Loyola of Los Angeles Law Review

Volume 56 | Number 2 Article 1

Spring 5-17-2023

Financial Incentives: The Fault in California's Privacy Framework

Hannah Donahue

FINANCIAL INCENTIVES: THE FAULT IN CALIFORNIA'S PRIVACY FRAMEWORK

Hannah Donahue∗

In 2018, California became the first state in the nation to enact comprehensive consumer data privacy legislation with its California Consumer Privacy Act. The law provides Californians with several rights regarding their consumer data, as well as a right not to be discriminated against for exercising any of those rights. The law, however, includes an exception by which businesses can offer financial incentives (i.e., differing prices, rates, or quality) if those incentives are correlated to the value provided by the consumer's data. In this way, the law offers consumers tools to control the collection and use of personal data and promises that consumers will not be discriminated against for using these tools, while simultaneously endorsing business schemes that entice consumers to give their data and punish those who do not. The exception also recklessly marries data valuation with data privacy.

This Article argues that the financial incentive exception creates a fundamental conflict within California's Privacy Framework, which cannot be reconciled with its promise to give consumers stronger privacy protection. Through an examination of the financial incentive exception, this Article offers critiques of data valuation in consumer privacy laws and presents recommendations for future privacy legislation. More fundamentally, this Article argues that data valuation in consumer privacy laws creates and exacerbates societal inequities and undermines consumer privacy.

∗ J.D., LMU Loyola Law School; B.A., University of California, Los Angeles; Associate Attorney in the Communications Practice Group, Davis Wright Tremaine LLP, Los Angeles. I would like to thank the outstanding editorial staff of the *Loyola of Los Angeles Law Review*, including Thomas Murtland, Willie Almack, and C.B. Rome, for their hard work, dedication, and leadership. My deepest gratitude goes to Associate Dean for Research and Professor of Law Lauren E. Willis for her indispensable guidance, editorial feedback, patience, and encouragement. I am grateful to my family and friends for surrounding me with unconditional love and support, and for reminding me of the importance of community. Finally, I thank my husband, Patrick, for doing all things, big and small, to help me pursue a career in law; you are the Marty to my Ruth.

TABLE OF CONTENTS

INTRODUCTION

For better or worse, data is the lifeblood of our modern economy. Consumers give their data to businesses in a variety of contexts, and businesses use that data in a variety of business operations: to improve the effectiveness of advertising through personalized messages; to inform the development of products and services; to facilitate efficient transactions; to resell as datasets or insights drawn from them; to inform pricing; to retain consumers and facilitate further data collection.[1] Fueled by advances in big data technology, our capacity to share, collect, process, and utilize data presents opportunities for tremendous growth.

More and more, legislators and their constituents are acknowledging that consumer data collection and use affects almost every American consumer and business. Several states are considering or have already passed consumer data privacy laws,[2] and federal lawmakers' appetites for comprehensive privacy legislation have grown significantly within recent months.[3]

California is a leader in consumer data protection lawmaking. The California Consumer Privacy Act of 2018, along with the accompanying regulations promulgated by the California attorney general (the "Attorney General's Regulations" or "Regulations"), and the California Privacy Rights Act of 2020[4] (collectively, the "California Privacy Framework" or "Framework") provide California consumers with four rights with regard to their data: (1) the right to know about the

1. Allan Stormon, *The 5 Forgotten Benefits of Consumer Data You Need to Know*, ORACLE ADVERT. BLOG (May 16, 2019), https://blogs.oracle.com/advertising/post/the-5-forgotten-benefits-of-consumer-data-you-need-to-know.

2. Anokhy Desai, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (Mar. 3, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/N4US-UDUT]; S.B. 21-190, 73d Gen. Assemb., 1st Reg. Sess. (Colo. 2021) (effective July 1, 2023); S.B. 6, 2022 Gen. Assemb., 2022 Reg. Sess. (Conn. 2022) (effective July 1, 2023); S.B. 227, 2022 Leg., 2022 Gen. Sess. (Utah 2022) (effective Dec. 31, 2023); VA. CODE ANN. §§ 59.1-575 to 59.1-585 (2022) (effective Jan. 1, 2023).

3. *See* MÜGE FAZLIOGLU, INT'L ASS'N OF PRIV. PROS., US FEDERAL PRIVACY LEGISLATION TRACKER 3, https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf [https://perma.cc/WDX6-ZZCV]; *see, e.g.*, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

4. In November of 2020, California voters passed Proposition 24, a ballot measure that amends the 2018 California Consumer Privacy Act (CCPA) to the California Privacy Rights Act (CPRA). The CPRA, which went into effect on January 1, 2023, establishes a new privacy enforcement agency, creates new definitions, and expands data security obligations, among other changes. Relevant comparisons and distinctions (and ambiguities) between the CCPA and the CPRA will be noted throughout this Article.

personal information covered businesses collect about a consumer[5] and how the information is used and shared;[6] (2) the right to request that businesses delete personal information collected from them;[7] (3) the right to opt out of the sale of their personal information;[8] and (4) the right to not be discriminated against for exercising these rights.[9] The animating principle of the California Privacy Framework is strengthening the state's constitutional right to privacy by giving California consumers tools to control their personal data.[10]

The last of the Framework's rights—the right of non-discrimination—runs headlong into a business practice predating the big data age: loyalty programs. Loyalty programs have existed since the late 1800s, beginning with stamps and evolving to include membership cards, frequent-flyer miles, discount codes, credit card cash-back and points rewards, grocery store rewards programs, and many other schemes across various industries.[11] These loyalty schemes "help firms identify the most valuable customers, improve customer retention, and enhance the efficiency of marketing communications."[12] Businesses offer consumers incentives to encourage increased brand loyalty and repeat purchases, for example. Traditionally, the aim of these programs was to "build stronger bonds with the sponsoring brand/firm than would result without such programs."[13]

Technology gives businesses an additional reason to employ loyalty programs: the facilitation of consumer data collection.[14] Many

5. A "consumer" is "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier." CPRA, CAL. CIV. CODE § 1798.140(g) (2020) (amending CCPA, CAL. CIV. CODE §§ 1798.100–.199 (2018)).

6. *Id.* §§ 1798.100, 1798.110, 1798.115.

7. *Id.* § 1798.105(a).

8. *Id.* § 1798.120.

9. *Id.* § 1798.125(a)(1).

10. Assemb. B. 375, 2017–2018 Leg., Reg. Sess. § 2(i) (Cal. 2018); *see also* CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining safety, happiness, and privacy.").

11. Russel Lacey & Julie Z. Sneath, *Customer Loyalty Programs: Are They Fair to Consumers?*, 23 J. CONSUMER MKTG. 458, 459 (2006); Byron Sharp & Anne Sharp, *Loyalty Programs and Their Impact on Repeat-Purchase Loyalty Patterns*, 14 INT'L J. RSCH. MKTG. 473, 473 (1997).

12. Valeria Stourm et al., *Refocusing Loyalty Programs in the Era of Big Data: A Societal Lens Paradigm*, 31 MKTG. LETTERS 405, 405 (2020).

13. Lacey & Sneath, *supra* note 11, at 459.

14. *See Internet Service Providers and Customer Privacy: Hearing on Assemb. B. 375 Before the S. Judiciary Comm.*, 2018 Leg., 2017–2018 Reg. Sess. 2 (Cal. 2018) [hereinafter *S. Judiciary Comm. B. Analysis*], https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375 [https://perma.cc/8ACM-TEJ3] (select "06/25/18 – Senate Judiciary" from menu) ("Consumers' Web browsing, online purchases, and involvement in loyalty programs also

modern incentive programs are operated through digital platforms, presenting businesses with greater capabilities to gather consumer data with which to personalize additional incentives,[15] and, importantly, to support hyper-targeted advertising.[16] Whether operated online or offline, loyalty programs are driven by big data.[17] Businesses combine consumer data collected through a loyalty program with other data they obtain, whether online or offline. For example, CVS Pharmacy explained in its 2021 privacy policy that CVS may combine information it collects from a consumer through its websites and mobile applications with information collected in stores to offer "content, advertisements, products, and services that are most likely to appeal" to that particular consumer.[18]

Continuing with this example, CVS Pharmacy operates a financial incentive program called ExtraCare.[19] Members receive ExtraBucks Rewards of two percent back on qualifying purchases, exclusive sale prices, and personalized deals.[20] Membership is "free," but members must provide personal information to become ExtraCare members.[21] Members who share their dates of birth also receive an annual birthday gift of three dollars in ExtraBucks Rewards.[22] On its

---

create a treasure trove of information on consumers. Advanced technologies and the use of sophisticated algorithms can create eerily effective profiling and targeted marketing.").

15. *See* Tiffany Hsu, *Why Rewards for Loyal Spenders Are 'a Honey Pot for Hackers,'* N.Y. TIMES (May 11, 2019), https://www.nytimes.com/2019/05/11/business/rewards-loyalty-program-fraud-security.html [https://perma.cc/99ER-J6ZL] ("But loyalty programs, as they shift from paper and plastic to apps and websites, are increasingly tracking a currency that can be more valuable than how much you spend: personal data.").

16. Nik Froehlich, *The Truth in User Privacy and Targeted Ads*, FORBES (Feb. 24, 2022, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2022/02/24/the-truth-in-user-privacy-and-targeted-ads/ [https://perma.cc/SJT7-A7EQ].

17. Stourm et al., *supra* note 12, at 406 ("The growth of [loyalty programs] and the increased availability and analysis of 'big data' are tied through a virtuous circle: Big data enable firms to make [loyalty programs] more effective, and [loyalty programs] are an ideal vehicle for collecting data such as purchase transactions that can in turn enhance the profitability of [loyalty programs] and other marketing actions. . . .").

18. CVS Privacy Policy, CVS (Sept. 16, 2021), https://www.cvs.com/help/privacy_policy.jsp [https://web.archive.org/web/20210917161407/https://www.cvs.com/help/privacy_policy.jsp].

19. CVS ExtraCare Homepage, CVS, https://www.cvs.com/extracare/home [https://perma.cc/4J8G-B2D7].

20. *CVS Pharmacy ExtraCare Program Terms*, CVS (Aug. 11, 2021), https://www.cvs.com/extracare-cvs/terms-conditions [https://perma.cc/JS4A-P99B].

21. CVS Privacy Policy, *supra* note 18 ("If you choose not to provide your personal information to us, we may not be able to provide you with requested products, services or information"); CVS Account Creation Page, CVS, https://www.cvs.com/account/creation?page=/account/signup.jsp [https://perma.cc/B9P5-V9PF] (during the sign-up process, a consumer must explicitly provide a full name, email address, and phone number).

22. *CVS Pharmacy ExtraCare Program Terms*, *supra* note 20.

face, CVS's ExtraCare program employs a discriminatory practice prohibited by the California Privacy Framework: CVS offers benefits to consumers who share personal data, but withholds benefits from consumers who do not.[23] California's Privacy Framework prohibits businesses from discriminating against consumers for exercising their data privacy rights:

> A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:
>
> (A) Denying goods or services to the consumer.
>
> (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
>
> (C) Providing a different level or quality of goods or services to the consumer.
>
> (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
>
> (E) Retaliating against an employee, applicant for employment, or independent contractor . . . for exercising their rights under this title.[24]

At the same time, the Framework provides that "[n]othing . . . 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."[25] Further, the Framework explicitly preserves businesses' uses of consumer loyalty programs that discriminate between consumers:

> A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention of personal information. A business may also offer a different price, rate, level, or quality of

23. CVS Privacy Policy, *supra* note 18 ("If you choose not to provide your personal information to us, we may not be able to provide you with requested products, services or information.").

24. CPRA, CAL. CIV. CODE § 1798.125 (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)).

25. *Id.*

> goods or services to the consumer if that price or difference is reasonably related to the value provided to the business by the consumer's data.[26]

The financial incentive exception creates a fundamental conflict within the California Privacy Framework that cannot be reconciled with the Framework's purposes. The Framework promises consumers stronger privacy protection by offering tools to control the collection and use of their personal data and promises that consumers will not be discriminated against for using these tools. At the same time, the exception endorses business schemes that entice consumers to give their data and punish those who do not. Further, the exception recklessly introduces data valuation into the Framework to justify this discriminatory practice.

This inconsistency did not go unnoticed. As the Senate Judiciary Committee observed, the financial incentive exception "could be read as an endorsement of pay-for-privacy type practices,"[27] creating an internal conflict with the law's purpose:

> Privacy is of such import to California that it is enshrined in the California Constitution as an inalienable right. (Cal. Const, art. I, Sec. 1.) Allowing for businesses to treat consumers differently on the basis of whether they forego exercising that right is problematic. These provisions arguably can contribute to the transformation of a constitutional right into a luxury product that is affordable by a select few, creating unequal access to privacy and further enabling predatory and discriminatory behavior. This is a constitutional right that the Legislature should not commodify lightly.[28]

Despite this fundamental conflict, the financial incentive exception survived efforts to remove it from the statute,[29] and loyalty programs were given a more explicit endorsement in the CPRA, which clarified that the non-discrimination right "does not prohibit a business

---

26. *Id.*; *Privacy, Personal Information, and Businesses: Informational Hearing on Assemb. B. 375 Before the Assemb. Comm. on Priv. & Consumer Prot.*, 2018 Leg., 2017–2018 Reg. Sess. 15–16 (Cal. 2018) [hereinafter *A.B. 375 Informational Hearing*], https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375 [https://perma.cc/8ACM-TEJ3] (select "06/27/18 – Assembly Privacy and Consumer Protection" from menu).

27. *S. Judiciary Comm. B. Analysis*, *supra* note 14, at 19.

28. *Id.*

29. *See, e.g.*, Assemb. B. 1760, 2019–2020 Leg., Reg. Sess. § 8 (Cal. 2019) (proposing amendments to the CCPA, including removing the exception from section 1798.125 completely).

from offering loyalty, rewards, premium features, discounts, or club card programs" so long as they are "reasonably related to the value provided to the business by the consumer's data."[30]

What, then, is "the value provided to the business by the consumer's data"? Can the value provided to a business by a consumer's data be calculated at the time of data collection? What is the difference in "price, rate, level, or quality of goods or services" to consumers who join loyalty programs and give their data to businesses versus consumers who exercise their data privacy rights?[31] How must businesses structure their loyalty programs to ensure that the difference in "price, rate, level, or quality of goods or services" is "reasonably related to the value provided to the business by the consumer's data"?[32] What are the effects of a privacy framework that allows data valuation, and, more fundamentally, should data valuation have a place in consumer privacy frameworks? Does data valuation enhance or inhibit consumers' ability to control their personal information?

This Article explores these questions and concludes that the Framework's financial incentive exception is practically unworkable. Further, the Article argues that the exception fatally undermines the non-discrimination right provided to California consumers and is contrary to the purpose of the law. The Framework places the burden on consumers to assess the risks and rewards of giving personal data based on the illusion of a reasonable valuation. Not only does this fail to give consumers greater control over their personal data, it gives businesses permission to discriminate if they can frame their valuation method in just the right way. It also incentivizes businesses to collect *more* data by which to refine these calculations and, more problematically, to target consumers with increased precision. These fundamental flaws in the Framework harm rather than empower consumers.

This Article begins with a brief history of the California Privacy Framework, describing the cultural and political context from which the financial incentive exception was born.[33] The California Privacy Framework's tumultuous development—from a thwarted ballot initiative, to legislative compromises and amendments, to another ballot

30. CPRA, CAL. CIV. CODE § 1798.125(a)(3), (b)(1) (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)).

31. *Id.* § 1798.125(b)(1).

32. *Id.*

33. *See* discussion *infra* Part I.

initiative—provides a useful backdrop for the subsequent analyses and recommendations.

Part II offers three critiques of data valuation, illustrated by the Framework's financial incentive exception. First, the Framework requires businesses offering financial incentives to calculate the value of the consumer's data, which falsely presumes the existence of reasonable methods for valuation.[34] As a result, businesses face tremendous challenges in conforming with the law, plaguing both compliance and enforcement efforts. Second, information asymmetries and cognitive burdens make it impossible for consumers to understand the terms of what they are agreeing to in a financial incentive transaction.[35] This dynamic disempowers consumers, contrary to the core purpose of the Framework. Third, treating data as a commodity that can be traded away in exchange for discounts and benefits leads to weaker privacy protection for vulnerable classes of consumers.[36]

Part III presents recommendations for amending the existing regulations and suggestions for privacy frameworks that protect, rather than undermine, the goals of ensuring meaningful consumer data privacy. It also cautions against other jurisdictions following California's lead. More fundamentally, this Article argues that data valuation in consumer privacy laws creates and exacerbates societal inequities and undermines any privacy laws' purposes.

I. THE CALIFORNIA PRIVACY FRAMEWORK: NON-DISCRIMINATION & FINANCIAL INCENTIVES

A. Development of the California Privacy Framework

The story of the California Privacy Framework's development deserves a dedicated treatise to fully capture the drama of the events and personalities involved.[37] For the purposes of this Article, California's consumer privacy story begins with a ballot initiative sponsored by an organization called Californians for Consumer Privacy. The purpose of the initiative, titled the "Consumer Right to Privacy Act of 2018," was "to further the constitutional right of privacy by giving

34. *See infra* Section II.A.

35. *See infra* Section II.B.

36. *See infra* Section II.C.

37. *See* Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [https://perma.cc/GGT8-U969] (explaining the early stages of the Framework's development).

consumers an effective way to control their personal information, thereby affording better protection for their own privacy and autonomy" by giving consumers certain rights and imposing certain requirements on businesses that collect personal information from consumers.[38]

With the hope of getting on the November 2018 ballot, Californians for Consumer Privacy filed the initiative in 2017 and began collecting signatures to qualify for the ballot.[39] They collected twice the number of required signatures by early spring of 2018.[40]

At this point, California lawmakers began negotiating with the organization to withdraw the initiative in favor of a legislative solution. There are at least two possible explanations for this intervention. One explanation is that changes to an initiative become very difficult once it formally qualifies for the ballot. Initiatives can only be amended or repealed by the Legislature through another measure presented to and passed by the voters.[41] Additionally, the initiative specified that amendments must be "consistent with and further the intent" of the initiative and must be approved by "seventy percent of the members of each house of the Legislature," signed by the Governor, and approved by voters.[42] Legislators wanted to avoid these high hurdles that would impede efforts to make any changes. Another reason for legislative intervention was that members of the Legislature had drafted privacy bills of their own.[43] One such bill was AB 375, introduced by Assemblymember Ed Chau. An earlier version of AB 375

38. CAL. ATT'Y GEN., INITIATIVE NO. 17-0039, CONSUMER RIGHT TO PRIVACY ACT OF 2018 § 3 (2017) [hereinafter INITIATIVE NO. 17-0039], https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf [https://perma.cc/7PE2-NEPC] (providing consumers with a right to know that businesses collect personal information and whether businesses sell or share that information; and requiring businesses to implement reasonable security measures to protect consumers' personal data).

39. *Id.*; *S. Judiciary Comm. B. Analysis*, *supra* note 14, at 3.

40. *See* CAL. SEC'Y OF STATE, CALIFORNIA GENERAL ELECTION: TEXT OF PROPOSED LAWS 42 (2020) [hereinafter PROPOSITION 24], https://vig.cdn.sos.ca.gov/2020/general/pdf/topl.pdf [https://perma.cc/C26V-GNJ3] ("[M]ore than 629,000 California voters signed petitions to qualify the California Consumer Privacy Act of 2018 for the ballot.").

41. CAL. CONST. art. II, § 10(c) ("The Legislature may amend or repeal an initiative statute by another statute that becomes effective only when approved by the electors unless the initiative statute permits amendment or repeal without the electors' approval.").

42. INITIATIVE NO. 17-0039, *supra* note 38, § 5(a).

43. *See*, *e.g.*, S.B. 1121, 2017–2018 Leg., Reg. Sess. (Cal. 2018) (introduced in February 2018 by Senator Bill Dodd in response to the 2017 Equifax data breach); Assemb. B. 1859, 2017–2018 Leg., Reg. Sess. (Cal. 2018) (introduced in 2018 by Assemblymember Ed Chau; requiring consumer credit reporting agencies to fix security vulnerabilities or be held liable for damages resulting from breaches).

would have implemented the Obama-era Federal Communications Commission's Broadband Privacy Rules, which never went into effect.[44] Though this effort to resurrect failed federal privacy protections ultimately fizzled, AB 375 was repurposed in June of 2018 as the legislative embodiment of the Californians for Consumer Privacy initiative. Californians for Consumer Privacy agreed to withdraw their initiative from the November 2018 ballot, and AB 375 became the California Consumer Privacy Act of 2018 (CCPA).[45] AB 375 was introduced on June 21; within seven days, it passed the Senate and Assembly and was signed into law by the Governor.[46] With minor technical revisions,[47] the CCPA became the nation's first comprehensive data privacy law, effective January 1, 2020.[48]

The California Attorney General, tasked with regulating and enforcing the CCPA, conducted rulemaking proceedings between October 2019 and August 2020.[49] The final regulations were approved on August 14, 2020, with amendments approved in March of 2021.[50]

Confusingly, even before the CCPA went into effect, Californians for Consumer Privacy filed another initiative, the California Privacy Rights and Enforcement Act, to appear on the November 2020 ballot.[51] In a statement, the organization's founder, Alastair Mactaggart, highlighted two developments since the CCPA's passage that prompted the new initiative: "First, some of the world's largest companies have actively and explicitly prioritized weakening the CCPA.

---

44. Kelly Ding, *Congress Rolls Back FCC Broadband ISP Privacy Rules*, JOLT DIG. (Apr. 4, 2017), https://jolt.law.harvard.edu/digest/congress-rolls-back-fcc-broadband-isp-privacy-rules [https://perma.cc/BUL3-H7PY] ("Congress has used its power under the Congressional Review Act (CRA) to block the new rules from taking effect, as well as prevent the FCC from passing similar regulations in the future.").

45. *S. Judiciary Comm. B. Analysis*, *supra* note 14, at 3, 8.

46. *AB-375 Privacy: personal information: businesses: Bill History*, CAL. LEGIS. INFO., https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180AB375 [https://perma.cc/N43F-85Z2].

47. A "clean-up" bill passed on September 23, 2018, made minor technical amendments to the CCPA to correct typos and other minor errors that the Legislature did not have time to address before AB 375's whirlwind passage. *See* S.B. 1121, 2017–2018 Leg., Reg. Sess. (Cal. 2018).

48. *See* Jeewon K. Serrato & Lawrence Wu, *Privacy, Pricing, and the Value of Consumer Data: The Complex Nature of the CCPA's Non-Discrimination Requirement*, 30 COMPETITION, Fall 2020, at 100, 100.

49. *CCPA Regulations*, CAL. ATT'Y GEN., https://oag.ca.gov/privacy/ccpa/regs [https://perma.cc/TRV4-JVQ2].

50. *Id.*

51. *A Letter from Alastair Mactaggart, Board Chair and Founder of Californians for Consumer Privacy*, CALIFORNIANS FOR CONSUMER PRIV. (Sept. 25, 2019) [hereinafter *Letter from Alastair Mactaggart*], https://www.caprivacy.org/a-letter-from-alastair-mactaggart-board-chair-and-founder-of-californians-for-consumer-privacy/ [https://perma.cc/93MK-8NH8].

Second, technological tools have evolved in ways that exploit a consumer's data with potentially dangerous consequences."[52] The new initiative would, among other things, create stronger protections for "sensitive personal information," impose transparency requirements around uses of automated decision-making and profiling, and establish a new agency—the California Privacy Protection Agency—to enforce the law and provide guidance to businesses and consumers.[53] Unlike the 2017 initiative, which would have made legislative modifications very difficult, the 2020 initiative allowed more flexibility for possible amendments:

> [The California Privacy Rights and Enforcement Act] would enshrine these rights by requiring that future amendments be in furtherance of the law, even though I am only setting the threshold to amend at a simple majority in the legislature. While amendments will be necessary given how technically complex and fast-moving this area is, this approach respects the role of the legislature while still providing substantial protections for Californians from attempts to weaken the law and their new human rights.[54]

The initiative ultimately qualified for the November 2020 ballot as Proposition 24 and was approved by California voters on November 3, 2020.[55] It is known as the California Privacy Rights Act (CPRA).

On March 17, 2021, Governor Gavin Newsom announced appointments for the new California Privacy Protection Agency's five-member board.[56] At the time of this writing, the agency is conducting formal rulemaking proceedings to implement the CPRA in 2023.[57]

Together, the CCPA, the CPRA, and the Attorney General's Regulations comprise the California Privacy Framework.

---

52. *Id.*

53. *Id.*

54. *Id.*

55. PROPOSITION 24, *supra* note 40, at 74; Sam Dean, *California Voters Approve Prop. 24, Ushering in New Rules for Online Privacy*, L.A. TIMES (Nov. 4, 2020, 10:43 AM), https://www.latimes.com/business/story/2020-11-03/2020-california-election-tracking-prop-24 [https://perma.cc/7JND-DKF2].

56. *California Officials Announce California Privacy Protection Agency Board Appointments*, CAL. STATE PORTAL (Mar. 17, 2021) [hereinafter *California Officials Announce CPPA Board Appointments*], https://www.gov.ca.gov/2021/03/17/california-officials-announce-california-privacy-protection-agency-board-appointments/ [https://perma.cc/2T9M-3HPH].

57. *California Consumer Privacy Act Regulations*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/regulations/consumer_privacy_act.html [https://perma.cc/MV4H-9NM7].

B. The Right to Non-Discrimination & the Financial Incentive Exception

The California Privacy Framework's non-discrimination right provides: "A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title . . . ."[58] This language was adapted from the 2017 initiative,[59] which framed non-discrimination as a right to equal service and price.[60] The Framework also closely follows the 2017 initiative's language in enumerating a non-exhaustive list of the types of practices that could be considered discriminatory:

> (A) Denying goods or services to the consumer.
> (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
> (C) Providing a different level or quality of goods or services to the consumer.
> (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
> (E) Retaliating against an employee, applicant for employment, or independent contractor . . . for exercising their rights under this title.[61]

58. CPRA, CAL. CIV. CODE § 1798.125(a)(1) (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)).

59. INITIATIVE NO. 17-0039, *supra* note 38, § 3 ("In enacting this Act, it is the purpose and intent of the people of the State of California to further the constitutional right of privacy by giving consumers an effective way to control their personal information, thereby affording better protection for their own privacy and autonomy, by . . . [p]reventing a business from denying, changing, or charging more for a service if a California consumer requests information about the business's collection or sale of the consumer's personal information, or refuses to allow the business to sell the consumer's personal information.").

60. *Id.* § 4.4 ("A business shall be prohibited from discriminating against a consumer because the consumer requested information pursuant to sections 1798.100 ['Right to Know What Personal Information is Being Collected'] or 1798.101 ['Right to Know Whether Personal Information is Sold or Disclosed and to Whom'], or because the consumer directed the business not to sell the consumer's personal information pursuant to section 1798.102 ['Right to Say No to Sale of Personal Information'], or because the consumer exercised the consumer's rights to enforce this Act . . . .").

61. CPRA, CAL. CIV. CODE § 1798.125(a)(1)(A)–(E) (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)); INITIATIVE NO. 17-0039, *supra* note 38, § 4.5.

The non-discrimination right is tempered by an exception that was not in the 2017 initiative. In the first draft of AB 375, an exception for financial incentives provided:

> Nothing in this [non-discrimination] 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.[62]

The CPRA is even more explicit, dedicating a new subsection to state that financial incentives are permitted:

> Nothing in this [non-discrimination] 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.[63]

The origin of this exception is unclear, but it appears to have been added as a concession for businesses concerned that the non-discrimination right would ban certain business practices. The legislative history explains that the exception was added as a compromise for "legitimate business practice concerns":

> The tradeoffs to address industry concerns and counterbalance the consumer rights added within this bill, include . . . authorization to engage in certain financial incentive programs, as specified, such as free subscription services in exchange for advertising where the value to the consumer is based on the consumer's data, as long as the financial incentive program is not unjust, unreasonable, coercive, or usurious and is directly related to the value provided to the consumer by the consumer's data . . . .[64]

62. Assemb. B. 375, 2017–2018 Leg., Reg. Sess. § 1798.125(a)(2) (Cal. 2018).

63. CPRA, CAL. CIV. CODE § 1798.125(a)(2) (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)).

64. *A.B. 375 Informational Hearing*, *supra* note 26, at 15–16. The language of the bill was amended after AB 375 was enacted to change "value to the consumer" to "value to the business," and to change "value provided to the consumer" to "value provided to the business." A.B. 1355, 2019–2020 Leg., Reg. Sess. (Cal. 2019).

As part of this compromise, the legislation incorporated heightened notice and consent requirements for businesses offering financial incentives[65]:

> (3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent . . . that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.
> (4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.[66]

The CPRA added a third provision to section 1798.125 to reassure businesses that certain types of practices are permitted within the exception: "This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title."[67] Under both the CCPA and the CPRA, the exception allows businesses to "offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention[68] of personal information."[69] Businesses may, without violating the non-discrimination right, "offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is *directly related* to the value provided to the consumer by the consumer's data."[70]

---

65. *A.B. 375 Informational Hearing*, *supra* note 26, at 17 ("[T]he bill subjects businesses that offer financial incentives to consumers to various notice requirements, and specifies that a business may enter into a consumer into a financial incentive program only if the consumer provides prior opt-in consent which clearly describes the material terms of the program and which may be revoked by the consumer at any time.").

66. CCPA, CAL. CIV. CODE § 1798.125(b)(3)–(4) (2018) (amended 2020). The CPRA adds clarifying language to subsection (b)(3): "If a consumer refuses to provide opt-in consent, then the business shall wait for at least 12 months before next requesting that the consumer provide opt-in consent, or as prescribed by regulations adopted pursuant to Section 1798.185." CPRA, CAL. CIV. CODE § 1798.125(b)(3) (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)).

67. *Id.* § 1798.125(a)(2)–(3).

68. The CCPA's language uses "deletion," not "retention." CCPA, CAL. CIV. CODE § 1798.125(b)(1) (2018) (amended 2020).

69. *Id.*; CPRA, CAL. CIV. CODE § 1798.125(b)(1) (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)).

70. CCPA, CAL. CIV. CODE § 1798.125(b)(1) (2018) (amended 2020) (emphasis added). The CPRA amends this allowance by requiring that the difference be "*reasonably related* to the value provided to the business by the consumer's data." CAL. CIV. CODE § 1798.125(b)(1) (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)) (emphasis added).

In its analysis of AB 375, the Senate Judiciary Committee highlighted the contradiction between the bill's non-discrimination right and the added financial incentive exception:

> Section 1798.125, where these anti-discrimination and incentive provisions reside, is internally inconsistent to a certain extent. It specifically prohibits "charging different prices or rates for goods or services." But, it also specifically authorizes in the following paragraph "charging a consumer a different price or rate." The same tension exists for "providing a different level or quality of goods or services." This is problematic in and of itself because it is vague as to exactly how a business can treat a consumer based solely on whether they have exercised their rights pursuant to the Act.[71]

In addition to the vagueness around how businesses can treat consumers, the analysis also noted that the exception "could be read as an endorsement of pay-for-privacy type practices."[72] Further, such an approach may conflict with California's Constitution:

> Privacy is of such import to California that it is enshrined in the California Constitution as an inalienable right. (Cal. Const, art. I, Sec. 1.) Allowing for businesses to treat consumers differently on the basis of whether they forego exercising that right is problematic. These provisions arguably can contribute to the transformation of a constitutional right into a luxury product that is affordable by a select few, creating unequal access to privacy and further enabling predatory and discriminatory behavior.[73]

Despite these concerns and the tension with the non-discrimination right, California lawmakers kept the financial incentive exception, and left to the Office of the Attorney General the task of reconciling these provisions in subsequent regulations.[74] The senate judiciary analysis advises that "strong regulations . . . are vital" to serve the function of ensuring that the anti-discrimination provision is not

71. *S. Judiciary Comm. B. Analysis*, *supra* note 14, at 19.

72. *Id.*

73. *Id.*

74. *A.B. 375 Informational Hearing*, *supra* note 26, at 17 ("Ultimately, the bill anticipates that the AG will develop regulations by the time it becomes operative regarding financial incentive offerings which presumably will help reconcile these provisions to prevent discriminatory pay for privacy regimes.").

undermined by the financial incentive exception.[75] Analysts also advised proceeding with caution with regard to the financial incentive exception: "This is a constitutional right that the Legislature should not commodify lightly."[76]

Section 1798.185 directs California's attorney general to "adopt regulations to further the purposes of [the CCPA], including establishing rules and guidelines regarding financial incentives." Pursuant to this directive, the Office of the Attorney General proposed regulations on October 11, 2019.[77] After several rounds of comments and modifications, the Regulations were finalized and became effective on August 14, 2020.[78] They were later amended on March 15, 2021.[79]

The Regulations provided definitions crucial to the non-discrimination right and the financial incentive exception:

> (j) "Financial incentive" means a program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information.
>
> . . . .
>
> (n) "Notice of financial incentive" means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.
>
> (o) "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, or sale of personal information, 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 related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.
>
> . . . .

75. *S. Judiciary Comm. B. Analysis*, *supra* note 14, at 22–23.

76. *Id.* at 19.

77. *CCPA Regulations*, CAL. ATT'Y GEN., https://oag.ca.gov/privacy/ccpa/regs [https://perma.cc/TRV4-JVQ2].

78. *Id.*

79. *Id.*

> (w) "Value of the consumer's data" means the value provided to the business by the consumer's data as calculated under section 7081.[80]

The Regulations also define "discriminatory practices"[81] and set out the differential treatment permitted under the exception.[82]

The Regulations reiterate that businesses offering "a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and section 7016."[83] The purpose of this notice is "to explain to the consumer the material terms of the financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate."[84] To that end, the notice must include certain information:

> (1) A succinct summary of the financial incentive or price or service difference offered;
> (2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;
> (3) How the consumer can opt-in to the financial incentive or price or service difference;
> (4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
> (5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:

80. CAL. CODE REGS. tit. 11, § 7001 (2022).

81. *Id.* § 7080(a) ("A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.").

82. *Id.* § 7080(b) ("A business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference.").

83. *Id.* § 7010(d).

84. *Id.* § 7016(a)(1).

> (A) A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and
> (B) A description of the method the business used to calculate the value of the consumer's data.[85]

The Regulations suggest several "reasonable and good faith method[s] for calculating the value of the consumer's data," including:

> (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.
> (2) The average value to the business of the sale, collection, or deletion of a consumer's data.
> (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.
> (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.
> (5) Expenses related to the sale, collection, or retention of consumers' personal information.
> (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.
> (7) Profit generated by the business from sale, collection, or retention of consumers' personal information.
> (8) Any other practical and reasonably reliable method of calculation used in good faith.[86]

Further, the Regulations provide four illustrations of the types of incentive schemes that would or would not be discriminatory.[87]

---

85. *Id.* § 7016(b)(1)–(5).
86. *Id.* § 7081(a).
87. *Id.* § 7080(d). The examples are as follows:

(1) *Example 1*: A music streaming business offers a free service as well as a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the $5-per-month payment is reasonably related to the value of the consumer's data to the business.

(2) *Example 2*: A clothing business offers a loyalty program whereby customers receive a $5-off coupon by email after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is

As of this writing, the newly established California Privacy Protection Agency (CPPA) is conducting formal rulemaking proceedings for the provisions of the CPRA that become effective on January 1, 2023.[88]

II. WHY DATA VALUATION HAS NO PLACE IN CONSUMER DATA PRIVACY LAWS

The California Privacy Framework prohibits businesses from discriminating against consumers who exercise their privacy rights, with one glaring exception: businesses can offer different prices or a different quality of service if the difference is "*reasonably related* to the value provided to the business by the consumer's data."[89] Knowing whether the relationship is "reasonably related" to the value of "the consumer's data" necessarily requires that businesses determine the specific value of each consumer's data. The Framework then requires consumers to understand the value of what the business is offering, know the costs to themselves of allowing the business to use the data, and then determine whether their loss of privacy is worth what the business is offering.

---

reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).

(3) *Example 3*: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

(4) *Example 4:* An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

Id.

88. *See California Consumer Privacy Act Regulations*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/regulations/consumer_privacy_act.html [https://perma.cc/MV4H-9NM7].

89. CPRA, CAL. CIV. CODE § 1798.125(b)(1) (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)) (emphasis added).

This section provides three critiques of the Framework's financial incentives exception and of the valuation scheme it establishes. First, calculating—or even reasonably approximating—the value of a consumer's data to a business may not be possible.[90] Second, consumers cannot make an informed decision about the deal the business is offering. They cannot reasonably assess the value to them of the benefits the business is offering in exchange for their data. They cannot fairly assess the costs (net of any benefits) and risks of sharing their own data with the business. And consumers cannot rationally weigh the benefits offered against the costs they will incur; studies repeatedly point to consumer inability to make rational decisions in the privacy context.[91] Third, the Framework's valuation scheme facilitates commercial practices that perpetuate inequality.[92] Using data valuation to justify discrimination is inconsistent with the California Privacy Framework's purposes.

A. Business-Side Valuation: Impracticable & Volatile

The California Privacy Framework requires that financial incentives be "reasonably related to the value provided to the business by the consumer's data,"[93] and delegates to businesses the task of assigning value to consumers' data[94]—a task that may be impracticable. Businesses must "use and document a reasonable and good faith method for calculating the value of the consumer's data."[95]

This valuation exercise is unsubstantiated and impracticable because no one has come up with a way to calculate the value to a business of a single consumer's data. Several empirical studies have endeavored to identify precise monetary values for consumers' privacy preferences, with widely varying results.[96] Paradoxically, the Attorney

90. *See infra* Section II.A.
91. *See infra* Section II.B.
92. *See infra* Section II.C.
93. CCPA, CAL. CIV. CODE § 1798.125(b)(1) (2018) (amended 2020).
94. CAL. CODE REGS. tit. 11, § 7081(a) (2022).
95. *Id.* § 7081(a).
96. *See* Bjoern Roeber et al., *Personal Data: How Context Shapes Consumers' Data Sharing with Organizations from Various Sectors*, 25 ELEC. MKTS. 95, 96 (2015) ("Hann et al. (2003) find valuation of privacy ranges from 30.49 US Dollar to 44.62 US Dollar per month based upon their investigation of website privacy. Krasnova, Günther and Hildebrand (2009) conducted a conjoint analysis with regard to privacy in online social networks and conclude that on average users are willing to pay between 14.14 Euro and 17.24 Euro a year for a more privacy friendly [sic] of the online social network. In contrast, Bughin (2011) reports an average valuation of privacy of just 4 Euro per month, based upon surveys conducted in the US, Germany, France and UK. Bauer et al. (2012) find the median value of all one's Facebook data is even zero."); Alessandro Acquisti et al.,

General's Office acknowledged this uncertainty when it issued its initial proposed regulations in October 2019:

> Studies have found that there is not a single generally accepted methodology for calculating the value of a consumer's data, whether to a business or to a consumer. One study found that the majority of the 36 companies that they studied with annual revenue over $1 billion did not have formal data valuation practices and that "there is no formula for placing a precise price tag on data." . . . Another study found that the number of businesses in the market for data significantly affects the value of consumers' data to businesses.[97]

Despite the unsettled nature of consumer data valuation, the Regulations place businesses in the position of determining these values. To that end, the Regulations provide eight valuation methods—including one catchall provision for "[a]ny other practical and reasonably reliable method of calculation used in good faith"—and leave to businesses the decision of which method or combination of methods to use.[98] The acceptable calculation methods are:

The Economics of Privacy, 54 J. ECON. LIT. 442, 478 (2015) ("Olejnik, Minh-Dung, and Castelluccia (2014) find that elements of users' browsing histories are being traded among Internet advertising companies for amounts lower than $0.0005 per person. Hann et al. (2007) quantify the value that US subjects assign to protection against errors, improper access, and secondary uses of personal information online to an amount between $30.49 and $44.62. Similarly, Savage and Waldman (2013) find that consumers may be willing to make a one-time payment of $2.28 to conceal their browser history, $4.05 to conceal their contacts list, $1.19 to conceal their location, $1.75 to conceal their phones identification number, $3.58 to conceal the contents of their text messages, and $2.12 to eliminate advertising. . . . [I]n a lab experiment, Tsai et al. (2011) find that a substantial proportion of participants were willing to pay a premium (roughly half a dollar, for products costing about $15) to purchase goods from merchants with more protective privacy policies; Jentzsch, Preibusch, and Harasser (2012) find that (only) a third of participants were willing to pay a similar premium to purchase cinema tickets from a merchant that requests less personal information than a competing, but cheaper, merchant; and Preibusch, Kubier, and Beresford (2013) find that a vast majority of participants chose to buy a DVD from a cheaper but more privacy-invasive merchant, than from a costlier (1 euro more) but less invasive merchant. In fact, behavioral and cognitive heuristics may also play a significant role in affecting privacy valuations.").

97. CAL. ATT'Y GEN., INITIAL STATEMENT OF REASONS (ISOR): PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS 38 (2019) [hereinafter OAG INITIAL STATEMENT OF REASONS], https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf [https://perma.cc/J3CZ-QJVT] (first quoting James E. Short & Steve Todd, *What's Your Data Worth?*, 58 MIT SLOAN MGMT. REV. 16, 17–18 (2017); then citing Rodrigo Montes et al., *The Value of Personal Information in Markets with Endogenous Privacy*, CTR. FOR ECON. & INT'L STUD. TOR VERGATA, Aug. 2015, at 1, 18–19).

98. CAL. CODE REGS. tit. 11, § 7081(a)(8) (2022).

(1) The marginal value to the *business* of the sale, collection, or deletion of a consumer's data.
(2) The average value to the *business* of the sale, collection, or deletion of a consumer's data.
(3) The aggregate value to the *business* of the sale, collection, or deletion of consumers' data divided by the total number of consumers.
(4) Revenue generated by the *business* from sale, collection, or retention of consumers' personal information.
(5) Expenses related to the sale, collection, or retention of consumers' personal information.
(6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.
(7) Profit generated by the *business* from sale, collection, or retention of consumers' personal information.
(8) Any other practical and reasonably reliable method of calculation used in good faith.[99]

The language of both the statute and the Regulations make clear that businesses, not consumers, are the price-setting party.[100] Section 7081 of the Regulations sets the standard for valuing a consumer's data as "the value provided to the business by the consumer's data."[101] The Regulations prescribe that this should be "an objective calculation . . . as opposed to a consumer's subjective estimation of the value of their data."[102] The legislative history is silent on the rationale for this choice.

Businesses face many challenges in applying any method of valuation due to the complex nature of consumer data markets. The endeavor is fraught with complexities that lead to commercial and regulatory uncertainty—a concern which businesses will likely raise[103]—

99. *Id.* § 7081(a)(1)–(8) (emphasis added).

100. *See* CCPA, CAL. CIV. CODE § 1798.125(b) (2018) (amended 2020). The first three methods use "value to the business" as the basis for valuing consumer data. CAL. CODE REGS. tit. 11, § 7081(a)(1)–(3) (2022). Two methods base the value of consumer data on the revenue or profit generated by the business from uses of those data. *Id.* § 7081(a)(4), (7). And two methods base the value of consumer data on the expenses incurred by the business to sell, collect, or retain consumer data or to offer financial incentive programs. *Id.* § 7081(a)(5)–(6).

101. OAG INITIAL STATEMENT OF REASONS, *supra* note 97, at 38; CAL. CODE REGS. tit. 11, § 7081 (2022).

102. *Id.*

103. Allison Grande, *Do Calif. AG's New Regs Exceed Scope of Privacy Law?*, LAW360 (Dec. 2, 2019), https://plus.lexis.com/api/permalink/fc9e5dd6-df15-43fc-bbc3-dcfb361c6335/

and that expose some of the fundamental flaws in commodifying consumer data privacy. The value of consumer data is inherently elusive and difficult to pin down, presenting businesses with considerable challenges in the valuation endeavor.

Assigning monetary value to a consumer's data, ex ante, presents many problems. As with any medium of exchange, consumer data must have some recognized value among the parties to the transaction; the recognized value can be based on intrinsic factors or external factors.[104] Data are similar to many resources in that their value "is not predetermined or fixed, but a function of supply and demand. It derives from organizations' willingness to collect or purchase data, which itself fluctuates over time depending on the utility of the data to the organization, and individuals' willingness to supply data."[105] Within this dynamic, determining the monetary value of consumer data is difficult because these data are non-fungible and lack intrinsic monetary value.[106] Data value is volatile.[107] Value can change depending on a business's "willingness to collect or purchase data, which itself fluctuates over time depending on the utility of the data to the organization, and individuals' willingness to supply data."[108] Relatedly, the number of businesses in the market for consumer data can influence the valuation.[109] Time and context also affect consumer data value.[110]

("Companies are likely to voice their reservations with this setup, given the complexity involved with putting a good-faith estimate on the value of consumers' data and the difficulty with uniformly applying across industries one type of formula.").

104. Magali Eben, *Market Definition and Free Online Services: The Prospect of Personal Data as Price*, 14 I/S: J.L. & POL'Y FOR INFO. SOC'Y 227, 243–44 (2018).

105. Noam Kolt, *Return on Data: Personalizing Consumer Guidance in Data Exchanges*, 38 YALE L. & POL'Y REV. 77, 90–91 (2019).

106. *Id.* at 90; *see also* Peter Leonard, *Beyond Data Privacy: Data "Ownership" and Regulation of Data-Driven Business*, SCITECH LAW., Winter 2020, at 10, 14.

107. *Id.* ("Markets for outputs of data are volatile and unpredictable. Refined (real) oil can be stockpiled, whereas much data is time sensitive and rapidly loses value.").

108. Kolt, *supra* note 105, at 90–91.

109. Blair Rose, Note, *The Commodification of Personal Data and the Road to Consumer Autonomy Through the CCPA*, 15 BROOK. J. CORP., FIN. & COM. L. 521, 539 (2021) ("[A]s 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.' 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' and thus, the number of professionals collecting and selling personal data continues to increase.").

110. Kolt, *supra* note 105, at 91 ("Data, like raw materials, are a valuable commodity. Their value is context-dependent and time-sensitive."); *see also* Acquisti et al., *supra* note 96, at 446 ("The value of information will change over time (an online advertiser may not be as interested in logs of your online activity from five years ago as in your activity right now)."); Short & Todd,

In addition, the costs of administering financial incentive programs likely affect the value calculation. While some of these costs are foreseeable (e.g., data storage costs), other costs of data collection are harder to predict.[111] For example, the costs of maintaining reasonable security change as new threats arise and industry standards adjust to address them.[112] The costs of responding to and recovering from a data security incident involving consumer data is also nearly impossible to predict.[113] The potential costs of legal liability may factor into the valuation as well.[114]

Two variables—how much the business uses the consumer's data and the value of the consumer's data when combined with other data sources—have significant impacts on data value and are very hard to quantify prospectively. "[D]ata has the potential . . . to increase in value the more it is used. . . . [D]ata viewed as an asset can exhibit increasing returns to use."[115] And the value of the consumer's data typically arises after the data is aggregated with many other data points such that businesses can create meaningful segments to target with personalized advertising or sell to data brokers.[116]

The Framework's approach to valuation is misaligned with the many challenges that businesses face in complying with the financial incentive exception's "reasonably related" requirement. Unsurprisingly, many businesses have voiced concern about the law's impracticability and the uncertainty it creates. One public comment responding to the Office of the Attorney General's proposed regulations illustrates the complications of the Framework's valuation scheme:

> The language requiring businesses to calculate and disclose the value of a consumer's personal information

supra note 97, at 18 ("Data value may change over time in response to new priorities, litigation, or regulations. These factors are all relevant and difficult to quantify.").

111. *See* Sarah Spiekermann et al., *The Challenges of Personal Data Markets and Privacy*, 25 ELEC. MKTS. 161, 162 (2015); Short & Todd, *supra* note 97, at 18 ("The major costs of data are in its capture, storage, and maintenance.").

112. *See* Spiekermann et al., *supra* note 111, at 162.

113. *Id.*

114. *Id.* at 161–62.

115. Short & Todd, *supra* note 97, at 18.

116. *See* Kolt, *supra* note 105, at 90–91; Hayley Tsukayama, *Why Getting Paid for Your Data Is a Bad Deal*, ELEC. FRONTIER FOUND. (Oct. 26, 2020), https://www.eff.org/deeplinks/2020/10/why-getting-paid-your-data-bad-deal [https://perma.cc/345B-6WGL] ("[A]ny valuation that focuses solely on individualized data, to the exclusion of aggregate data, will be woefully inadequate. This is another reason why individuals aren't well-positioned to advocate for good prices for themselves.").

> incorrectly presumes each piece of personal information collected from a consumer has an inherent and fixed value to the business, which is especially untrue for startups still iterating on their products and establishing their business models. For instance, a startup website that offers a subscription service for cooking videos may offer users a discounted subscription in exchange for data on whether each user makes it to the end of the cooking video to see an ad for a cookbook. The startup website can have no way to determine a consistent, set value for the user's personal information as it relates to the discount in the subscription price.[117]

Another commenter called the Framework's valuation requirement "a fraught exercise."[118]

Whether a financial incentive is "reasonably related to the value of the consumer's data"[119] will likely change with any slight shift in the variables discussed in this section.[120] Businesses have little certainty about their compliance with the Framework's requirements and may opt for vague notices that do not serve the purpose of informing consumers of "unjust, unreasonable, coercive, or usurious" financial incentives.[121] These vague notices do not provide consumers with the

117. CAL. ATT'Y GEN., PUBLIC COMMENTS ON CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS: 45-DAY WRITTEN COMMENTS 963 (2019) [hereinafter PUBLIC COMMENTS TO THE OAG], https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf.

118. *Id.* at 1248–50 (explaining that businesses must choose between several arbitrary methods to calculate the potential value of consumers' data, with results that are ultimately meaningless with regard to any particular consumer's data).

119. CAL. CODE REGS. tit. 11, § 7016(b)(5) (2022).

120. *See supra* notes 108–118 and accompanying text.

121. *See* CCPA, CAL. CIV. CODE § 1798.125(b)(4) (2018) (amended 2020); Rose, *supra* note 109, at 538; *see, e.g.*, *Target Privacy Policy*, TARGET (July 1, 2022), https://www.target.com/c/target-privacy-policy/-/N-4sr7p?Nao=0#CACPA [https://perma.cc/BKR9-LZD9] ("Under the CCPA, Target Circle is considered a Financial Incentive Program. In order to provide you with the incentives described above, we use personal information about you including your name, phone number, email address, purchase history, birthdate, etc. to identify you as a member of the program and provide you with relevant messaging, experiences[,] and deals. These financial incentives are reasonably related to the value of the data you provide. . . . The expenses associated with the program incentives will vary as it is dependent on your engagement with the loyalty program, including total annual spend at Target and frequency and depth of discounts you choose to use."); *Your Rights and Choices*, KROGER CO., https://www.kroger.com/i/privacy-policy/rights-and-choices (last visited Oct. 18, 2022) ("In determining the value of this data to Kroger, we consider the profit generated from the solutions or products that include personal information (as defined by CCPA), which is reasonably correlated to the value provided to the consumer through personalized coupons, promotions, and other discounts or offers. . . . These programs are valuable to us to understand what matters to you, our customer. These allow us to deliver relevant value to our customers. As part of our Loyalty program, our best customers currently save $699 per year on average.").

information necessary to make rational privacy decisions, as discussed in the following section.

B. Consumer-Side Valuation: Opaque & Unreasonable

The California Privacy Framework's financial incentive exception depends upon consumers being able to assess the value of what the business is offering and any risks and costs that will flow from the sharing of their data, and then compare the two. Each consumer must engage in a personal evaluation of the costs and benefits of sharing or withholding their data. Although this calculus is different from the "reasonably related" evaluation required of businesses under the Framework, it suffers similar defects. The Framework does not equip consumers with the information and sophistication they would need to conduct these assessments and cost-benefit calculations so they might intelligently exercise the privacy choices afforded to them under the law.

Consumers, left on their own, face several challenges that prevent them from making reasoned privacy decisions in this context. The first challenge is an asymmetry of information. Consumers do not have access to information to evaluate the "privacy value to privacy cost" tradeoff. The first part of this section describes the information asymmetries that exist in the data economy, illustrating the chasm between business and consumer knowledge.

The second challenge is that consumers are limited, cognitively and practically, from making rational privacy decisions. The individual costs of assessing each data transaction to make rationally and practically sound decisions would be enormous and would require a level of expertise that is unrealistic to expect from consumers. The second part of this section explores the cognitive and practical burdens that consumers bear when transacting in the data economy.

1. Information Asymmetries: Consumers See Only a Portion of the Data Privacy Ecosystem

Information asymmetries prevent consumers from fairly assessing the risks they face when businesses use their data. Generally, consumers do not understand the data marketplace. A recent poll found that "[o]nly 6% of adults say they understand a great deal what

companies do with the data collected."[122] This lack of consumer understanding "leads to a data market in which one set of parties does not even know that negotiation is taking place."[123] Consumers have incomplete information with which to make decisions about what businesses can and will do with their data and how business uses will impact them in the future. This prevents consumers from fairly assessing privacy value in relation to risks. Ironically, non-transparency is also part of what makes the data business valuable.[124]

The Framework proposes to remedy this asymmetry by giving consumers rights to know what data are collected and how these data are used in relation to the offered financial incentive. Businesses that operate financial incentive programs are required to provide consumers with a "succinct summary of the financial incentive or price or service difference offered" and a "description of the material terms, including the categories of personal information that are implicated by the financial incentive or price or service difference."[125] Businesses must also provide an "explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data."[126] However, these notices are far too vague to equip consumers with the information and background knowledge needed to make an informed choice about their privacy rights.

For example, CVS's Privacy Policy contains the following financial incentive notice for its ExtraCare loyalty program:

---

122. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/9MB2-B62E].

123. Sarah Spiekermann & Jana Korunovska, *Towards a Value Theory for Personal Data*, 32 J. INFO. TECH. 62, 64 (2017) (quoting Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2078 (2004)).

124. MARK BARTHOLOMEW, ADCREEP: THE CASE AGAINST MODERN MARKETING 71 (2017) ("The covert nature of today's market research (in addition to its sheer size and detail) is what makes it so valuable.").

125. CAL. CODE REGS. tit. 11, § 7016(b)(1)–(2) (2022); *see also* CPRA, CAL. CIV. CODE § 1798.125(b)(2) (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018) ("A business that offers any financial incentives pursuant to [section 1798.125(b)(2)] shall notify consumers of the financial incentives pursuant to Section 1798.130."); *id.* § 1798.130(a)(5)(A) (Businesses are required to "[d]isclose the following information in its online privacy policy or policies . . . and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website, and update that information at least once every 12 months: [a] description of consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125").

126. CAL. CODE REGS. tit. 11, § 7016(b)(5) (2022).

> We offer ExtraBucks and other exclusive incentives for purchasing certain volumes and dollar amounts of products. To offer these discounts, we must track your personal information, such as purchase history and other demographic data. The value we place on the personal information in connection with these incentives is calculated by determining the approximate additional spending per customer, per year compared to individuals who are not enrolled in ExtraCare.[127]

The dollar value of the benefits the consumer will receive is impossible to determine from this language. In addition to the financial incentive notice, the CVS Privacy Policy lists ten categories of information it may collect from consumers, such as "Identifiers" (e.g., an "Internet Protocol ('IP') address," a "MAC address," or "other similar identifiers"); "Biometric information" (e.g., "facial scans" and "voice recognition information"); and "Geolocation Data" (e.g., location information based on GPS data, an IP address, or cellular network).[128] The Privacy Policy states that CVS may use consumer data for twelve general purposes, such as "[i]nternal analytics," "[m]arketing products and services," and "[a]ssessing third party vendors / service providers."[129] Despite these notices, it seems unlikely that consumers would understand all of these categories of data, how they might be used to achieve the purposes listed, and what risks or costs, if any, they will incur from these categories of information being used for these purposes.

The CVS Privacy Policy further states that CVS "do[es] not *sell* personal information or otherwise provide personal information to third parties, other than service providers receiving information to perform services for us on our behalf."[130] Within the same section, CVS states that it does, however, "share" personal information to, for example, "enhance [CVS's] ability to communicate with" and

127. CVS Privacy Policy, *supra* note 18.

128. *Id.*

129. *Id.* ("We may collect or use personal information from you for the following purposes: Internal analytics; Assessing third party vendors / service providers; Audit, compliance, policy, procedures, or regulation; Billing, payment, and fulfillment; Customer claims and fraud investigation and prevention; Customer communications; Customer relationship management; General business administration; Marketing products and services; Financial reporting and accounting; Website optimization and maintenance; Systems and data security.").

130. *Id.*

"provide . . . promotional information" to the consumer.[131] The Privacy Policy further explains that it may "share" personal information with third parties, including "[a]ffiliates," "[a]dvertising and marketing companies," "[s]ocial media companies," and "[t]echnology companies."[132] Nothing explains the uses to which these "third parties" might put the consumer's personal data.

In the unlikely event that consumers read these notices,[133] most consumers do not possess the background knowledge needed to decode them. For example, consumers likely do not understand what a "MAC address" is or that it uniquely identifies their device, allowing businesses to track them within a store and immediately offer tailored messages.[134] Consumers also do not understand the distinction between "selling" and "disclosing,"[135] and thus would likely be unable to discern the relationships between CVS and "[s]ocial media companies" or "[a]ffiliates."

131. *Id.*

132. *Id.*

133. *See* Auxier et al., *supra* note 122 ("[O]nly about one-in-five adults overall say they always (9%) or often (13%) read a company's privacy policy before agreeing to it. Some 38% of all adults maintain they sometimes read such policies, but 36% say they never read a company's privacy policy before agreeing to it.").

134. *Definition of MAC Address*, PC MAG., https://www.pcmag.com/encyclopedia/term/mac-address [https://perma.cc/XN84-TB7C] ("(Media Access Control address) The unique 48-bit serial number in the network circuitry of every Ethernet and Wi-Fi device. The MAC address, which holds 256 trillion unique numbers, identifies that device from every other globally. Also used in earlier Token Ring networks, the ID is assigned to vendors by the IEEE and "burned into" the network circuit at the time of manufacture."); *see* Chris J. Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy* Homo Economicus, 49 WAKE FOREST L. REV. 261, 293–95 (2014). *Cf.* JOSEPH TUROW, ANNENBERG PUB. POL'Y CTR. UNIV. PA., AMERICANS & ONLINE PRIVACY: THE SYSTEM IS BROKEN 3 (2003), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1411&context=asc_papers [https://perma.cc/X3HJ-JFYH] ("The study is also the first to provide evidence that the overwhelming majority of U.S. adults who use the internet at home have no clue about data flows—the invisible, cutting edge techniques whereby online organizations extract, manipulate, append, profile and share information about them. Even if they have a sense that sites track them and collect individual bits of their data, they simply don't fathom how those bits can be used.").

135. *See* CPRA, CAL. CIV. CODE § 1798.140(ad)(1) (2020) (amending CCPA, CAL. CIV. CODE § 1798.140 (2018)) ("'Sell,' 'selling,' 'sale,' or 'sold,' means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration."); *id.* § 1798.140(ah)(1) ("'Share,' 'shared,' or 'sharing' means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.").

Notices do not provide consumers with enough information to fully appreciate the real-world consequences of sharing personal data with businesses. Consumers have little visibility into how data are used beyond the initial exchange.[136] This makes it impossible for consumers to make informed choices.[137] For example, consumers are likely unaware that businesses use "geolocation data" or "CPU ID and type, build, model, manufacturer" to determine which prices are offered to them, which may differ from prices offered to other consumers.[138] Consumers also would not expect that their real-time location data, which a business may share with "advertising and marketing companies," might then be sold to bounty hunters, creditors, and landlords,[139] or that it might be used to identify persons visiting abortion clinics to target them with anti-choice marketing in real time.[140]

---

136. Kolt, *supra* note 105, at 80 ("At present, individual consumers cannot assess precisely how much personal data they pay for the services they receive. Nor can they assess the specific utility they gain in return for the data they supply. . . . [*T*]*he relationship between the data price consumers pay and the benefits they receive*—is unknown.").

137. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1397 (2000) ("In reality, individuals face enormous difficulty assessing how their personal information will be used. The decision about how much information a privacy policy should provide is hotly contested. The problem is especially acute for secondary and tertiary uses of personally[]identified information. Routine practice is to specify these classes of recipients only in the most general terms. Yet without information about the nature and identity of secondary and tertiary users, individuals cannot easily determine what information to provide or withhold.").

138. *See, e.g.*, Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012, 12:01 AM), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534 [https://perma.cc/63QY-QQ9L] (revealing that Staples, Office Depot, Discover Financial Services, Rosetta Stone, and Home Depot were "consistently adjusting prices and displaying different product offers based on a range of characteristics that could be discovered about the user," including geolocation and browsing history); Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J. (Aug. 23, 2012, 6:07 PM), https://www.wsj.com/articles/SB10001424052702304458604577488822667325882 [https://perma.cc/JNC5-V6C7] (reporting that Orbitz presented higher hotel prices to users of Mac computers after finding that "Mac users on average spend $20 to $30 more a night on hotels than their PC counterparts" and "are 40% more likely to book a four- or five-star hotel than PC users").

139. Maria Dinzeo, *Class Claims AT&T Sold Their Real-Time Locations to Bounty Hunters*, COURTHOUSE NEWS SERV. (July 16, 2019), https://www.courthousenews.com/class-claims-att-sold-their-real-time-locations-to-bounty-hunters/ [https://perma.cc/Z56N-49VU]; *see also* Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, VICE (Jan. 8, 2019, 9:08 AM), https://www.vice.com/en/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile [https://perma.cc/G564-SCPA] (detailing the under-the-table process that bounty hunters use to geolocate mobile phones); Joseph Cox, *Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years*, VICE (Feb. 6, 2019, 2:10 PM), https://www.vice.com/en/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years [https://perma.cc/R8XQ-RPRM] ("Around 250 bounty hunters and related businesses had access to AT&T, T-Mobile, and Sprint customer location data.").

140. Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022, 9:46 AM), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood [https://perma.cc/BXP3-B5DT].

Information asymmetries are particularly troublesome in the data valuation context because for many businesses, value comes not from the consumer's initial disclosure of personal information but from secondary and aggregate uses of consumer data.[141] It is a common practice for businesses to combine data collected from consumers with many other data sources and use analytics tools to sort through the data looking for patterns and making predictions about consumers' future behaviors.[142] Advances in big data analytics and computing power give businesses the capacity to "assemble these seemingly innocent and insignificant facts into a comprehensive personal profile" from which the business can more effectively target future messages or "use[] for purposes other than those for which it was intended."[143]

In this way, data aggregation obscures consumers' capacity to understand the prolonged implications of sharing data in a single transaction.[144] While consumers may be aware that businesses collect certain data points in the exchange, they have no visibility into how their data are combined with other data points—about them and about other consumers—in ways that benefit the business.[145] And privacy notices cannot provide consumers with sufficient information to understand and evaluate future uses:

> The types of new information that can be gleaned from analyzing existing information and the kinds of predictions that can be made from this data are far too vast and complex, and are evolving too quickly, for people to fully assess the risks and benefits involved. This state of affairs makes it very hard to assess whether revealing any piece of information will

141. *See* Shaun B. Spencer, *Privacy and Predictive Analytics in E-Commerce*, 49 NEW ENG. L. REV. 629, 639–40 (2015) (citing VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 118–20 (2013)) ("The data valuation challenge arises because most of data's value lies in unknown future secondary uses, rather than the original purpose of collection.").

142. *See* BARTHOLOMEW, *supra* note 124, at 70 ("Consumers may not think they are disclosing much personal information in individual transactions, but what they do not realize is that all these transactions add up and they are often accumulated into a single digital record. Businesses recognize the predictive value from such records and are investing heavily in greater data collection.").

143. Michael McFarland, *Ethical Implications of Data Aggregation*, MARKKULA CTR. FOR APPLIED ETHICS SANTA CLARA UNIV. (June 1, 2012), https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/ethical-implications-of-data-aggregation/ [https://perma.cc/A868-BTDY].

144. BARTHOLOMEW, *supra* note 124, at 70.

145. *See id.*; Alessandro Acquisti et al., *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509, 509 (2015).

> sometime later on, when combined with other data, reveal something sensitive.[146]

Additionally, consumers would need a much more sophisticated understanding of the data ecosystem in order to comprehend the "privacy threats and the consequences of sharing [or] protecting their personal information."[147] And not all privacy harms are readily ascertainable.[148] For example, consumers likely would not know—and businesses would be unlikely to disclose—that loyalty program data are typically protected with inferior data security compared to other commercial services, making them a "honey pot for hackers."[149]

Thus, the Framework's notice requirements do not remedy the information asymmetries preventing consumers from fairly assessing the benefits, risks, and costs of sharing their data with businesses. The requirement does not help consumers to understand, in concrete terms, what businesses know about consumers based on the types of data they collect. And the requirements do not help consumers to understand the risks of present or future uses of their data. Without these, the Framework cannot achieve its own purpose—to give consumers control over their personal data.

2. Practical & Cognitive Burdens: Consumers Are Ill-Equipped to Evaluate the Privacy Value-to-Risk Exchange

Even with perfect information symmetry, a fundamental flaw remains: consumers are simply unable, as a practical and cognitive matter, to keep up with the burdens the Framework places on them.

146. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1890 (2013).

147. Acquisti et al., *supra* note 96, at 444 ("[C]onsumers are rarely (if ever) completely aware about privacy threats and the consequences of sharing and protecting their personal information. Hence, market interactions involving personal data often take place in the absence of individuals' fully informed consent."); Rose, *supra* note 109, at 539 ("[C]onsumers 'still don't know all the ways their information is being sold, traded, and shared,' and therefore cannot know whether an offer is 'unjust' or 'coercive.' 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.'").

148. Acquisti et al., *supra* note 145, at 509 ("[W]hereas some privacy harms are tangible, such as the financial costs associated with identity theft, many others, such as having strangers become aware of one's life history, are intangible.").

149. Hsu, *supra* note 15; *see* Daniel Shkedi, *How Loyalty Programs Have Become a New Target for Cyber-Criminals*, FORTER (Feb. 12, 2020), https://www.forter.com/blog/loyalty-met-with-betrayal/ [https://perma.cc/6TAR-27VM] ("While the value and liquidity of loyalty program rewards has heightened, protecting these assets has lagged behind other digital services such as online banking, credit cards, or media-service providers.").

Consumers lack the capacity to navigate complex decisions about their personal data and privacy.[150] Though it prescribes notices of financial incentives, the Framework fails to acknowledge and address the many practical and cognitive burdens consumers must shoulder under this regime.

a. Practical burdens

The first burden borne by consumers is one of volume. Consumers make dozens—if not hundreds—of privacy decisions every day.[151] Each decision requires consumers to process information, which demands time and attention.[152] A 2008 study estimated that "reading privacy policies carries costs in time of approximately 201 hours a year."[153] Given the time and attention required to assess these privacy policies, it is unsurprising that consumers tend to make privacy decisions irrationally and without consistency.[154]

Additionally, the Framework provides no guidance to consumers about how to evaluate the offered benefits in relation to the offered incentive. This leaves consumers with the burden of analyzing the proposed privacy transaction on their own. As discussed above, the Framework falsely assumes that the notice of financial incentives is sufficient, and burdens consumers with the expectation that they understand something that they cannot. "In the absence of tools to

150. Acquisti et al., *supra* note 96, at 484 ("While, overall, [privacy-enhancing] technologies seemingly leave privacy choices in the hands of consumers, many (if not most) consumers, in practice, lack the awareness and technical sophistication required to protect and regulate the multiple dimensions of their personal information."); Cohen, *supra* note 137, at 1397 ("In reality, individuals face enormous difficulty assessing how their personal information will be used.").

151. *See* Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 115 (2017) ("Even the most diligent consumer would lack the time to read the hundreds of privacy policies he or she might encounter in a single day.").

152. *See* Stefan Korff & Rainer Böhme, *Too Much Choice: End-User Privacy Decisions in the Context of Choice Proliferation*, 2014 SYMP. ON USABLE PRIV. & SEC. 69, 71 ("[A]n increase in choice amount requires a decision maker to process more information and make more tradeoffs. It increases the frequency of preference changes and time needed.").

153. Aleecia M. McDonald & Lorrie F. Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 565 (2008) ("We estimate that reading privacy policies carries costs in time of approximately 201 hours a year, worth about $3,534 annually per American Internet user. Nationally, if Americans were to read online privacy policies word-for-word, we estimate the value of time lost as about $781 billion annually."); *see also* Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ [https://perma.cc/D2UN-6J2K] (equating the 201 hours per year to about seventy-six eight-hour workdays).

154. Alessandro Acquisti et al., *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249, 268 (2013).

effectively assess the data price and utility, consumers cannot—and thus do not—scrutinize data-for-services deals."[155]

b. Cognitive burdens

Consumers generally do not read or understand privacy notices; and even if they did read and understand those notices, consumers face many practical and cognitive hurdles to make rational decisions about their privacy.[156] "Human beings' rationality is bounded, which limits our ability to acquire and then apply information."[157] These "cognitive and behavioral biases" inhibit consumers' abilities to scrutinize privacy transactions,[158] which leads to contradictory and potentially harmful privacy decisions.[159]

For example, one study found that habits, more than cost-benefit assessments, are a "significant driver of self-disclosure."[160] Consumers may rely on their habitual behavior to disclose or withhold data to determine whether they disclose or withhold data when asked in subsequent transactions. This is likely explained as a response to cognitive burdens:

> Prior habits may have a particularly crucial role when the environment is diversified and ever-changing . . . —as it occurs in the digital landscape—with individuals often relying on heuristics to accelerate decisions whenever they feel cognitively overloaded . . . or constrained by information asymmetries . . . .[161]

Context also influences the decision-making process. From one situation to the next, a person's privacy attitudes or actions are shaped

155. Kolt, *supra* note 105, at 101.

156. *See* Solove, *supra* note 146, at 1888.

157. Alessandro Acquisti & Jen Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE SEC. & PRIV. 26 (2005).

158. Kolt, *supra* note 105, at 104.

159. Acquisti et al., *supra* note 154, at 268 ("From choosing whether to join a grocery loyalty program to sharing sensitive information (such as one's Social Security number) with a merchant, individuals make frequent privacy-relevant decisions, and this research suggests that they do so inconsistently."); Solove, *supra* note 146, at 1880–81 ("[E]mpirical and social science research demonstrates that there are severe cognitive problems that undermine privacy self-management. These cognitive problems impair individuals' ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data.").

160. Teresa Fernandes & Nuno Pereira, *Revisiting the Privacy Calculus: Why Are Consumers (Really) Willing to Disclose Personal Data Online?*, TELEMATICS & INFORMATICS, Dec. 2021, at 1, 6.

161. *Id.* at 7.

by past experiences, prior habits, social expectations and norms, the surrounding policy landscape, and numerous other factors.[162] "The same person can in some situations be oblivious to, but in other situations be acutely concerned about, issues of privacy."[163]

Marketers are keenly aware of consumers' bounded rationality and are adept at exploiting it.[164] A report by KPMG advises companies to "[f]ind the right irrationality point" to maximize loyalty program successes:

> A good loyalty program's customers will take "irrational" actions to achieve certain benefits. Consider the results in our survey, which revealed that 50 percent of customers said that they would do "almost anything" to earn more rewards in at least one loyalty program.[165]

One way that businesses manipulate these cognitive boundaries is through design. Businesses employ "dark patterns"—"design tricks platforms use to manipulate users into taking actions they might otherwise have not"—to "weaponize the design" in ways that lead consumers to share more information.[166] These design tactics intentionally exploit consumers' cognitive boundaries, "hid[ing] disclosure dangers while simultaneously highlighting the powerful social cues to share."[167] The CPRA added to the Framework a prohibition on the use of "dark patterns."[168] These are, however, only one of many tactics businesses use to exploit consumers' bounded rationality. Waldman,

---

162. Acquisti et al., *supra* note 145, at 511–12; Fernandes & Pereira, *supra* note 160, at 7.

163. Acquisti et al., *supra* note 145, at 509.

164. Ari E. Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox,'* 31 CURRENT OP. PSYCH. 105, 107 (2020) ("The evidence suggests that individuals care about their privacy. They are, however, dissuaded from acting effectively on those preferences by cognitive limitations leveraged by the digital platforms themselves."); Kolt, *supra* note 105, at 101 ("Importantly, many firms are familiar with these behavioral insights. They can therefore exploit consumers' apathy to nudge them into sharing greater quantities of more valuable personal data. By not demanding monetary payment for the services they offer, companies can conceal the data costs consumers pay and magnify the benefits they receive. For now, consumers are mostly resigned to the terms set by data-driven service providers. . . . The privacy paradigm, although consumer-oriented, actually obstructs efforts to increase *transactional* transparency and, consequently, reinforces consumer apathy.").

165. MATT HAMORY & KATHERINE BLACK, KPMG, IS IT TIME TO RETHINK LOYALTY PROGRAMS? 7 (2016), https://advisory.kpmg.us/content/dam/advisory/en/pdfs/is-it-time-to-rethink-your-loyalty-program.pdf [https://perma.cc/H6CJ-N5B6].

166. Waldman, *supra* note 164, at 105.

167. *Id.* at 108 ("Websites cue trust through professional design while hiding their invasive data collection practices in inscrutable privacy policies.").

168. CPRA, CAL. CIV. CODE §§ 1798.140(h), 1798.185(a)(20)(C)(iii) (2020) (amending CCPA, CAL. CIV. CODE § 1798.140 (2018)).

for example, has identified five "cognitive and behavioral barriers" that inhibit "rational privacy and disclosure decision-making"[169]: anchoring;[170] framing;[171] hyperbolic discounting;[172] overchoice;[173] and metacognitive processes.[174] The Framework fails to address these and other cognitive and behavioral barriers preventing consumers from making rational privacy decisions.

Given these significant practical and cognitive limitations, the Framework's unfounded reliance on consumers' capacity to make informed and rational decisions harms consumers rather than empowering them. As this section establishes, the Framework's approach falsely assumes that consumers are extremely capable of "navigat[ing] the marketplace with great dexterity, negotiating trade-offs between privacy and desired services with awareness."[175] In the face of empirical evidence to the contrary, the Framework leaves to consumers the impossible task of navigating the morass of privacy choices.[176] This places consumers at a disadvantage, despite the Framework's stated purpose of empowering consumers to take control of their privacy.[177] "In this context, relying on informed consent to prevent information harms would be similar to letting people decide for themselves what

169. Waldman, *supra* note 164, at 106.

170. Anchoring is a "disproportionate reliance on the information first available when we make decisions" that "can skew individuals' disclosure behavior based on what they see others have shared." *Id.* "[O]ur tendency to overvalue current rewards while inadequately discounting the cost of future risks makes us more willing to share now." *Id.*

171. Framing refers to the manner in which the privacy practice is presented to consumers, such as the use of leading language (e.g., "if you don't allow cookies, website functionality will be diminished" or "opting in to data collection will enable new and easier functionality"). *Id.* These framing techniques "[have] the effect of establishing the positives of data collection while glossing over or ignoring the negatives." *Id.*

172. Hyperbolic discounting refers to a consumer's "tendency to overweight the immediate consequences of a decision and to underweight those that will occur in the future." *Id.*

173. "Overchoice is the problem of having too many choices, which can overwhelm and paralyze consumers." *Id.*

174. Metacognitive processes "impair individuals' ability to make choices that accurately reflect their preferences." *Id.* For example, "the more users feel it is difficult to maintain their privacy online, as many do, the more likely many of them are to nihilistically decline to manage their disclosure." *Id.* at 107.

175. BARTHOLOMEW, *supra* note 124, at 163.

176. Acquisti et al., *supra* note 145, at 513 ("The task of navigating those boundaries, and the consequences of mismanaging them, have grown increasingly complex and fateful in the information age, to the point that our natural instincts seem not nearly adequate.").

177. Assemb. B. 375, 2017–2018 Leg., Reg. Sess. § 2(i) (Cal. 2018); PROPOSITION 24, *supra* note 40; *see also* Kolt, *supra* note 105, at 101 ("The privacy paradigm, although consumer-oriented, actually obstructs efforts to increase *transactional* transparency and, consequently, reinforces consumer apathy.").

level of exposure to toxic substances they would accept in the workshop or the environment."[178]

C. Valuation & Inequality

The financial incentive exception will almost certainly have problematic and unintended consequences: disparate negative impacts on vulnerable socioeconomic groups. This section unpacks the many ways in which the Framework's financial incentive exception is likely to engender and exacerbate inequality. The first part of this section explains that the financial incentive exception drives greater economic inequity. The second part describes the ways in which existing privacy disparities are worsened by the Framework's financial incentive exception.

1. Driving Greater Economic Inequality

The financial incentive exception in the California Privacy Framework gives businesses permission to offer preferential treatment to certain consumers over others based on the value of the consumer's data to businesses. In general, wealthier consumers and their data are more valuable to businesses[179] because wealthy consumers have greater "lifetime value."[180] Affluent consumers represent a "lower churn rate, more frequent orders, and larger expenditure per order."[181] Businesses court these consumers with personalized marketing messages and deals because these efforts will have greater returns (i.e., repeat purchases and larger purchases).[182] "[M]arketers would rather have your data if you're rich than if you're poor. Thus, marketers are likely to spend extra money to identify wealthier customers and recruit them to loyalty programs that offer incentives for repeat shoppers."[183]

Lower-value consumers will still have access to some benefits in exchange for personal data, but they won't be on par with those offered to the high-value segment of consumers.

---

178. Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 425, 428 (2011).

179. Cohen, *supra* note 137, at 1398.

180. JOSEPH TUROW, THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY, AND DEFINE YOUR POWER 10 (2017) ("Part of retail discrimination is to identify customers deemed to have a relatively high 'lifetime value' (a shopper's lifetime being typically defined as five years).").

181. Stourm et al., *supra* note 12, at 408.

182. TUROW, *supra* note 180, at 10 ("These profitable shoppers receive tailored deals aimed to keep them coming back.").

183. Cohen, *supra* note 137, at 1398.

> Customers on the lower-valued end of the shopping spectrum typically aren't treated poorly; they may even get personalized discount offers in the hope that their value to the store might increase. But they will not enjoy anything like the attention and value the loyal customers enjoy. Moreover, some retailers downgrade the benefits of their loyalty program for customers judged to be of less value to the store based on the amounts they spend.[184]

As a result, the more affluent consumers receive greater benefits—despite the fact that they would likely make the same purchases in the absence of incentives[185]—and less affluent consumers receive lesser benefits, even though a discount would likely go further for them.

As a justification for discriminatory treatment of consumers who exercise their data privacy rights, the Framework incorporates into its privacy scheme this commercial practice of valuing consumers. Under the financial incentive exception, the financial incentive and the value of a consumer's data must be "reasonably related."[186] This can be interpreted at least two ways. Where the value of the incentive is high, the value of the consumer's data to the business must also be high to be "reasonably related" to it.[187] Similarly, where the value of the incentive is high, and the value of the consumer's data is low, the business must collect more data in order for the relationship to be "reasonably related." For example, a business offers a $10 discount for every $100 spent by a consumer in its loyalty program. A high-value consumer's data might be reasonably related to the $10 discount, but a low-value consumer's data might only be reasonably related if they give twice as many data points or share more valuable types of data. As another "reasonably related" approach, the business may require that all consumers give the same amount and types of data but might offer a more valuable incentive to its high-value consumers (e.g., a $20 discount) and a less valuable incentive to its low-value consumers

184. TUROW, *supra* note 180, at 10–11.

185. Brett Hollenbeck & Wayne Taylor, *How to Make Your Loyalty Program Pay Off*, HARV. BUS. REV. (Oct. 28, 2021), https://hbr.org/2021/10/how-to-make-your-loyalty-program-pay-off [https://perma.cc/Q4Y5-4CE2] ("[R]etailers often target loyalty promotions at their highest-spending customers, which can seriously backfire, since these are customers who would have spent their money regardless, rather than customers for whom discounts would actually convince them to spend more.").

186. CAL. CODE REGS. Tit. 11, § 7080(b) (2022).

187. Stourm et al., *supra* note 12, at 413.

(e.g., a $10 discount). Ultimately, less valuable consumers pay more, in real money or in data, or both[188]:

> A perverse consequence of a purely market-based approach to data privacy rights, then, may be more discounts for the rich. If so, then the poor will lose twice over. They will have less privacy, and they will also pay more for goods and services than more desirable customers. Privacy in markets, then, is more than a luxury. Personally-identified data is the wedge that enables "scientific," market-driven, and increasingly precise separation of "haves" from "have-nots."[189]

The underlying problem with this justified differential treatment is that it is driven by data collection. It requires data collection initially to get to know each consumer. It requires more data to refine its determinations about which consumers the business should focus its marketing resources on. And data collection continues indefinitely until the consumer takes affirmative steps to opt out of the loyalty program or requests data deletion. Under the guise of giving consumers greater privacy control and autonomy, the financial incentive exception encourages ever-greater data harvesting that reinforces a system of inequality, favoring commercial interests over protecting consumers.

2. Perpetuating Privacy Poverty

The Framework's financial incentive exception perpetuates systemic inequality. The poor have historically enjoyed "far less control over the privacy of their homes, bodies, and decisions than their more affluent counterparts."[190] Far from remedying privacy inequality, the financial incentive exception enshrines it in the law, to the great disadvantage of all Californians and to vulnerable Californians in particular.

Economically disadvantaged consumers are more vulnerable to privacy harms in general. There are many reasons for this, including greater exposure through reliance on mobile devices for internet

188. *See* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 141 (2017) ("While both the wealthy and the poor are subjected to privacy invasions, those invasions result in the wealthy getting better deals on more coveted products; meanwhile, the poor are left to pay more for less desirable products.")

189. Cohen, *supra* note 137, at 1398.

190. Madden et al., *supra* note 151, at 58.

connectivity;[191] use of more affordable, but less secure, mobile devices;[192] lack of understanding of privacy settings and policies, particularly in social media practices;[193] fewer resources to mitigate privacy harms;[194] and predatory business behaviors.[195] This is not because these consumers care less about privacy than wealthy consumers. They may, in fact, care more: one survey observed that low-income social media accountholders were more concerned about commercial use of their personal information than more affluent social media accountholders.[196]

The financial incentive exception places low-income consumers in a difficult position, whether they are aware of it or not. Economically disadvantaged consumers would be hard-pressed to turn down a discount or some other financial benefit.[197] Even meager incentives would likely have tangible and immediate impacts on cash-strapped consumers. Knowing this, businesses can take advantage of a consumer's financial circumstances—and their inability to understand data transactions—to entice them into sharing personal information that benefits the business.

---

191. *Id.* at 70, 73–75.

192. *Id.* at 62.

193. *Id.* at 75–76 ("Low-income social media users are less likely to feel as though they 'know enough' about managing the privacy settings for the information they share online (65% vs. 77%) and are less likely to feel they have a good understanding of the privacy policies for the applications and websites they use (64% vs. 74%). At the same time, low-income social media users are more likely than higher earning groups to feel as though it would be 'somewhat' or 'very' difficult to find tools and strategies that would help them protect their personal information online (25% vs. 15%). Low-income social media users are also less likely to engage in other privacy-protective strategies that may impact the way they are tracked online. For instance, they are less likely to say that they have avoided communicating online when they had sensitive information to share. About half (52%) report this, compared with 63% of social media users in wealthier households. Similarly, a smaller share of low-income social media users say they have set their browsers to turn off cookies or notify them before receiving a cookie (47% vs. 58%).").

194. *Id.* at 53, 63; *see id.* at 62–63 ("Consider identity theft, a growing concern shared across social classes. This crime is particularly devastating for low-income individuals, who face not only financial losses that impact their ability to meet basic needs such as housing and utility services, but are also left coping with more severe consequences of someone else using their identity, such as wrongful arrests, improper child support garnishments, and harassment by collection agencies.").

195. Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1426 (2017); Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 849, 853, 868–69 (2014).

196. Madden et al., *supra* note 151, at 77–78 ("[L]ow-income users express deeper worries about commercial data collection. About half (52%) say they are 'very concerned' about not knowing what personal information is being collected about them by companies or how it is being used, compared with just over a third (37%) of more affluent social media users.").

197. Elvy, *supra* note 195, at 1424 ("[C]onsumers from vulnerable communities may be more willing to accept discounts offered under PFP discount models.").

> Many consumers have only a limited understanding of privacy risks and may therefore opt for monetary discounts over data protection. The prospect of a monetary discount entices them to supply more personal data. In addition, not all consumers are in a position to pay a monetary premium (or refuse a monetary discount) in order to protect their privacy. Many consumers, even if they are particularly concerned about their privacy, may be financially compelled to supply more personal data.[198]

The financial incentive exception props open the door for practices that fuel the modern economy: segmentation and targeting.[199] To be effective, these strategies require massive amounts of data, and loyalty programs provide an abundance of data. As discussed above, data collected through loyalty programs are aggregated and analyzed to build profiles about consumers or group them in ways that facilitate efficient messaging and media strategies.[200] In this way, businesses and their affiliates derive highly revealing insights about a consumer that can be used in ways that maximize profit for the business at the expense of the consumer's financial well-being and privacy.

One clear example of this is price discrimination. "Offering only full-price offers to some online buyers while selectively offering discounts to others based on online profiling is one of the most pervasive forms of price discrimination operating in online sales."[201] While an equitable application of this practice would be to offer the full price to wealthier consumers and lower prices to those of lesser means, the approach is actually the opposite. One report found that "'areas that tended to see the discounted prices had a higher average income than areas that tended to see higher prices,' largely on the assumption that poor areas have fewer retail options locally so a higher price can be extracted from them by online retailers."[202]

A more insidious example is predatory advertising. "Some companies have used consumer data to identify low-income and

198. Kolt, *supra* note 105, at 120 (footnote omitted).

199. *See generally Market Segmentation: Definition, Types, Benefits, & Best Practice*, QUALTRICS, https://www.qualtrics.com/experience-management/brand/what-is-market-segmentation/ [https://perma.cc/5WLH-GZ7U] (outlining the mechanics of market segmentation and how the process leads to more focused targeting by advertisers).

200. *See supra* notes 14–16 and accompanying text.

201. Newman, *supra* note 195, at 869.

202. *Id.* at 868–69.

vulnerable consumers for predatory marketing campaigns."[203] As noted in a report by the Senate Commerce Committee on the practices of data brokers, "the poor have been profiled into various 'financially vulnerable' market segments such as 'Rural and Barely Making It,' and 'Fragile Families.'"[204] These segments have been used "to easily target vulnerable consumers for dubious financial products such as payday loans, online classes, or debt relief services."[205] Coupled with price discrimination, "[a]dvertisers can deliver ads not just to the users most likely to be interested in the product, but can tailor prices for individual consumers in ways that can maximize the revenue extracted from each purchaser."[206]

These concerns are not restricted to loyalty programs, but loyalty programs contribute to the disproportionate harms these practices inflict on vulnerable communities.

> [Loyalty programs] enable the collection of big data, and big data can be used to enhance and expand [loyalty programs]—a virtuous cycle. As a result, [loyalty programs] trigger (1) privacy concerns related to the collection and usage of fine-grained, identifiable data on consumers, (2) inequality concerns related to the design of the program where consumers can or cannot enter/benefit, and (3) sustainability concerns related to the usage of rewards. So, the inherent link between [loyalty programs] and big data naturally links [loyalty programs] to a variety of societal issues . . . .[207]

Worse, loyalty programs may actually exacerbate harms.[208] As discussed above, loyalty programs are easy and lucrative targets for hackers.[209] Even under a pretense that consumers of all socioeconomic

---

203. Elvy, *supra* note 195, at 1423–24 ("During the housing bubble preceding the most recent financial crisis, companies used data about consumers to engage in predatory lending and discriminatory behavior to the detriment of marginalized communities.").

204. Madden et al., *supra* note 151, at 77.

205. *Id.*

206. Newman, *supra* note 195, at 852.

207. Stourm et al., *supra* note 12, at 414.

208. *Id.* at 406.

209. *See supra* note 149 and accompanying text; *see also* Shkedi, *supra* note 149 ("While the value and liquidity of loyalty program rewards has heightened, protecting these assets has lagged behind other digital services such as online banking, credit cards, or media-service providers."); Hsu, *supra* note 15 ("Loyalty programs are 'almost a honey pot for hackers,' said Kevin Lee, a risk expert for the digital security firm Sift. They tend to be, he said, 'the path of least resistance': easy to sign up for, shielded by flimsy passwords and often neglected by users. The programs, and their appetite for data, have grown, but security has not kept pace."); *id.* ("Some criminals use stolen

levels are equally exposed to the risk of a data breach, low-income consumers are more deeply harmed because they have fewer resources with which to bounce back.[210] "Identity theft can be especially devastating for low-income people because it jeopardizes basic income sources and vitally necessary services."[211] Additionally, consumers of all types likely cannot detect these practices or resulting harms due to the information asymmetries discussed above.[212]

Vulnerable consumers likely will not receive discounts or deals to offset the inequitable treatment and privacy risks resulting from their participation in any financial incentive scheme. Yet, California's Framework blesses financial incentives so long as the business can justify them with an impossible-to-calculate valuation that reasonably relates to them. Several commenters criticized the incongruity of this approach in their comments to the Regulations. The Electronic Privacy Information Center urged the California Attorney General to "mitigate[] to the maximum extent possible" this "pay-for-privacy" exception because it "encourages consumer discrimination."[213] As the ACLU, joined by the Electronic Frontier Foundation, Oakland Privacy, and several other public interest groups, argued:

> Permitting different valuations for different people might seem like an innocuous application of the simple economic principle of price discrimination . . . . But the implications of charging some groups more because of the value of their information compared with other groups has the possibility of deepening the harm associated with a regime that permits charging people for exercising their privacy rights.
>
> People's information is most valuable not when they are rich, but when they are vulnerable.[214]

---

credentials to impersonate customers, breach loyalty profiles and then tap into separate accounts. Others deplete balances or sell points on dark web marketplaces.").

210. Madden et al., *supra* note 151, at 62.

211. Sarah Dranoff, *Identity Theft: A Low-Income Issue*, A.B.A.: DIALOGUE (Dec. 15, 2014), https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft—a-lowincome-issue/ [https://perma.cc/T4EG-ZQ8W].

212. *See supra* notes 154–157 and accompanying text; Madden et al., *supra* note 151, at 68 ("In cases of big-data-related decision-making and discrimination, it is nearly impossible for respondents to know what personal or behavioral information may have factored into an unfavorable outcome.").

213. PUBLIC COMMENTS TO THE OAG, *supra* note 117, at 571.

214. *Id.* at 1466.

As this section details, the Framework's financial incentive exception disproportionately harms less affluent and less educated consumers. Contrary to the law's purpose of giving consumers greater autonomy and control over their personal information, the financial incentive exception begets inequity and privacy harms. Instead of remedying the existing inequities among an already vulnerable class of consumers, the financial incentive exception reinforces them, paving the way for greater inequality in the future.

III. LOOKING FORWARD: COURSE-CORRECTION & TRENDSETTING

This Article highlights several problems with the California Privacy Framework's financial incentive exception. In response, this Article suggests ways to mitigate the harms of this approach.

As an overarching point, consumer privacy laws should not frame data as commodities. As discussed throughout this Article, the benefits that a consumer may gain from financial incentives are miniscule when compared to the individual and societal risks. As a matter of policy, laws that encourage consumers to trade away their privacy should not be normalized:

> [I]t is important to avoid conflating economic and privacy considerations, and avoid a situation where consumers will be trading away their data or privacy rights.
>
> . . . .
>
> . . . By distinguishing clearly between economic objectives and privacy objectives, and moving away from consent-based models that fall short of both objectives, we can best protect consumers and their data, while still enabling companies to unlock the benefits of AI and machine learning for industry, society, and consumers.[215]

215. Lokke Moerel & Christine Lyon, *Commoditization of Data Is the Problem, Not the Solution—Why Placing a Price Tag on Personal Information May Harm Rather Than Protect Consumer Privacy*, FUTURE OF PRIV. F. (June 24, 2020), https://fpf.org/blog/commoditization-of-data-is-the-problem-not-the-solution-why-placing-a-price-tag-on-personal-information-may-harm-rather-than-protect-consumer-privacy/ [https://perma.cc/R56R-JWLK] ("Although societies certainly may decide to require some degree of compensation to consumers as a wealth redistribution measure, it will be important to present this as an economic tool and not as a privacy measure."); *see also* Hayley Tsukayama, *Knowing the "Value" of Our Data Won't Fix Our Privacy Problems*, ELEC. FRONTIER FOUND. (July 15, 2019), https://www.eff.org/deeplinks/2019/07/knowing-value-our-data-wont-fix-our-privacy-problems [https://perma.cc/2K4N-QQLK] ("Our information should not be thought of as our property this way, to be bought and sold like a widget. Privacy is a fundamental human right. It has no price tag. No person should be coerced or encouraged to barter

As this Article highlights, the Framework's financial incentive exception is flawed in ways that hurt consumers and society at large. Yet several states have either considered or enacted financial incentive exceptions in their own privacy laws.[216] At the time of this writing, four other states have passed comprehensive consumer data privacy laws: Colorado,[217] Connecticut,[218] Utah,[219] and Virginia.[220] All four of these states' privacy laws contain an exception for financial incentives, but these do not include a valuation requirement. Other proposed privacy laws, however, do contain financial incentive exceptions that require valuation in some form. Alaska's bill, H.B. 159, contains a financial incentive exception accompanied by a valuation requirement that is nearly identical to the language in California's section 1798.125.[221] Bills from the Wisconsin and Ohio legislatures require that a financial incentive be "*related* to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts,

---

it away. And it is definitely not a good deal for people to receive a handful of dollars in exchange for allowing companies' invasive data collection to remain unchecked.").

216. Desai, *supra* note 2; *see, e.g.*, S.B. 46, 192d Gen. Ct., 2021–2022 Reg. Sess. § 5 (8)(ii)(1) (Mass. 2021); Assemb. B. A680B, 204th Leg., 2021–2022 Reg. Sess. § 1102 (2)(j)–(k) (N.Y. 2021); S.B. S6701B, 204th Leg., 2021–2022 Reg. Sess. § 1102 (3)(h)(ii)–(iii) (N.Y. 2021); Assemb. B. A6042, 204th Leg., 2021–2022 Reg. Sess. § 899-ee(12)–(13) (N.Y. 2021); S.B. 569, 155th Gen. Assemb., 2021 Reg. Sess. § 75-72(a)(4) (N.C. 2021); H.B. 1492, 92d Leg., 2021–2022 Reg. Sess. § 7(3)(b) (Minn. 2021); H.B. 376, 134th Gen. Assemb., 2021–2022 Reg. Sess. § 1355.09(D)(2) (Ohio 2022); H.B. 1126, 2021 Gen. Assemb., Reg. Sess. § 4(k)(1)–(2) (Pa. 2021); S.B. 1614, 54th Leg., 2d Reg. Sess. § 18-701(j)–(k) (Ariz. 2020); H.B. 2729, 54th Leg., 2d Reg. Sess. (Ariz. 2020); Serrato & Wu, *supra* note 48, at 102 ("Even if we have determined that CCPA does not apply to a specific data processing activity, over a dozen states are contemplating CCPA-like laws and thus the concept of non-discrimination may be extended to other jurisdictions.").

217. S.B. 21-190, 73d Gen. Assemb., 1st Reg. Sess. (Colo. 2021) (effective July 1, 2023).

218. S.B. 6, 2022 Gen. Assemb., 2022 Reg. Sess. (Conn. 2022) (effective July 1, 2023).

219. S.B. 227, 2022 Leg., 2022 Gen. Sess. (Utah 2022) (effective Dec. 31, 2023).

220. VA. CODE ANN. §§ 59.1-575 to 59.1-585 (2022) (effective Jan. 1, 2023).

221. H.B. 159, 32d Leg., 2d Reg. Sess. § 45.48.870 (Alaska 2022).

> (a) A business may not retaliate against a consumer in response to a consumer exercising rights under this chapter. Retaliation includes
>
> (1) denying goods or services;
>
> (2) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
>
> (3) providing a different level or quality of goods or services to a consumer;
>
> (4) suggesting that a consumer will receive a different price or rate for goods or services, or a different level or quality of goods or services.
>
> (b) Notwithstanding (a) of this section, a business may charge a consumer a different rate or provide a different level or quality of goods or services to a consumer if the difference is reasonably related to the value provided to the business by the consumer's data.

Id.; *see* CPRA, CAL. CIV. CODE § 1798.125 (2020) (amending CCPA, CAL. CIV. CODE § 1798.125 (2018)).

or club card program."[222] New York's Assembly Bill A680B permits businesses to "operate a program in which information, products, or services sold to the consumer are discounted based on such consumer's prior purchases from the controller."[223]

When drafting legislation for comprehensive data privacy laws, states should consider the contradictory nature of financial incentive exceptions to a right of non-discrimination and the impracticability of an accompanying valuation scheme. When developing regulations, the newly formed California Privacy Protection Agency should take an approach to data valuation that considers the many challenges businesses and consumers face in navigating the valuation requirement and the inequities it perpetuates.

Lawmakers should also center data privacy laws around equity. Giving consumers rights without ensuring that the regulations provide comprehensible information does not help them take control of their data. Lawmakers should consider the consumer data ecosystem and empirical evidence about consumers' abilities to navigate privacy decisions rationally.

Policymakers should place equity at the center of data privacy conversations. In addition to addressing several of the harms discussed in this Article, a policy objective grounded in preventing inequality may be more rhetorically powerful than merely protecting consumers from data breaches or price discrimination. "[T]he specter of discrimination is easier to actualize and may serve as a stronger civil liberties argument."[224] In contrast, the consumer protection argument "is not strong enough to overcome corporate claims of profitability, job creation, and innovation."[225] Thus, placing privacy inequity at the heart of data privacy discussions will benefit consumers while also being politically advantageous.[226]

Given the information asymmetries and limits on rational consumer decision-making, privacy frameworks should take a more paternalistic approach. As this Article demonstrates, "individuals cannot

222. Assemb. B. 957, 105th Leg., Reg. Sess. § 3(a)(4) (Wis. 2021); H.B. 376, 134th Gen. Assemb., 2021–2022 Reg. Sess. § 1355.07(D)(2) (Ohio 2022).

223. Assemb. B. A680B, 204th Leg., 2021–2022 Reg. Sess. § 2(k) (N.Y. 2021).

224. Benjamin W. Cramer, *A Proposal to Adopt Data Discrimination Rather Than Privacy as the Justification for Rolling Back Data Surveillance*, 8 J. INFO. POL'Y 5, 5, 19 (2018).

225. *Id.* at 5.

226. *Id.* at 6 ("While privacy is a crucial American value, it may be more realistic to convince judges and politicians that a different American value, freedom from discrimination, is also at risk in the world of big data.").

adequately self-manage their privacy, and consent is not meaningful in many contexts involving privacy."[227]

CONCLUSION

The California Privacy Framework's financial incentive exception subverts the non-discrimination right provided to California consumers and undermines the Framework's purpose. Instead of giving consumers greater control over their data, the law contributes to the already-obscure data privacy ecosystem and exacerbates existing disparities.

Lawmakers considering data privacy policy should steer clear of this approach and should not marry data valuation with data privacy. As demonstrated throughout this Article, such an approach undermines efforts to protect privacy and exacerbates inequities.

227. Solove, *supra* note 146, at 1894.