CORP. FIN. & COM. L. 539, 548 (2019) (citing *Data Breaches Compromised 4.5 Billion Records in First Half of 2018*, BUS. WIRE (Oct. 9, 2018), https://www.businesswire.com/news/home/20181008005322/en/.).

70. *See generally* Latoya Irby, *10 Biggest Data Breaches That Affected U.S. Consumers*, BALANCE: PERS. FIN. (June 25, 2019), https://www.thebalance.com/the-10-biggest-data-breaches-that-affected-u-s-consumers-4570940.

Congress and state legislatures have felt increased pressure to address the deficiency of data privacy legislation within the nation.[71] Additionally, the proliferation of privacy regimes in other advanced economies,[72] most notably the implementation of the General Data Protection Regulation (GDPR) in the European Union, has compelled the United States to turn discussion into action.[73]

B. CURRENT FEDERAL PRIVACY REGULATIONS

Under the current regime in the United States, there are several federal laws that oversee different aspects of personal information protection[74] including: 1) the Gramm-Leach-Bliley Act (GLBA),[75] which imposes duties on financial institutions[76] regarding consumer "nonpublic personal information;"[77] 2) the Securities and Exchange Act of 1934,[78] which offers some regulation over data breaches;[79] 3) the Federal Trade Commission Act (FTC Act),[80] which provides significant data protection safeguards[81] and has a "uniquely important role . . . in the U.S. data protection landscape;"[82] and 4) the Consumer Financial Protection Act (CFPA),[83] which regulates financial services provided to consumers[84] but is relatively "inactive in the data privacy and security space."[85]

71. *See* Joseph V. Moreno, Sohie K. Cuthbertson, James A. Treanor, Keith M. Gerver & Stephen Weiss, *The Digital Revolution Takes on New Meaning: Among Calls for Heightened U.S. Data Privacy Measures, California is King*, CADWALADER (Mar. 1, 2019), https://www.cadwalader.com/resources/clients-friends-memos/the-digital-revolution-takes-on-new-meaning-among-calls-for-heightened-us-data-privacy-measures-california-is-king.

72. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection (noting that Canada, Israel, and Japan, have all started implementing privacy regimes comparable to the GDPR).

73. *Id.*

74. Mulligan et al., *supra* note 4, at 7.

75. *See* Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801–6809 (2012).

76. Mulligan et al., *supra* note 4, at 8.

77. *See* Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6809(4)(a)–(c) (2012) (defining "nonpublic personal information" as "personally identifiable financial information" provided to a financial institution by a consumer, "resulting from any transaction with the consumer," or "otherwise obtained by the financial institution" and "does not include publicly available information.").

78. *See* Securities and Exchange Act of 1934, 15 U.S.C. §§ 78a–78qq (2012).

79. Mulligan et al., *supra* note 4, at 21–22.

80. *See* Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45(a) (2012).

81. Mulligan et al., *supra* note 4, at 32 ("The FTC has brought hundreds of enforcement actions against companies alleging deceptive or unfair data protection practices.").

82. *Id.*

83. *See* Consumer Financial Protection Act (CFPA), Pub. L. No. 111-203, tit. X, 124 Stat. 1376, 1955–2113 (2010) (codified at 12 U.S.C. §§ 5491–5603).

84. There is a comprehensive list defining "financial products or services," which includes extending credit, brokering leases of property, engaging in deposit-taking activities, and providing payment processing services, among others. *See* 12 U.S.C. § 5481(15) (2010).

85. Mulligan et al., *supra* note 4, at 36.

Despite the aforementioned regulations, there is no comprehensive federal privacy law that safeguards the personal data obtained through new technologies[86] and used within the online data marketplace.[87] The Federal Trade Commission (FTC) has undertaken an important task of patrolling cybersecurity and enforcing consumer protection violations,[88] often managing actions related to a corporation's failure "to protect consumer data against hackers."[89] In *FTC v. Wyndham Worldwide*, the Third Circuit upheld the FTC's authority to "regulate corporate cybersecurity through 45(a)."[90] Despite Wyndham's attempt to limit the span of the FTC Act[91] by excluding cybersecurity violations from the Commission's reach,[92] the court reaffirmed the FTC's ability to bring "unfairness actions against companies whose inadequate cybersecurity resulted in consumer harm."[93] Nevertheless, the Third Circuit also "recognize[d] that the Commission's existing authority may not be sufficient to effectively protect consumers with regard to *all* data privacy issues of potential concern."[94] Though the "FTC currently remains a key linchpin in the U.S. data protection regulatory regime,"[95] there are still large gaps within data privacy law that remain unfilled. Notably, the sectoral approach to data privacy in the United States has created gaps in data protection where specific industries that lack privacy regulation remain unchecked.[96]

86. *See generally What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing on S. Hrg. 113-693 Before the S. Comm. on Commerce, Science, and Transportation*, 113th Cong. 55 (2015) (statement of Hon. John Thune, U.S. Senator from South Dakota).

87. The "data marketplace" concept represents the online platform where data is exchanged and personal information is traded by companies and data brokers, often without consumer consent or knowledge. *See* Wibson, *supra* note 58.

88. *See generally* Memorandum from the Federal Trade Commission on its consumer protection powers and enforcement authority, *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (Oct. 2019), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

89. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

90. *Id.* at 248.

91. *See* FTC Act, 15 U.S.C. § 45(a) (2012) ("The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.").

92. *See Wyndham Worldwide Corp*., 799 F.3d at 247.

93. *Id.* at 249.

94. *Id.* (citing *In the Matter of LabMD, Inc.*, 2014-1 Trade Cases P 78784 (F.T.C.), 2014 WL 253518, at *6 (Jan. 16, 2014)).

95. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2269 (2015).

96. A sectoral approach "means that there are a multitude of different laws regulating different industries rather than just one general statute to regulate all collection and use of personal data." *See id.* at 2267.

II. CREATION OF THE CCPA

"*If you're not paying for it, you're not the customer; you're the product being sold*." [97]

A. GENERAL PURPOSE OF THE ACT

The crescendo of personal data exploitation continued to intensify as "data broker[s] and ad-tech industries" [98] overwhelmingly misused consumer information, and finally reached its peak in March 2018[99] when the Cambridge Analytica[100] scandal shocked the nation. After Cambridge Analytica improperly harvested[101] data from roughly 87 million Facebook profiles,[102] the misappropriated "information was later deployed in political campaigns"[103] and allegedly used by President Trump's campaign staff to create targeted ads based on user data during the 2016 election.[104] Although theories and suppositions about how data *could* be mishandled were beginning to swell, it took this event for many individuals to grasp how this "squishy, intangible thing called privacy has real-world consequences."[105] The California Legislature recognized the harm caused to the entire tech industry[106] by these "scandals and blowbacks,"[107] which heightened the "desire for privacy controls and transparency in data practices." [108] Accordingly, it created the CCPA with "the intent . . . to further

97. *See* Timothy Taylor, *"If You're Not Paying for It, You're the Product"*, CONVERSABLE ECONOMIST (Jan. 2, 2018, 8:00 AM) (statement of Andrew Lewis), http://conversableeconomist.blogspot.com/2018/01/if-youre-not-paying-for-it-youre-product.html.

98. *Stop companies from exploiting our data!*, GDPR TODAY (Dec. 17, 2018), https://www.gdprtoday.org/stop-companies-from-exploiting-our-data/.

99. *See generally* Assemb. Bill 375, 2017-2018 Reg. Sess., Ch. 55, Sec. 2(g) (Cal. 2018).

100. Cambridge Analytica is a data analytics firm that "provides data-driven campaigning and marketing services" to customers "for the electoral process." *See Cambridge Analytica,* Section on Company Profile and News, BLOOMBERG L., https://www.bloomberg.com/profile/company/1584842D:LN (last visited Dec. 23, 2019).

101. The term "data harvesting" refers to the process of extracting and analyzing "data collected from online sources." *See Data Mining Process: The Difference Between Data Mining & Data Harvesting*, IMPORT.IO (Apr. 23, 2019), https://www.import.io/post/the-difference-between-data-mining-data-harvesting/.

102. *See In re Facebook – Cambridge Analytica*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/facebook/cambridge-analytica/ (last visited Feb. 4, 2021).

103. *See* Alexandra Ma & Ben Gilbert, *Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here's everything that's happened up until now.*, BUS. INSIDER (Aug. 23, 2019, 3:30 PM), https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3.

104. *Id.*

105. *See* Issie Lapowsky, *How Cambridge Analytica Sparked the Great Privacy Awakening*, WIRED: BUS. (Mar. 17, 2019, 7:00 AM), https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/.

106. *See id*.

107. *See id*.

108. Assemb. Bill 375, 2017-2018 Reg. Sess., Ch. 55, Sec. 2(g) (Cal. 2018).

Californians' right to privacy by giving consumers an effective way to control their personal information."[109]

Though California is known to be a trailblazer in technology,[110] California law has not kept pace with growing privacy concerns.[111] In an attempt to safeguard consumer's personal information,[112] the state legislature passed the Act.[113] While it "is intended to provide California residents with greater transparency and control over how businesses collect and use their personal information,"[114] in its original form, "[t]he CCPA is riddled with typos and has provisions that are vague or simply do not make sense."[115]

B. AMENDMENTS AND PROPOSED REGULATIONS TO THE ACT

In the attempt to clarify "several important issues," the California Attorney General passed numerous amendments to the CCPA and released the third and "Final Text of Regulations"[116] on August 14, 2020.[117] The draft regulations were adopted "to operationalize the CCPA and provide clarity and specificity to assist in the implementation of the law."[118] To that end, the regulations offer "illustrative examples"[119] to assist businesses draft permissible financial incentives and a pilot program for calculating the value of consumer data.[120]

The statute omits any methodology capable of appraising consumer data,[121] which is one of the main factors used to determine allowable

109. *Id.* at 2(i).
110. *Id.* at 2(c).
111. *Id.* at 2(d).
112. *Id.* at 2(e).
113. *Id.* at 2(c).
114. *See* Richard B. Newman, *California AG Releases Draft California Privacy Act Regulations*, NAT. L. REV. (Oct. 12, 2019), https://www.natlawreview.com/article/california-ag-releases-draft-california-privacy-act-regulations.
115. *See Overview of the New California Consumer Privacy Law*, BAKERHOSTETLER (last visited Dec. 27, 2019), https://www.dataprivacymonitor.com/wp-content/uploads/sites/5/2019/01/Overview-of-the-New-California-Consumer-Privacy-Law.pdf.
116. *See generally* CAL. CODE REGS. tit. 11, § 999 (2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf?.
117. *See* Press Release, Attorney General Becerra Submits Proposed Regulations for Approval Under the California Consumer Privacy Act (June 2, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-submits-proposed-regulations-approval-under-california.
118. *See* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, Section I, at 1, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.
119. *See* CAL. CODE REGS. tit. 11, § 999.336(d) (2020).
120. *See* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, Section IV, at 37, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.
121. *See id.*

exceptions to the prohibition of discriminatory practices.[122] Hence, the regulations attempt to provide clarity and instruction to businesses in offering financial incentives to consumers, as well as transparency to consumers on how those businesses utilize their data.[123] Be that as it may, the illustrations are unavailing and many aspects of the law remain obscure and unresolved[124] — particularly the "interpretation of the statutory exemptions."[125] Therefore, it is unlikely that the regulations will sufficiently explain section 1798.125 so as to push the provision across the goal line.

III. PROBLEMS WITH SECTION 1798.125

"*Offering consumers a few dollars while failing to address the more problematic issues surrounding data use seems to miss the mark*."[126]

A. UNCLEAR LANGUAGE

Section 1798.125(a)(2)'s reasonable-relationship exception allows businesses to charge a different price or provide a different quality of goods or services to consumers who relinquish their data, so long as that difference is "reasonably related to the value provided to the business by the consumer's data."[127] In the same subdivision and immediately preceding that authorization, section 1798.125(a)(1) forbids businesses from charging altered prices or providing different quality goods to consumers who exercise their privacy rights and deems these acts discriminatory.[128] The plain language of this provision appears contradictory. Within section 1798.125(a), the legislature proscribes discrimination against consumers who exercise their rights under the statute, yet simultaneously allows for consumers to be treated differently,[129] and explicitly empowers businesses to incentivize consumers to renounce their rights by offering a different price and quality for goods in exchange for their data.[130] Navigating through

122. *See generally* CCPA, Cal. Civ. Code § 1798.125 (2018).

123. *See* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, Section IV, at 36, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

124. *See* Nadine Peters & Andrew Rusczek, *Proposed Regulations Under the CCPA Provide Some Clarity, But Questions Remain*, JD SUPRA (Oct. 28, 2019), https://www.jdsupra.com/legalnews/proposed-regulations-under-the-ccpa-65684/.

125. *Id.*

126. Jessica B. Lee, *The Value of Talking About the Value of Consumer Data*, ADMONSTERS (Aug. 13, 2020), https://www.admonsters.com/value-consumer-data/.

127. CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018).

128. *See id.* § 1798.125(a)(1).

129. *See* Seamus Duffy, Natasha Kohne, Meredith Slawe & Michael Stortz, *California Businesses Avoid Privacy Class Action Explosion*, LAW 360 (May 21, 2019), https://www.law360.com/articles/1161746/calif-businesses-avoid-privacy-class-action-explosion.

130. *See* CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018) ("Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.").

these confusing statutory intricacies is comparable to a "trip down the rabbit hole into Wonderland,"[131] and may expose a business to massive liability[132] despite its "good faith efforts to make sense of this maze."[133]

Notwithstanding the pronounced contradiction of section 1798.125, interpreting this provision is far from simple as it is difficult to unravel compliance requirements from the plain statutory language.[134] To adhere to this provision's directives, businesses must quantify the value of an individual consumer's data and come up with an enticement that is reasonably related to that valuation, yet appraising a commodity like consumer data is no easy feat. In October 2019, the California Attorney General promulgated proposed regulations in an attempt to clarify specific language in the Act to ensure the law was implemented successfully.[135] Despite the supplementation of explanatory elaborations[136] to the anti-discrimination provision, the regulations were ineffectual. Although the regulations mandate that a business utilize a reasonable and good faith method for calculating the value of the consumer's data and record its findings,[137] its enumeration of eight approaches[138]—including a "catchall provision" that enables businesses to use "[a]ny other practical and reasonably reliable method of calculation used in good-faith" [139] — exacerbated the uncertainty in calculating the value of consumer data, yielded a non-uniform methodology for computation, and created a blueprint that is likely to produce inconsistent appraisals. Further, these methods would help businesses to justify different cost and services structures for consumers who elect to opt-out of sale.

131. *See* Duffy, *supra* note 129.

132. *See* CCPA, Cal. Civ. Code § 1798.155(b) (2018) ("Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars … for each violation or seven thousand five hundred dollars … for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.").

133. *See* Duffy, *supra* note 129.

134. *See* Timothy Tobin, James Denvil, Laurie Lai, Aaron Lariviere & Filipo Raso, *California Consumer Privacy Act: The Challenge Ahead – The Impact of the CCPA on Data Driven Marketing and Business Models*, HOGAN LOVELLS (Nov. 30, 2018), https://www.hldataprotection.com/2018/11/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-the-impact-of-the-ccpa-on-data-driven-marketing-and-business-models/.

135. *See* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, Section I, at 1, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

136. Press Release, Attorney General Becerra Publicly Releases Proposed Regulations under the California Consumer Privacy Act (Oct. 10, 2019), https://oag.ca.gov/news/press-releases/attorney-general-becerra-publicly-releases-proposed-regulations-under-california. The entire text of the draft regulations is available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

137. *See* CAL. CODE REGS. tit. 11, § 999.337(a).

138. *See id.* § 999.337(a)(1)–(8).

139. *See id.* § 999.337(a)(8).

In his "initial statement of reasons"[140] for the proposed regulations, the California Attorney General recognized the multiplicity of valuation formulas available to businesses and acknowledged that the value of data fluctuates since the aggregate of businesses that collect data significantly impacts the value of consumers' data.[141] Nonetheless, the Attorney General presumed that the provisional list, which stipulates modes for calculating the value of a consumer's data,[142] is a suitable resolution to the abstruse nature of consumer data and sufficient to assist businesses in quantifying that value. This presumption is sadly misguided as its "modeling may be more complicated than it first appears, and difficult to defend if challenged."[143] Even if businesses understood and could utilize the first seven methods enumerated in section 999.337(a),[144] the blanket safeguard that allows businesses to depart "from the methods listed in the subdivision so long as the calculation method"[145] is "practical . . . reliable . . . [and] used in good faith,"[146] will likely open the floodgates to a host of arbitrary methodologies that directly affect the incentives offered to consumers. Moreover, the regulations provide no delineation of what "practical" or "reliable" implicates and therefore, yet again, businesses are empowered to decipher the language on their own.[147]

Section 999.337[148] of the regulations is also completely deficient of any language demarcating the latitude of businesses in vacillating between permissible methods when quantifying data of individual consumers.[149] The omission is likely due to an assumption that all of the listed methods would produce the same valuation irrespective of who supplies the data or when the computation is made. Without evidentiary certainty, this presumption

140. *See generally* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

141. *See* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, Section IV, at 38, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

142. *See* CAL. CODE REGS. tit. 11, § 999.337(a)(1)–(8).

143. *See* Alston & Bird, *The Draft CCPA Regulations: 21 Potentially Significant Business Impacts*, JD SUPRA (Oct. 15, 2019), https://www.jdsupra.com/legalnews/the-draft-ccpa-regulations-21-54730/.

144. *See* CAL. CODE REGS. tit. 11, § 999.337(a).

145. *See* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, Section IV, at 39, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

146. *See* CAL. CODE REGS. tit. 11, § 999.337(a)(8).

147. *See* Luke Sosnicki & James Shreve, *What businesses need to know about the Attorney General's proposed CCPA regulations*, THOMPSON COBURN LLP (Oct. 14, 2019), https://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2019-10-14/what-businesses-need-to-know-about-the-attorney-general-s-proposed-ccpa-regulations.

148. *See* CAL. CODE REGS. tit. 11, § 999.337.

149. *See id.* § 999.337(a) ("A business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data.").

may lead to internal inconsistency in calculating specific data valuations and exasperate the overall uncertainty of how much a consumer's personal data is really worth. Furthermore, the Attorney General's disclosure that the legislature provided businesses with considerable discretion in finding a valuation approach so that it could learn through their trials which method was actually best[150] exposes this solution's shortcomings. This explanation disguises section 999.337[151] as a panacea that allows businesses to choose from the buffet of methods for consumer data appraisal. In reality, it reveals how businesses have carte blanche to select any valuation methodology that generates the greatest return after swindling consumers into relinquishing their data.

B. APPROXIMATING REASONABLENESS IN DATA TRANSACTIONS

Assuming that we can calculate the value of a consumer's data, sections 1798.125(a)(2) and (b)(1) mandate that the price or quality differential[152] offered to consumers who provide their data must be "reasonably related to the value provided to the business by the consumer's data."[153] Again, this "reasonably related" constraint [154] is asserted with no particularity or guidance for interpretation. The regulations attempt to expound this unclear language by providing impotent illustrative examples[155] depicting a "price or service difference" [156] that is "reasonably related." [157] However, the periphrastic nature of the examples and the oversimplification of the underlying process that furnishes these models constrict the regulation's usefulness.

Once a business determines what it believes to be an accurate appraisal of a consumer's personal information, it must then construct a "reasonably

150. *See* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, Section IV, at 38, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

151. *See* CAL. CODE REGS. tit. 11, § 999.337.

152. *See id.* § 999.301(o) ("'Price or service difference' means (1) any difference in the price or rate charged for any goods or services to any consumer . . . including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer . . . including the denial of goods or services to the consumer.").

153. *See* Cal. Civ. Code § 1798.125(a)(2) (2018); *see also* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, Section IV, at 37, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf (noting that the "directly related" language used in § 1798.125(b)(1) should be interpreted as "reasonably related" since this is more aligned with the intent of the CCPA to match the difference to the value of the data).

154. *See* CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018).

155. *See* CAL. CODE REGS. tit. 11, § 999.336(d).

156. *See id.* § 999.301(o).

157. *See id.* § 999.336(b).

related"[158] offer that provides a different price or quality of service to the consumer based on that initial valuation.[159] The difficulty in devising a "reasonable" offer to exchange for personal information is concealed by an assumption that overlooks the subjectivity involved in defining "reasonable" within the data privacy context. Specifically, businesses would need to transmute the monetary value that represents the data's worth into an incremental measurement of quality that can be reasonably manipulated depending on whether the consumer retains or relinquishes their information. Considering businesses' profit-seeking motives, coupled with the mandate that the offer must be "reasonably related"[160] to the data's value, it quickly becomes apparent that determining reasonableness in the context of data transactions will be difficult.

C. INCENTIVES WITH NO BOUNDS

Similarly, the financial incentives exception, which is described in section 1798.125(b)(1),[161] also demands further clarification because of its poor drafting and unclear parameters.[162] The financial incentives exception reads, in part "[a] business may offer financial incentives,[163] including payments to consumers as compensation, for the collection of personal information, [or] the sale or sharing of personal information,"[164] so long as such "financial incentive practices"[165] are not "unjust, unreasonable, coercive, or usurious in nature."[166] As drafted, the financial incentives exception is written in section 1798.125(b)[167] which "is a separate clause that is not part of the anti-discrimination clause, and therefore not tied to a consumer's exercise of rights."[168] Moreover, this exception is not explicitly curtailed by the "reasonably related to"[169] mandate that applies to businesses that offer enticing prices or qualitatively different services to consumers.

Nevertheless, this exception has some qualifiers[170] that require businesses that offer financial incentives to notify consumers of the

158. *See* CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018).
159. *See id.*
160. *Id.*
161. CCPA, Cal. Civ. Code § 1798.125(b).
162. *See* Tobin et al., *supra* note 134.
163. *See* CAL. CODE REGS. tit. 11, § 999.301(j) ("'Financial incentive' means a program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information.").
164. CCPA, Cal. Civ. Code § 1798.125(b)(1) (2018).
165. *Id*. § 1798.125(b)(4).
166. *Id.*
167. *See id.* § 1798.125(b).
168. *See* Tobin et al., *supra* note 134.
169. *See* CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018).
170. *See id*. § 1798.125(b)(2)–(4).

incentives pursuant to section 1798.130 [171] and obtain prior opt-in consent.[172] Yet, section 1798.125(b) is relatively boundless with regard to compensation payments made to consumers for the collection, sale, or deletion of personal information. [173] Consequently, the qualifying characteristics[174] provide the sole backstop for preventing discriminatory incentives and businesses are left with "more questions than answers"[175] about "how to structure their financial incentives." [176] Although the regulations require businesses to notify consumers of the "good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive,"[177] and to provide "[a] description of the method the business used to calculate the value of the consumer's data,"[178] the Act provides no method by which the compensation payment must be computed. Additionally, since this exception is not governed by the "reasonably related to"[179] constriction, businesses have wide latitude in devising financial incentive payments. Finally, the Act's failure to define the scope of "unjust, unreasonable, coercive, or usurious"[180] invites further controversies as to the breadth of this exception.

Leaving businesses to decide the value of a consumer's data and thereafter fabricating a non-exhaustive list of methodologies [181] that businesses may employ to compute this appraisal is dangerously imprudent. Moreover, a business that offers financial incentives that it believes are allowable and in harmony with the Act's requirements may unknowingly beget financial ramifications resulting from liability for noncompliance since the Act offers no guidance for defining "unjust, unreasonable, coercive, or usurious in nature"[182] in the context of permissible financial incentives. At the same time, consumers are in no position to appreciate whether they are making a "good deal." As it stands now, because of its ambiguous language and boundless exceptions, the danger of this

171. *See id*. § 1798.125(b)(2).

172. This "opt-in" consent clause requires explanation of material terms of the incentive program and must allow consumers the right to revoke their consent at any time. *Id*. § 1798.125(b)(3).

173. *See* CCPA, Cal. Civ. Code § 1798.125(b)(1) ("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.").

174. *See id.* § 1798.125(b)(4).

175. *See* Jessica B. Lee, *A Little Clarity, A Lot of Questions: An Analysis of the California AG's Proposed CCPA Regulations*, LOEB & LOEB. (Oct. 25, 2019), https://www.loeb.com/en/insights/publications/2019/10/an-analysis-of-the-california-ags-proposed-ccpa-regulations.

176. *See id.*

177. *See* CAL. CODE REGS. tit. 11, § 999.307(b)(5)(a).

178. *See id.* § 999.307(b)(5)(b).

179. *See* CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018).

180. *See id.* § 1798.125(b)(4).

181. *See* CAL. CODE REGS. tit. 11, § 999.337(a).

182. *See* CCPA, Cal. Civ. Code § 1798.125(b)(1) (2018).

provision[183] poses a serious risk to businesses because of the financial liability[184] imposed on businesses that violate the Act. Additionally, consumers "still don't know all the ways their information is being sold, traded, and shared,"[185] and therefore cannot know whether an offer is "unjust" or "coercive."[186] Thus, even if a business obtains consent before it enters a consumer into a financial incentive program, "[u]ntil consumers actually understand the ecosystem they've unwittingly become a part of, [they] won't be able to grapple with it in the first place."[187]

IV. SOLUTION

"*A valid consent presupposes that a data subject has fully understood the consequences of his or her approval*."[188]

A. VOID THE REASONABLE RELATIONSHIP EXCEPTION

The California legislature must void the reasonable-relationship exception detailed in section 1798.125(a)(2).[189] The variability in data value across different industries is too erratic and therefore, businesses that offer consumers a different price or provide an altered quality of service will be unable to formulate an alternative that would contemplate the inconsistent valuations ascribed to specific data and pass muster under the Act. For example, as noted by the California legislature, one factor that transforms the value provided by a consumer's data to the business is the "number of businesses in the market for data."[190] Additionally, the value assigned to the kind of information obtained is also highly subjective and often varies as "data brokers and data exchange centers are multiplying"[191] and thus, the number of professionals collecting and selling personal data continues to increase. For instance, general information about an individual, such as "age, sex, [or] locality" is typically worth less than personal data on a

183. *See generally id.* § 1798.125.

184. *See id*. § 1798.155(b) ("Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars for each violation or seven thousand five hundred dollars for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.").

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

186. *See* CCPA, Cal. Civ. Code § 1798.125(b)(4) (2018).

187. *Id*.

188. I. van Ooijen & Helena U. Vrabec, *Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective*, J. CONSUM. POL. 42: 91–107, at 100 (2019), https://doi.org/10.1007/s10603-018-9399-7.

189. CCPA, Cal. Civ. Code § 1798.125(a)(2) (2018).

190. *See* CA. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS, Section IV, at 38, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

191. *See* Pauline Glikman & Nicolas Glady, *What's The Value Of Your Data?*, TECHCRUNCH (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

consumer such as their interests in a specific service or product.[192] The capriciousness of appraising data and the co-dependency of its valuation on various factors like "who uses it, how it is being used, and in what context,"[193] renders compliance with this provision unattainable. Therefore, the exception must be voided as it is completely futile.

B. SUPPLEMENT THE FINANCIAL INCENTIVES EXCEPTION WITH MANDATED DISCLOSURES

With regard to the financial incentives exception described in section 1798.125(b)(1), [194] the California Attorney General must curtail the indeterminable and unbridled exception that allows businesses to offer compensatory payments to consumers. The restraints on businesses that decide to offer financial incentives to consumers in exchange for their data are insufficient since the Act provides no guidance on how to construe its limitations. Although section 1798.125(b)(4) attempts to delineate impermissible incentives by proscribing "financial incentive practices" that are "unjust, unreasonable, coercive, or usurious in nature,"[195] the California Attorney General must include additional requirements that enhance transparency from businesses to satisfactorily protect consumers from any potentially discriminatory practices.

While much of the opposition surrounding the financial incentives exception[196] stems from the impracticability of quantifying consumer data, further consideration is due concerning the tension between data privacy as right and data privacy as a commodity. Generally, consumers do not consciously register how retailers will subsequently profit from an email address or other personal information that individuals often share when signing up for loyalty programs or the like.[197] Nor do they immediately contemplate the "the possible security ramifications if the email address is obtained by a third party through a data breach."[198] In contrast to businesses collecting this data, consumers attribute value to their data by the sensitivity and breadth of the information being shared, and "expect more value in return for data used to target marketing, and the most value for data that will be sold to third parties."[199] Ultimately, consumers' willingness to give

192. *See id*.
193. *See id.*
194. CCPA, Cal. Civ. Code § 1798.125(b) (2018).
195. *Id*. § 1798.125(b)(4).
196. *See generally* CCPA, Cal. Civ. Code § 1798.125(b) (2018).
197. *See* Sam Sabin, *In Data-Driven World, Consumers Likely to Overestimate Their Information's Value*, MORNING CONSULT (June 3, 2019), https://morningconsult.com/2019/06/03/data-driven-world-consumers-likely-overestimate-their-informations-value/.
198. *See id*.
199. *See* Timothy Morey, Theodore Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARVARD BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

up their data to businesses in exchange for some return value turns on trust and transparency about use.[200] Yet, instead of operating from the vantage point of the consumer, the financial incentives exception provides a market-based solution for quantifying a monetary value for consumer data, and fails to provide transparency to consumers who lack the competency needed in order to transact in the data marketplace. While any financial incentive should be directly related to the value provided by the consumer's data,[201] businesses must also provide value in the form envisaged by consumers. This means increased disclosure and information that specifies exactly what will happen with their data when they hit, "I agree," in terms comprehensible to the average consumer. Even if businesses must now state how much your information is worth to them, without stricter requirements surrounding disclosure, consumers will not feel in control over their data and cannot provide knowing consent.

The legislative intent behind the CCPA was to enhance "Californians' right to privacy by giving consumers an effective way to control their personal information."[202] Accordingly, the regulations needed to clarify this provision should construe its terms in harmony with that intent. The exception must provide *consumers* greater control over their data and mandate that businesses articulate uniform practices to formulate these incentives which are clearly outlined from the start. If consumers comprehend how their data is used and what they earn in exchange for such use, they may be more willing to relinquish their information.[203] Hence, businesses fare better "if they offer consumers safety, security, and trust,"[204] while consumers get digestible answers concerning their information. By adding these requirements, the legislative intent of providing "California residents with greater transparency and control over how businesses collect and use their personal information,"[205] would also be promoted.

The CCPA has the potential to substantially alter the data marketplace. Therefore, California must be judicious in implementing any exceptions to these fundamental restrictions now imposed on businesses. Accordingly, to advance the intent behind the Act generally, the financial incentives exception [206] should survive since it attempts to transfer control over personal data back to its rightful owner—the consumer. Autonomy includes "the right to make decisions about oneself and one's life trajectories, which

200. *Id*.
201. *See* CCPA, Cal. Civ. Code § 1798.125(b)(1) (2018).
202. Assemb. Bill 375, 2017-2018 Reg. Sess., Ch. 55, Sec. 2(g) (Cal. 2018).
203. Jessica B. Lee, *The Value of Talking About the Value of Consumer Data*, ADMONSTERS (Aug. 13, 2020), https://www.admonsters.com/value-consumer-data/.
204. *See id.*
205. *See* Newman, *supra* note 114.
206. *See generally* CCPA, Cal. Civ. Code § 1798.125(b) (2018).

we call 'decisional privacy.'"[207] To promote consumer autonomy, the California Attorney General must produce additional regulations to the financial incentives exception[208] that limit the latitude afforded to businesses in constructing these incentive practices so as to clearly draw a "line separating persuasion from coercion"[209] in the context of permissible incentives.

CONCLUSION

To achieve architectural perfection in data privacy legislation, one must consider and untangle the surfeit of moving parts that go into building such laws. To promulgate effective data privacy legislation in the 21st century requires one to contemplate the benefits of "the proliferation of internet technology," [210] which has provided incomparable conveniences to consumers, as well as the concomitant privacy invasion that is achieved through the "tracking, storing, and sharing of what some consumers view as their private information."[211] In order to advance the legislative intent behind the CCPA and give consumers autonomy over their personal data, the California Attorney General should void the reasonable-relationship exception[212] since it fails to provide meaningful protection to consumers and offers a safe harbor for businesses exploiting their data. Additionally, the legislature must implement further restrictions that reframe the financial incentives exception to operate through the lens of a consumer, so that businesses are forced to provide comprehensible disclosures regarding their use of our data, rather than proffer arbitrary dollar amounts to justify its collection. This is needed not only to maintain the integrity of the Act, but also to promote genuine consumer autonomy over personal data.

Blaire Rose[*]

207. *See* Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J. L. & TECH. 106, 129–30 (2019).

208. *See generally* CCPA, Cal. Civ. Code § 1798.125(b) (2018).

209. *See* Manheim & Kaplan, *supra* note 207.

210. *See* J.H. Jennifer Lee, Kimberly B. Frumkin, Susan Tran & Nicolas Sanchez-Mandery, *Consumer Protection in the New Economy: Privacy Cases in E-Commerce Transactions or Social Media Activities*, 73 CONSUMER FIN. L. Q. REP. 6, 7 (2019).

211. *See id.*

212. *See* CCPA, Cal. Civ. Code § 1798.125(a)(2).

* J.D. Candidate, Brooklyn Law School, 2021; B.A. in Economics, Connecticut College, 2017. Many thanks to each and every staff member of the Brooklyn Journal of Corporate, Financial & Commercial Law who helped prepare this piece for publication. And thank you to anyone else who reads this Note.