Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU ePrivacy Regulation

*By Christie Dougherty**

* Northeastern University School of Law, Class of 2020; Certified Information Privacy Professional in Europe (CIPP/E). She would like to thank Professor Woodrow Hartzog for his advice and guidance on this Note's topic, and Miranda Jang and Alex Nally for their constant support and feedback along the way.

Table of Contents

I. INTRODUCTION

At noon you meet with your friend over lunch. You both have your iPhones out on the table while you talk about everything from your dream vacation to Bali to your sneaking suspicion that your partner is going to propose soon. At eight o'clock that evening, as you begin winding down from your day, you scroll through Instagram and see someone in your feed posted a picture of a beautiful beach resort in Bali. As you hover, a brown bar pops up over the bottom of the picture saying, "Book Now." *How did Instagram know that?* You switch to Facebook and notice a little blue advertisement for engagement rings on the side of your newsfeed. *Creepy*, you think to yourself, as you put your devices to sleep and prepare to do the same.

Creepy is a term frequently used by someone having difficulty explaining technology that they do not understand; yet few people in these creepy situations take steps to try to learn how that technology works. For example, did you know that Facebook and its subsidiaries, including Instagram, collect information about your activities off of Facebook, regardless of whether you have a Facebook account or are logged into Facebook?[1] Every move you make, Facebook's watching you. Testifying before Congress in April 2018, Mark Zuckerberg, CEO of Facebook, stated that consumers themselves had "control" over their information thirty-five times, are empowered to make "choices" twice, and "choose" Facebook four times.[2] Committee Member Ben Luján (D-NM) pointed out, "[I]t may surprise you that, on Facebook's page, when you go to 'I don't have a Facebook account and would like to request all my personal data stored by Facebook,' it takes you to a form that says, 'Go to your Facebook page, and then, on your account settings, you can download your data.'"[3] Yet, consumers still believe that if they delete their Facebook, Facebook cannot use and misuse their personal

1 *Data Policy*, Under *Information from Partners*, FACEBOOK, https://www.facebook.com/policy.php (last visited Jan. 29, 2020) ("For example, a game developer could use [Facebook's] API to tell [them] what games you play, or a business could tell [them] about a purchase you made in its store. [They] also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide [them] with your information.").

2 *See Facebook: Transparency and Use of Consumer Data: Hearing Before the Comm. of Energy & Commerce*, 115th Cong. (2018) (testimony of Mark Zuckerberg, CEO, Facebook).

3 *Id.* at 119.

information.[4]

This theme of technology controlling society, such as Facebook or the internet in general, has existed since at least the creation of 18th century mechanical clocks, which manifested social control through providing a new method of keeping records on human activity.[5] With the advent of the internet, society was enraptured by the possibilities it could offer. In 1992, the internet was referred to as the "information highway."[6] By 1993, society began referring to the internet as "cyberspace." The term "cyber" is derived from the Greek root for control.[7] Today, the term "cyber" is often associated with privacy violations: cyberattack, cyberterrorism, cybersecurity.[8] And, although cybersecurity and privacy are imperfect synonyms,[9] privacy is often defined in terms of control.[10]

For the purposes of this note, privacy is defined as the ability of consumers to provide informed consent to the dissemination of their personal information so that they can better control their personal information. This definition of privacy suggests that informed consent is something that should be considered by regulations seeking to restrict companies that process and sell consumer data, by framing privacy as an "ability," or positive right, rather than a "right," or a negative right. Constructing the definition as an ability further acknowledges that the practical application of consent regimes is less than ideal. In Section II, this note will discuss the informed consent requirements in Europe's proposed ePrivacy Regulation and compare them to the informed consent requirements in California's recently passed California Consumer Privacy Act ("CCPA"). It will also discuss the different lenses that Europe and the United States

4 *See* The N.Y. Times, *Why Leaving Facebook Doesn't Always Mean Quitting | NYT,* YOUTUBE (Mar. 27, 2018), https://www.youtube.com/watch?v=mE2fSvbmWFs; *see also* Alfred Ng, *Facebook Still Tracks You After You Deactivate Account,* CNET (Apr. 9, 2019), https://www.cnet.com/news/facebook-is-still-tracking-you-after-you-deactivate-your-account/.

5 JAYNE GACKENBACH, PSYCHOLOGY OF THE INTERNET: INTRAPERSONAL, INTERPERSONAL, AND TRANSPERSONAL IMPLICATIONS 15 (2d ed. 2006).

6 *Id.* at 22.

7 *Id.* at 22–23.

8 *See generally* Andrea M. Matwyshyn, *CYBER!,* 2017 BYU L. REV. 1109 (2017) (discussing privacy conflation, incommensurability, and internet exceptionalism as three analytical flaws in "cyberized" legal scholarship).

9 *Id.* at 1135.

10 *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 63 (2018) ("Control has become the archetype for data protection regimes.").

use to explain and regulate the right to privacy. In Section III, this note will explain that informed consent is not a realistic standard for regulations to apply to businesses that process and sell consumer data due to information asymmetries and the paradox of choice, wearing down by design, and nudging. These are techniques used to manipulate consumer behavior and lead consumers to a predestined choice based on a series of design decisions, rendering informed consent meaningless. This note proposes throughout Section III that privacy by design should be considered the gold standard approach to framing future federal legislation in the United States. Section IV discusses why the CCPA and ePrivacy Regulation will be ineffective in their respective approaches. Finally, Section V acknowledges the practical limitations of the privacy by design framework deriving from the First and Fourteenth Amendments.

II. REGULATORY SCHEME

Samuel Warren and Louis Brandeis, in 1890, explored why privacy claims and the "right to be let alone" were inevitable.[11] They discussed that although the privacy of manuscripts and publications could be seen as rights rooted in property law, once privacy developed into "[t]he principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, [privacy] is in reality not the principle of private property, but that of an inviolate personality."[12] Although they ultimately dismiss property and copyright laws as methods of analyzing privacy claims, privacy in the United States is still viewed as a property right.[13]

For example, while European privacy law views it as a civil right, the United States' laws view privacy as a property right.[14] The different lenses used between the two countries offer two different views of "possession" and "ownership" that may provide a useful

11 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

12 *Id.* at 205.

13 *See id.* at 198–205; Detlev Zwick & Nikhilesh Dholakia, *Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right Versus Civil Right*, 11 ELECTRONIC MKTS. 116, 117–18 (2001).

14 *Compare* Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, *opened for signature* Nov. 4, 1950, E.T.S. No. 5 (entered into force Mar. 9, 1953) [hereinafter European Convention on Human Rights], *with* U.S. CONST. amend. IV. *See generally* Zwick & Dholakia, *supra* note 13.

understanding for the informed consent provisions.[15] "Possession is a physical circumstance, while ownership is socially constructed (i.e., property right)," but "[o]nly ownership bestows the right to exchange in the marketplace."[16]

The ePrivacy Regulation defines the consumer as the person who has control and ownership over the personal information.[17] Consumers under the ePrivacy Regulation, as under traditional European privacy law, are treated as "passive objects of protection from market forces," as the Regulation seeks to protect consumers from companies placing unknown and unconsented to cookies on their computers.[18] In contrast, the CCPA was created based on the assumption that privacy is a digital commodity that can be bought and sold on the internet with the consumer's consent.[19] Consumers under the CCPA are treated more as active, entrepreneurial participants in the digital marketplace.[20]

15 *See* Zwick & Dholakia, *supra* note 13, at 117.

16 *Id.* (emphasis omitted).

17 *See id.* at 117–18 (discussing the philosophical history of European privacy laws, including the EU Directive on Privacy Protection—the directive that preceded the GDPR); *see also Council Preparatory Document for Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications* at 8–9, No. 14054/19 (Nov. 15, 2019) [hereinafter *2019 Council Preparatory Document for Proposed ePrivacy Regulation*] (The first three recitals of the Regulation refer to the Charter of Fundamental Rights of the European Union, the concept of highly sensitive information and the GDPR, all of which seek to provide EU citizens ownership over their personal information.).

18 *See* Zwick & Dholakia, *supra* note 13, at 118 (discussing the different lenses applied to privacy laws in the US and EU); *2019 Council Preparatory Document for Proposed ePrivacy Regulation*, *supra* note 17, at 55.

19 *See* Zwick & Dholakia, *supra* note 13, at 118 (discussing the different lenses applied to privacy laws in the US and EU); California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.120 (West 2018) [hereinafter CCPA] ("A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information."); Rachel Haberman, *CCPA 101: A Marketer's Guide to the California Consumer Privacy Act*, JEBBIT (Feb. 7, 2019), https://www.jebbit.com/blog/ccpa-101-a-marketers-guide-to-the-california-consumer-privacy-act ("Data privacy legislation, and the data privacy movement as a whole, will force marketers to change their relationship with consumer data. The CCPA and other data privacy legislation effectively turn consumer data from a commodity into a privilege that can be revoked.").

20 *See* Zwick & Dholakia, *supra* note 13, at 118 (discussing the different lenses applied to privacy laws in the US and EU); *see also* Mike Duffy, *Worried About Your Data? The California Consumer Privacy Act Gives You New Tools*, ABC10, https://www.abc10.com/article/news/worried-about-your-data-the-

In the European Union ("EU"), there are two distinct rights to privacy that are not found in the United States: the right for private and family life, and the right of protection of personal data.[21] Conversely, the United States identifies informational privacy, the right to privacy in a person's "houses, papers, and effects," and decisional privacy in the person's freedom from government interference.[22] This contrast highlights the emphasis the two jurisdictions place on positive and negative rights. European laws are drawn as positive rights as they "require the state to act positively to promote the well-being of its citizens, rather than merely refraining from acting."[23] The United States draws its laws as negative rights, which operate to restrain the state from acting.[24] European laws, and positive rights, assert claims to affirmative rights, whereas the United States' laws, and negative rights, call for prohibitions.[25] These distinctions between the United States' and European laws lay the framework for the discussion on creating a privacy framework for the United States.[26]

A. Informed Consent in the ePrivacy Regulation

The ePrivacy Regulation is a current proposal promulgated by the European Parliament that concerns "the respect for private life and the protection of personal data in electronic communications."[27] This proposal would modernize the previous Directive 2002/58/EC, which was a regulation on privacy and electronic communications.[28] While the European General Data Protection Regulation ("GDPR")

---

california-consumer-privacy-act-gives-you-new-tools/103-0ad01e28-0357-4f00-86f9-cd53143c9ada (last updated Jan. 3, 2020) ("[The CCPA] requires the active participation of consumers.").

21 *See* G.A. Res. 217A (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 19, 1948); European Convention on Human Rights, *supra* note 14, art. 8; *see also* Charter of Fundamental Rights of the European Union, art. 7–8, 2012 O.J. (C326) 397.

22 *See* U.S. CONST. amend. IV; Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965).

23 Ran Hirschl, *"Negative" Rights vs. "Positive" Entitlements: A Comparative Study of Judicial Interpretations of Rights in an Emerging Neo-Liberal Economic Order*, 22 HUM. RTS. Q. 1061, 1071–72 (2000).

24 *Id.*

25 *Id.*

26 *See* discussions *infra* Sections IV and V.

27 *See generally 2019 Council Preparatory Document for Proposed ePrivacy Regulation*, *supra* note 17.

28 *Id.* at 1.

protects personal data, the ePrivacy Regulation would "ensure[] the confidentiality of communications, which may also contain non-personal data and data related to a legal person."[29]

The ePrivacy Regulation would adopt the GDPR's definition of consent: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[30] Further, the ePrivacy Regulation would adopt the GDPR's conditions for consent, including: "the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data;" the data subject's consent should be requested in a way that is "presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language;" the data subject has the right to withdraw his or her consent at any time and "[i]t shall be as easy to withdraw as to give consent;" and "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[31] The ePrivacy Regulation, however, would go a step further than the GDPR by also defining consent as "using the appropriate technical settings of a software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet."[32]

Under the ePrivacy Regulation, data subjects must provide consent in most cases to "[t]he use of processing and storage ca-

29 *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, at 5, (COM 2017) 10 final (Jan. 10, 2017) [hereinafter *2017 Proposed ePrivacy Regulation*].

30 EU Regulation 2016/676, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(11), 2016 O.J. (L 119) 34 [hereinafter GDPR]; *see also 2019 Council Preparatory Document for Proposed ePrivacy Regulation, supra* note 17, at 55 (addressing "consent" in Article 4a).

31 GDPR, *supra* note 30, art. 7, at 37; *see also 2019 Council Preparatory Document for Proposed ePrivacy Regulation, supra* note 17.

32 *Compare 2019 Council Preparatory Document for Proposed ePrivacy Regulation, supra* note 17, at 55, *with* GDPR, *supra* note 30, art. 4(11), at 34.

pabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned."[33] This means that data subjects must consent to companies placing cookies[34] on their devices. When non-essential information is collected by terminal equipment in order to connect to another device or to network equipment, "a clear and prominent notice shall be displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under" the GDPR.[35] These two provisions mostly focus on targeting internet sites that place cookies on the end-user's computer without their knowledge or consent.

B. Informed Consent in the California Consumer Privacy Act

The CCPA also incorporates many of the same privacy concepts as the European Union's GDPR. The CCPA, however, operationalizes these European ideas through the property lens, where consent is framed as a series of negative rights that require consumers to opt-out of data collection and sharing. [36]

Privacy policies must incorporate informed consent under the CCPA. A privacy policy shall be "reasonably accessible to consumers" and outline the consumer's rights and "one or more designated methods for submitting requests" for information regarding the processing of the consumer's data.[37] It must also include "a list of the categories of personal information it has collected about consumers" that describes the personal information collected; "[a] list of the categories of personal information it has sold about consumers" that describes the personal information collected or a disclosure that the business has not collected information; and "[a] list of the categories of personal information it has disclosed about consumers for a business purpose" that describes the personal information disclosed, or a disclosure that the business has not disclosed any

33 *2019 Council Preparatory Document for Proposed ePrivacy Regulation*, *supra* note 17, at 66.

34 *See* discussion *infra* Section III.B about cookies.

35 *2019 Council Preparatory Document for Proposed ePrivacy Regulation*, *supra* note 17, at 67.

36 *See* Zwick & Dholakia *supra* note 13 (discussing the different lenses applied to privacy laws in the US and EU); *see also* CCPA, *supra* note 19, §§ 1798.110, 1798.115, 1798.120, 1798.125(b)(1), 1798.130(a)(5)(A) –(C), 1798.135(a)(2).

37 CCPA, *supra* note 19, § 1798.130(a)(5)(A)–(C).

information.[38]

The CCPA assumes that the information provided to the consumer in these privacy policies should be enough, then, for the consumer to opt-in or opt-out to certain described business activities. Consumers are permitted to enter into opt-in financial incentive agreements with businesses to sell their personal information when the agreement "clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time."[39] Businesses that are selling personal information to third parties are required to provide notice to consumers that their information is being sold.[40] The consumer has the right to opt-out of the sale of their personal information by directing the business to cease sales.[41] Unless the business later receives express authorization for the sale of the consumer's information, the business must refrain from selling the consumer's information indefinitely.[42]

The fatal flaw of the CCPA and the ePrivacy Regulation is their reliance on informed consent. Consumers cannot effectively evaluate the privacy tradeoffs and do not have all of the information that they need to make this assessment. Consequently, privacy can only be effectively regulated if it does not rely on consent. Although the ePrivacy Regulation better regulates the methods by which companies get informed consent from consumers, neither regulation is bold enough to remove consent altogether.

III. Informed Consent is Meaningless

Privacy decisions are irrational, and consumers' preferences can be easily swayed. Consumers may be willing to exchange privacy for "convenience, functionality, or financial gain, even when the gains are very small."[43] When faced with privacy-sensitive decisions, these seemingly irrational consumer preferences can by swayed through three distinct concepts: 1) information asymmetry; 2) bounded rationality; and 3) psychological distortions.[44]

38 *Id.*
39 *Id.* at § 1798.120(c).
40 *Id.* at § 1798.120(b).
41 *Id.* at § 1798.120(a).
42 *Id.* at § 1798.120(c).
43 Serge Egelman et al., *Choice Architecture and Smartphone Privacy: There's a Price for That*, in The Economics of Information Security and Privacy 211, 216 (Rainer Böhme ed., 2013).
44 Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, EC '04: Proc. 5th ACM Conf. on Electronic Com., May

The two different informed consent structures found in the CCPA and ePrivacy Regulation do not reflect the realities of the internet and the consumers using it. Both the CCPA and the ePrivacy Regulation attempt to require privacy policies that are easily accessible and understandable by the consumer in order for the consumer to better provide informed consent; yet these laws, and privacy policies in general, assume all consumers have the same level of understanding, thereby creating information asymmetries. Further, in 2012, the median length of a privacy policy was 2,514 words and would take a consumer seventy-six work days to read every policy they encountered.[45] Also, as the European Union saw with the implementation of the GDPR, consumers often experience a wearing down by the way these regulations and policies are designed to get informed consent.[46] Further, the ways in which websites are designed make consumers believe they are required to give consent, which present ethical and consumer protection problems.

A. Information Asymmetry & the Paradox of Choice

Facebook purports that it seeks to enhance consumer's understanding of their privacy settings throughout all aspects of its platform.[47] People are often surprised, however, when they are scrolling through their newsfeed on Facebook or Instagram and receive an advertisement for a product they have only talked about with their friends in person.[48] If consumers had all the information, would they

---

2004, at 21.

45 Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, 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/.

46 *See* Jessie Yeung, *Too Many GDPR Emails? Here's Some Light Relief*, CNN: BUSINESS (May 24, 2018), https://money.cnn.com/2018/05/24/technology/gdpr-jokes-memes-twitter/index.html. The GDPR required companies to request permission to continue sending emails to consumers, inundating consumers with emails "like the ramblings of a desperate ex-boyfriend." Sarah O'Connor (@sarahoconnor_), TWITTER (May 23, 2018, 7:25 AM), https://twitter.com/sarahoconnor_/status/999249873827483648.

47 *See* Sheera Frenkel & Natasha Singer, *Facebook Introduces Central Page for Privacy and Security Settings*, N.Y. TIMES (Mar. 28, 2018), https://www.nytimes.com/2018/03/28/technology/facebook-privacy-security-settings.html (citing Mark Zuckerberg, FACEBOOK (Mar. 21, 2018), https://www.facebook.com/zuck/posts/10104712037900071). *See generally* Association V.A.A., *Mark Zuckerberg Testifies on Capitol Hill. April 10, 2018.*, YOUTUBE (Apr. 10, 2018), https://www.youtube.com/watch?v=XmGbfsWMIZ4.

48 Facebook owns Instagram, WhatsApp, Occulus VR, FriendFeed, and LiveRail.

still be as surprised?

Information asymmetry is common between consumers and internet companies. Consumers are constantly asked to consent to privacy policies, cookies, and email marketing, and must do so by assessing each situation individually and guessing what the privacy tradeoffs will be.[49] Even in scenarios where the tradeoffs appear or should appear obvious, people perceive the risks differently and assess their own preferences in accordance with the risks presented.[50] Risk perception is also highly malleable: often consumers are influenced based on people who have better insight into consumer decision-making, and consumers' subsequent decisions are molded by those individuals.[51] "Much as seat belts in cars are justified by the fact that people's natural driving habits (as well as those of other drivers) create an unacceptable level of risk, privacy interventions can be justified by similar limitations of individuals' abilities to manage privacy-related risks."[52] Additionally, privacy harms and risks are difficult for consumers to properly assess because the harms are diverse and dependent on the context.[53]

Studies have examined how consumers make decisions, which can be used to help them make more rational decisions based on the risks and benefits of a transaction.[54] In one study, consumers were asked to purchase items using "Privacy Finder, a 'privacy-en-

Nathan Reiff, Nathan Reiff, *Top Companies Owned by Facebook*, INVESTOPEDIA (Mar. 1, 2019), https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp.

49 HARTZOG, *supra* note 10, at 37.

50 *Id.*

51 *Id.* at 36–37.

52 Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 J. SOC. PSYCHOL. & PERSONALITY SCI. 340 (2012).

53 HARTZOG, *supra* note 10, at 37.

54 Julia Gideon et al., *Power Strips, Prophylactics, and Privacy, Oh My!*, 2006 PROC. SECOND SYMP. ON USABLE PRIVACY & SECURITY, https://cups.cs.cmu.edu/soups/2006/proceedings/p133_gideon.pdf (concluding that "when privacy policy comparison information is readily available, individuals may be willing to seek out more privacy friendly websites and perhaps even pay a premium for privacy depending on the nature of the items to be purchased."); Janice Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 2007 INT'L CONF. ON INFO. SYS. PROC. 20, https://www.econinfosec.org/archive/weis2007/papers/57.pdf (concluding that providing accessible privacy rating icons on an online search engine reduced information asymmetry between merchants and consumers and "that once privacy information is made more salient, some consumers are willing to pay a premium to purchase from more privacy protective websites.").

hanced' search engine that displays search results annotated with the privacy policy information of each site."[55] These search results provided consumers with more complete information about the privacy risks and the study found that this made the tradeoffs easier for consumers to compute.[56] Timing and placement are crucial to closing the gap of information asymmetry.[57] For example, another study tested timing and placement of privacy indicators when shopping online, and concluded that both privacy-conscious and "non-privacy-conscious shoppers will pay more for privacy when indicators are presented before visiting websites rather than after the user has already selected a website to visit."[58]

If a consumer were to sit down and read every single privacy policy they were presented, it would take them over seventy-six business days.[59] Most of these privacy policies highlight that the consumer is in "control" of their data and information and that the consumer has the "choice" to use the service and sign up for the website.[60] This false sense of empowerment is the companies' way of having a "positive spin placed upon the structural reallocation of privacy."[61] The consumer is empowered to exercise control over how

55 Julia Gideon et al., *supra* note 54, at 3; *see also* Janice Tsai et al., *supra* note 54.

56 *See, e.g.*, Julia Gideon et al., *supra* note 54; Janice Tsai et al., *supra* note 54.

57 *See, e.g.*, THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY, *supra* note 43, at 217.

58 *Id.*

59 Madrigal, *supra* note 46. Also note that this article was published in 2012, indicating that possibly 8 years later it would take consumers even *longer*.

60 *See* HARTZOG, *supra* note 10 at 63–64 ("Control is an industry favorite privacy tool as well. To hear tech companies tell it, the answer to all modern privacy problems is just to give users more control. . . . People were said to have 'control' over their information when they were notified about a company's information collection, use, and disclosure practices and given a choice to opt out (usually by not using the service). . . . The most salient example of this notice and choice regime is the ubiquitous privacy policy: that dense, unreadable, boilerplate text tucked away in some corner of practically every website and application on the Internet."); *Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. On Commerce, Sci., & Transp.*, 116th Cong. 3 (2019) (testimony of Prof. Woodrow Hartzog) (identifying that the traditional approach to data protection results in "some combination of 'privacy self-management' concepts like control, informed consent, transparency, notice, and choice. These concepts are attractive because they seem empowering. They promise to put people in charge of what happens to their personal data. While notice and choice regimes enable the collection, use, and sharing of personal information, consumers are left . . . exposed and vulnerable.").

61 Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L.J. 1181,

their information is collected and used, but, ultimately, that means that they also bear the responsibility of "bad choices, even when . . . good options are limited or nonexistent."[62] The paradox of choice exists "such that people who experience more perceived control over limited aspects of privacy sometimes respond by revealing more information, to the point where they end up more vulnerable as a result of measures ostensibly meant to protect them."[63] Privacy can be seen as "flatter[ing] [the] sense of autonomy and accommodat[ing] . . . diverse notions of privacy and preferences for disclosure,"[64] yet when privacy policies are framed this way consumers are left more vulnerable.

Facebook's Data Policy in the United States ("Data Policy") is a prime example of information asymmetry and the paradox of choice. The Data Policy explains in clear and relatively simple[65] terms that it collects all of the following information about consumers: communication and other information while using the product, "including when you sign up for an account, create or share content, and message or communicate with others;"[66] content metadata (like photo location or content);[67] "people, [p]ages, accounts, hashtags and groups you are connected to and how you interact with them" across all of Facebook's platforms; contact information from devices that you upload, sync or import content from;[68] "types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; . . . the time, frequency and duration of your activities;"[69] "payment information, such as your credit or debit card number and other card information; other account and authentication information; . . . billing, shipping, and contact details;"[70] information and communications that your network provides across all of Facebook's platforms;[71] information

1203 (2017) [hereinafter *Privacy's Trust Gap*].

62 *Id.*

63 Laura Brandimarte et al., *supra* note 52.

64 *See Privacy's Trust Gap*, *supra* note 62.

65 There are a few terms that would still be unclear and are not explained in a manner that an ordinary consumer would understand, including the use of terms like API and SDK. *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last visited Apr. 28, 2019).

66 *Id.*

67 *Id.*

68 *Id.*

69 *Id.*

70 *Id.*

71 *Id.*

about your device's attributes, operations, identifiers, signals, settings, network and connection, and cookie data; information provided about your activities off Facebook by advertisers, app developers and publishers "including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services," whether or not you have a Facebook account or are logged into Facebook.[72] In short: every breath you take, every move you make, Facebook is watching you.

In order to make the consumer feel like they have power over their data, the Data Policy also uses the word "control" six times[73] and "choose" thirteen times,[74] but "the reality is that many consumers can't possibly understand how their data is being used and abused, and they don't have meaningful control when forced to choose between agreeing to turn over their data or not [using Facebook]."[75] Interestingly to this point, Facebook hides the fact that they track consumers whether or not they have an account.[76] This is probably the most egregious policy, and is listed one-half to two-thirds of the way through the Data Policy, so that by the time the consumer (if they ever take the time to read the policy) gets there, "the content is more familiar and the reader is more likely to skim information quickly. Thus, putting a point in the middle encourages the reader to skim the point quickly, with less involvement."[77]

With regard to the ePrivacy Regulation particularly, "studies show that even if [] 90% of experienced internet users claim to know cookies, only [] 15% can correctly answer any specific questions about them."[78] In a study of sophisticated Dutch users who

72 *Id.*

73 *Id.*

74 *Id.*

75 Neema Singh Guliani & Jay Stanley, *Three Big Battlegrounds in the Coming War over National Privacy Legislation*, ACLU (Oct. 23, 2018), https://www.aclu.org/blog/privacy-technology/internet-privacy/three-big-battlegrounds-coming-war-over-national-privacy.

76 *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last visited Apr. 28, 2019).

77 BEYOND THE BASICS: A TEXT FOR ADVANCED LEGAL WRITING 200 (Mary Barnard Ray & Barbara J. Cox eds., 3d ed. 2012); *see also Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last visited Apr. 28, 2019).

78 Joasia A. Luzak, *Privacy Notice for Dummies?: Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use In Order to Protect the Internet User's Right to Online Privacy*, 3 J. CONSUMER POL'Y 547, 547 (2014) (citing Anthony D. Myiyazaki, *Online Privacy and the Disclosure of*

were regulated by the 2012 version of the Directive, respondents answered on average four out of eight statements correctly about cookies, and only 0.2% of respondents answered all statements correctly.[79] The study found that "[m]ost of the misunderstandings regarded the idea that cookies save your browsing history, that cookies are person-based and that computers will slow down when cookies are not regularly removed."[80]

B. Wearing Down by Design

The concept of design is critical to developing privacy laws, as it can shape and erode consumers' reasonable expectations of privacy.[81] Design features center around altering how a product is brought into the market by thinking about how users will act and interact with the product from the beginning.[82] It involves getting software developers and entrepreneurs to think about privacy needs and expectations before even marketing a product.

When signing up for any web service or application, consumers are always asked to consent to the service's privacy practices, yet it is common knowledge that consumers do not read them. This practice and culture is so common in the United States, it has become the subject of satire on cultural norms.[83] Requiring consent works best in situations where consumers infrequently make such decisions,[84] as having a tsunami of consent emails renders them

Cookie Use: Effects on Consumer Trust and Anticipated Patronage, 27 J. PUB. POL. & MARKETING 19, 21 (2008)).

79 Edith G. Smit, et al., *Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe*, 32 COMPUTERS & HUM. BEHAV. 15, 17, 19 (2013). The ePrivacy Regulation modernizes the previous ePrivacy Directive, *see supra* Section II.A.

80 Edith G. Smit, et al., *supra* note 79, at 19.

81 HARTZOG, *supra* note 10, at 6.

82 Dr. Ann Cavoukian suggests that there are seven foundational principles to privacy by design: 1) proactive, not reactive; preventative not remedial; 2) privacy as the default; 3) privacy embedded into design; 4) full functionality—positive-sum, not zero-sum; 5) end-to-end security—lifecycle protection; 6) visibility and transparency; and 7) respect for user privacy. *See* Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices* (2011), https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

83 *See, e.g.*, *South Park: HUMANCENTiPAD* (Comedy Central broadcast Apr. 27, 2011) (depicting a satirical world where all but three people in a town read the updates to Apple's privacy policy).

84 Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1461 (2019) [hereinafter *The Pathologies of Digital Consent*].

useless because consumers cannot be expected to read them all.[85] Pew Research Center found that apps can seek 235 unique types of permissions (consent requests) from smartphone users, with most apps averaging five permissions before a user could install it.[86] Consumers will often "cheerfully disclose information about themselves to obtain particular transactional and relational advantages without pausing to consider the longer-term consequences."[87] For example, Sören Preibusch, Kat Krol, and Alastair R. Beresford recruited 1,500 web users for a study where they asked for "ten items of identity . . . of varying levels of sensitivity."[88] Users were compensated for participation in order to ascertain the costs of privacy invasion.[89] They ensured that participants understood that the additional disclosures were voluntary and that the information that they were providing was considered sensitive data.[90] Nevertheless, their study revealed that "[p]articipants regularly completed more form fields than required, or provided more details than requested."[91] They also observed that "making [certain] fields mandatory jeopardised [sic] voluntary disclosure for the remaining optional fields," finding that "as the number of mandatory fields in a form is increased, the total number of completed fields reduces".[92]

Consumers are also worn down and overwhelmed with advertisements on social media. Behavioral advertisements have become a norm, and consumers have accepted it as creepy because privacy policies are too difficult to understand. Marketers' and web sites' privacy policies do not adequately explain that super specific advertisements are placed in front of consumers using a combination of consumer data points that were bought and sold within

85 *See* Yeung, *supra* note 46 (discussing how the GDPR consent requests inundated consumers with emails, with one European citizen tweeting that they were allowing "all the GDPR emails [to] wash over me").

86 Michelle Atkinson, *Apps Permissions in Google Play Store*, PEW RES. CTR. (Nov. 10, 2015), https://www.pewresearch.org/internet/2015/11/10/apps-permissions-in-the-google-play-store/; *see also* HARTZOG, *supra* note 10, at 66.

87 Julie E. Cohen, *Irrational Privacy*, 10 J. TELECOMM. & HIGH TEC. L. 241, 242 (2018) (citing Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future*, 105 NW. U. L. REV. 1153, 1157–58 (2011)).

88 THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY, *supra* note 43, at 183, 202–03.

89 *Id.*

90 *Id.*

91 *Id.*

92 *Id.* at 183, 203.

200 milliseconds.[93] There is no utility value in reading such privacy policies since they are ineffective at explaining to the consumer how their information was used in a way that they can understand. For example, companies use internet behaviors in order to create different user segment groups and then show certain categories of consumers targeted advertisements.[94] These companies may track online behaviors through the use of cookies,[95] which "exchange . . . small strings of text characters, [and] information about the user's interaction at a particular visited Web site can be sent from the site to the user's hard drive and back when the user revisits the site."[96] Cookies are not tied to an individual's browser history,[97] but rather a user's clicks, including navigating from site to site, registering for newsletters, purchasing products, and perusing social media, are tracked by two different groups: first-parties and third-parties.[98]

First-party cookies embody the original intent of cookie development—they enhance a user's experience and interaction on a particular site by allowing the user to return at a later time and pick up browsing exactly where they left off.[99] First-party cookies allow consumers to fill their shopping cart on an online retailer and later come back to purchase the contents.[100] They also allow consumers to "purchase multiple items online in the same transaction. [Without cookies,] [e]ach time [consumers] add[] something to the cart from another page on the site, it would be treated as a new order."[101] On the other hand, third-party cookies are where privacy concerns multiply. Third-party cookies are often referred to as "tracking cookies" and monitor a user's clicks from site to site, purchase to purchase.[102] Third-party cookies place behaviorally targeted advertisements in

93 *Real-Time Bidding (RTB): The Complete Guide*, SMAATO, https://www.smaato.com/resources/real-time-bidding/ (last visited Apr. 20, 2019).

94 Smit, et al., *supra* note 79, at 17.

95 *Id.* at 15.

96 Janice C. Sipior et al., *Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons*, 10 J. INTERNET COM. 1, 2–3 (2011).

97 *See* Smit et al., *supra* note 79, at 19.

98 Sipior et al., *supra* note 96, at 3, 7–8; *see infra* Section II.B (discussing sales to third parties under the CCPA).

99 Sipior et al., *supra* note 96, at 2.

100 *Id.* at 8.

101 *First-party cookie*, PC MAG., https://www/pcmag.com/encyclopedia/term/43229/first-party-cookie (last visited May 1, 2019).

102 *See* Smit et al., *supra* note 79, at 15; *see also* Sipior et al., *supra* note 96, at 3 (2011).

front of consumers.[103]

Slowly, however, third-party cookies are becoming obsolete as marketers have developed complex algorithms that can help them understand how the consumer *feels* in real-time, allowing them to go deeper into the minds of consumers than ever before.[104] That Instagram advertisement for a product you were only just talking about was more likely a result of real-time bidding algorithms ("RTB"). To combat the dismal click-through rate on advertisements (0.11% globally), and to make "the digital display of advertising more ROI friendly," ad targeting companies use RTB functions which can now, "in real-time, capture, analyze and determine the 'audience' arriving on the Web site and serve targeted advertisements and communication."[105] This method of behavioral targeting has been adopted by industry leaders including Google, Yahoo, and Facebook.[106] It is impossible for a consumer to understand the technical underpinnings that are masked in privacy policies.[107]

Additionally, marketers and companies want the consumer to exert as little effort as possible when making a purchase on their website. In order to alleviate the pain of filling out the fields in the transaction, marketers focus on "lowering the cognitive and mechanical effort of completing forms" either through label positioning, the way in which mandatory fields are indicated, or "unified text field[s] to reduce tabbing and mouse-keyboard switching."[108] They want consumers to divulge as much information as possible by limiting the number of times a consumer's hands are lifted off

103 *See* Smit et al., *supra* note 79, at 15; *see also* Sipior et al., *supra* note 96, at 2.

104 *See* COGNIZANT, PEERING INTO THE FUTURE OF DIGITAL ADVERTISING 4 (2014), https://www.cognizant.com/InsightsWhitepapers/peering-into-the-future-of-digital-advertising-codex1018.pdf.

105 *Id.* ROI (return on investment) measures the efficiency of the investment as a ratio of profit to cost of the investment. James Chen, *Return on Investment (ROI)*, INVESTOPEDIA, https://www.investopedia.com/terms/r/returnoninvestment.asp (last updated Jan. 22, 2020).

106 COGNIZANT, *supra* note 104, at 4.

107 *See* Smit et al., *supra* note 79, at 19 (finding that "Only [0].2% of the respondents answered all of the statements [about cookies] correctly"); *see also id.* at 16 (citing A.M. McDonald & L.F. Cranor, *American's Attitudes About Internet Behavioral Advertising Practices*, 2010 PROC. 9TH WORKSHOP ON PRIVACY IN THE ELECTRONIC SOC'Y 63 (finding "half of American respondents believed that their location could not be identified if they did not accept cookies or that cookies contain information from when they purchased their computer . . .")).

108 THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY, *supra* note 43, at 185.

the keyboard.[109] Another way in which companies ensure the transaction requires as few clicks as possible is through autocompletion of web forms.[110]

Wearing down by design facilitates ineffectual regimes. Consumers alone cannot be expected to understand the nuances of the policies they are asked to consent to. They do not have the technical expertise to understand how their information can be used for their benefit and to their detriment. Further, consumers cannot reasonably be expected to wade through the large volume of technical policies that they are presented with on a daily basis. "Privacy policies become antiprivacy policies because companies know we will never read them."[111]

C. *Nudging & Dark Patterns*

Nudging is a type of dark pattern and is another technique that renders consumers' informed consent meaningless. Dark patterns develop when products are designed in a way that may not be in the user's best interest.[112] "Dark Patterns are tricks used in websites and apps that make you buy or sign up for things that you didn't mean to."[113] Websites may also "trick users into doing things that they might not want to do, but which benefit the business in question."[114] Nudging and dark patterns raise ethical implications, particularly with regard to deceptive and misleading practices.

Nudging leverages the design elements of attractiveness of choice, choice visibility, [115] and choice architecture[116] to coerce users

109 *See id.*

110 *See id.*

111 HARTZOG, *supra* note 10, at 66.

112 *The Privacy Advisor Podcast: Product Design as an Exercise of Power and Manipulation*, INT'L ASS'N OF PRIVACY PROFS. (Aug. 24, 2018), https://iapp.org/news/a/the-privacy-advisor-podcast-podcast-product-design-as-an-exercise-of-power-and-manipulation/.

113 Alexis Hancock, *Designing Welcome Mats to Invite User Privacy*, ELECTRONIC FRONTIER FOUND., (Feb. 14, 2019), https://www.eff.org/deeplinks/2019/02/designing-welcome-mats-invite-user-privacy-0 (quoting DARK PATTERNS, darkpatterns.org (last visited Mar. 9, 2020)).

114 *Id.* (quoting FORBRUKER RÅDET, DECEIVED BY DESIGN: HOW TECH COMPANIES USE DARK PATTERNS TO DISCOURAGE US FROM EXERCISING OUR RIGHTS TO PRIVACY 7 (Jun. 27, 2018) (Nor.), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.).

115 *See id.* (defining "attractiveness of choice" and "choice visibility" as "effectively warn[ing] some users about . . . hazards" present on the sites consumers were visiting).

116 *See* HARTZOG, *supra* note 10, at 35 (2018) (defining "choice architects" as

into following a predestined path. Nudges can serve to exploit cognitive and behavioral biases in consumers.[117] "Cognitive and behavioral biases are systematic errors in judgments and behaviors. . . . [T]hey represent deviations from the stylized economically rational behavior predicated by rational choice theory."[118] The designer behind the technology has the power "to nudge the user to take actions that the business would like the user to take."[119] Nudging uses design to alter consumers' "behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[120]

Presentation nudges provide contextual cues in the user interface to reduce cognitive load and convey what may or may not be the appropriate level of risk.[121] When first downloading the Facebook Messenger app, for example, it requests to be the consumer's primary SMS application and uses a bright blue box surrounding the "OK" response while the "Not Now" text is far less prominent, coercing the consumer to click "OK" even if they may not want to.[122] This same choice is presented on Venmo with the "Connect Facebook" option,[123] the Guardian with the "Become a Digital Subscriber" button on the homepage,[124] and even Spotify with the "Sign Up with Facebook" option.[125]

Another common example of design nudges are the embedded advertisements on Instagram: they look just like regular user posts, but if the consumer hovers over the image a bar pops up at the bottom of the image that says, "Shop Now." This native advertise-

"people who have 'the responsibility for organizing the context in which people make decisions.'").

117 Alessandro Acquisti et al., *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online*, 50 ACM COMPUTING SURVS. 44:1, 44:25 (2017).

118 *Id.* at 44:6.

119 Hancock, *supra* note 113.

120 HARTZOG, *supra* note 10, at 35 n.40 (quoting RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH AND HAPPINESS 3, 6 (2009)).

121 Acquisti et al., *supra* note 117, at 44:13.

122 Hancock, *supra* note 113.

123 *Id.*

124 GUARDIAN, https://www.theguardian.com/us (last visited Feb. 5, 2020).

125 *Get Spotify Free*, SPOTIFY, https://www.spotify.com/us/signup/?forward_url=https%3A%2F%2Fwww.spotify.com%2Fus%2Fdownload%2F (last visited Feb. 5, 2020).

ment[126] looks like it was posted by one of the consumers' followers, but secretly it is a company watching the consumer across the web. Design can be used to positively impact a consumer's visit to a website, but it can be used just as easily to manipulate their behavior.

The key with design is that it is never neutral.[127] "It is political. And it should be a key part of our information policy."[128] Again, using the Instagram advertisement as an example, it uses the advertisement to frame a select aspect of a consumer's perceived reality (looking like one of the consumers' followers) and makes the photo more salient in communicating to promote a particular result (clicking through on the advertisement and hopefully purchasing the advertised product).[129] "Once design affects our perceptions, it begins to shape our behavior. Once it shapes our behavior, it can be used to control us because it shapes what we perceive as normal. And once norms are established, they are difficult to change."[130] People can be expected, over time, to overshare information because it has become the norm and can be required as a condition to market entry.[131]

Consumers operating in a technological world are inherently irrational. Because consumers cannot possibly have all the information needed to provide meaningful consent to online operators, consent cannot be a valid measure of online operator practice. Regulations should not be framed in the context of consumer control because information asymmetries cause consumers to be manipulated to act in ways that the company believes will serve *the company's* best interests, which do not necessarily align with the best interest of the consumer. The consumer, however, has no way of evaluating these tradeoffs to understand if their consent to a particular policy is in their own best interest. In this regard, the CCPA is ineffective because it relies on companies providing consumers with information that, while maybe relevant, they will never get around to reading due to the utility value of privacy policies. While the ePrivacy Regulation frames the law as within the company's control,[132] consumers are still unaware of the policies they are consenting to and the technical parameters described therein.[133] Informed consent requires the con-

126 COGNIZANT, *supra* note 104, at 10.
127 HARTZOG, *supra* note 10, at 23.
128 *Id.*
129 *See id.* at 38–39.
130 *Id.* at 42.
131 Cohen, *supra* note 87, at 243.
132 As it places responsibilities on the companies, rather than the consumers.
133 *See* Smit et al., *supra* note 79.

sumer to have an understanding of *all* the information—not just the information that companies find relevant. Because of this, consent regimes cannot function in our current reality.

IV. WHY THE EPRIVACY REGULATION AND CCPA WILL NEVER WORK: PROPOSAL FOR NEW FOCUS IN LEGISLATION

It is this lack of reality that makes the futures of the consent regimes contained in the ePrivacy Regulation and the CCPA fairly predictable, even though their effects have yet to be seen.[134] Consent is an unnecessary and insufficient condition for privacy protection.[135] Consent regimes do not work.

The United States has a history of insufficient and inadequate consent regimes that have been manipulated in ways that are not beneficial to the individual. For one example, look at the history of abortion in the United States. Case law agrees that consent in this area of law must be truthful, relevant, and non-misleading, but state and federal legislatures, advocates, and courts disagree on what these terms actually mean.[136] For another, look at the many consent-based frameworks from criminal law in the United States, such as searches. In the context of Fourth Amendment searches, individuals who voluntarily turn over information to third parties have no reasonable expectation of privacy.[137] Until recently, voluntary disclosure was sufficient for location information, which many people,

134 As of this writing, the ePrivacy Regulation negotiations continue into 2020 under the Croatian presidency of the EU and the CCPA requires the California Attorney General to adopt regulations by July 1, 2020 to operationalize the law. *See* Osborne Clarke, *The e-Privacy Regulation: Latest Delays Leave Important Questions Unanswered*, LEXOLOGY (Dec. 3, 2019), https://www.lexology.com/library/detail.aspx?g=8e14f8b8-4000-4425-b944-d77153d8d913; CAL. ATT'Y GEN., INITIAL STATEMENT OF REASONS: PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATION (2019).

135 *See generally* Brandimarte et al., *supra* note 52; *The Pathologies of Digital Consent*, *supra* note 84. *See also* discussion *infra* Section IV.

136 Texas Med. Providers Performing Abortion Servs. v. Lakey, 667 F.3d 575, 578 (5th Cir. 2012) (citing Planned Parenthood v. Casey, 505 U.S. 833, 882 (1992)). *See* Sabrina Tavernise, *'The Time is Now': States are Rushing to Restrict Abortion, or to Protect It*, N.Y. TIMES, May 15, 2019 (discussing the tensions and variations between state laws, Supreme Court appointments, and advocates).

137 Until *Carpenter v. United States*, people were doubted to "entertain any actual expectation of privacy in the numbers they dial" because "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company." Smith v. Maryland, 422 U.S. 735, 743 (1979); *cf.* Carpenter v. United States, 138 S. Ct. 2206 (2018).

and now the Supreme Court, would claim is inadequate consent.[138] Individuals also cannot assert a reasonable expectation of privacy over trash that they placed outside their house since they voluntarily left it in a collection area, yet many citizens (maybe even society as a whole) could find this to be a serious invasion of privacy.[139]

Regulations based on the definitions of these terms result in cases pitting ideologies against each other instead of determining what is best for the individual. But, leaving these terms unregulated will also leave the individuals susceptible to the beliefs and opinions of the state actors. Either way, consent is not the answer in these situations.

Relying on consumer consent is inefficient. Consumers cannot constantly keep up with the rapid changes in technology and cannot be expected to read every new privacy policy that exists for every website or application they visit. Technological exceptionalism[140] should apply, and consumers should be given the benefit of the doubt. Information asymmetries are greater than ever before because of attitudes of technological determinism, where technologies are pushed into consumer mainstreams disregarding consumer harms, and regulations are only made *ex post facto*. Privacy policies should be the stepping stone to consumer education. Regulations governing privacy policies need to be precise, providing clear examples of what constitutes deceptive language and impermissible dark patterns. Because of the values in the United States, this will not be an easy regulation to draw, and, as this note will discuss, it could be considered as proscribing elements of speech, and creating two unequal groups for advertising.[141]

The ePrivacy Regulation gets closer towards this aim of pro-

138 *Compare* Carpenter v. United States, 138 S. Ct. 2206 (2018) *with Smith*, 422 U.S. at 743.

139 California v. Greenwood, 486 U.S. 35, 40–41 (1988); *see also* William Brinton, *Right to Privacy is Thrown Out with the Trash,* N.Y. TIMES, Jun. 1, 1988, at A30 (finding it "astonishing" that the Supreme Court concluded that individuals do not have a reasonable expectation of privacy over their trash and that the decision "places Fourth Amendment protection from warrantless searches well beyond the reach of even innocent people").

140 Technological exceptionalism is the belief that no two technologies can be compared. *See, e.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 358 (2019) (discussing how the Court in *Carpenter* applied technological exceptionalism by declining to entertain amici and scholars' Fourth Amendment reasoning, which relied on traditional disciplines such as history or economics).

141 Discussed *infra* Section V.

viding consumer education by requiring policies and mechanisms that warn consumers of how cookies work and by regulating software providers. Ironically, although the CCPA relies heavily on consumer consent, it is drawn in a more pro-business perspective, as it does not actually define or have a section that identifies what constitutes informed consent.[142] In order for businesses to know and understand how to educate consumers, the guidelines must be narrowly drawn in a regulation.

While tactics like nudging and wearing down by design have existed long before the internet, it may be time to begin to regulate some of these tactics (more than consent elements) due to technological exceptionalism. Because of the magnitude and quality of the data that is collected and traded, there are many ethical concerns with the way RTB and online behavioral advertisement targeting work. As demonstrated in the following paragraph, the four-step analysis from *Carpenter v. United States* could easily be adopted from the criminal law context and applied as a framework for regulation of RTB and other user interface/user experience regulations.[143]

Because RTB uses "sophisticated real-time algorithms that target specific customer profiles across devices, content, geographies, etc.," it provides companies with information of a "deeply revealing nature,"[144] which may allow companies to predict a consumer's thoughts and emotions long before the consumer is aware. Marketers, through RTB, have a more comprehensive reach than ever before due to the amount of information that can be tracked and collected across the internet.[145] The collection is necessarily "inescapable and automatic [in] nature," as marketers wear consumers down through design and use presentation and information nudg-

142 *Supra* Section II.B.

143 The four factors are: 1) the information is of a "deeply revealing nature;" 2) the information possesses "depth, breadth, and comprehensive reach;" 3) the information is collected in an "inescapable and automatic nature;" and 4) society does not expect that the information processed leads to a gain in efficiency. *Carpenter*, 138 S. Ct. at 2223; Ohm, *supra* note 140, at 366–69 (suggesting the fourth factor, efficiency gain, was also used in *Carpenter*).

144 COGNIZANT, *supra* note 104, at 4; *Carpenter*, 138 S. Ct. at 2223 (stating the first factor of the *Carpenter* test: the information is of a "deeply revealing nature.").

145 *See* COGNIZANT, *supra* note 104, at 4 (discussing how RTB algorithms can collect and track users across the internet); *Carpenter*, 138 S. Ct. at 2223 (stating the second factor of the *Carpenter* test: the information possesses "depth, breadth, and comprehensive reach.").

ing to exploit consumers.[146] All of this can be done due to efficiency gains: RTB is a cost-effective solution that allows marketers to access consumers in ways they never could before.[147] Despite the fact that this four-step analysis has already been used to evaluate the government's ability to request cell site location information from consumers when suspected of criminal activity in *Carpenter*, Congress has failed to take this rationale and apply it to user interface/user experience regulations. Funny, how nine justices who haven't "really 'gotten to' email"[148] have figured out a better framework than 535 Congress people with tech-savvy interns to help them.

V. The Proposed Deceptive Experiences to Online Users Reduction ("DETOUR") Act is Not a Beacon of Hope for US Regulation: Problems with Regulating Privacy by Design

Recently, United States Senators Mark Warner (D-VA) and Deb Fischer (R-NE) introduced a bill, the DETOUR Act, that would prohibit internet companies from "using deceptive design tricks as methods to trick users into handing over their personal data."[149] Warner commented that the "goal [of the bill] is simple: to instill a little transparency in what remains a very opaque market and ensure that consumers are able to make more informed choices about how and when to share their personal information."[150] While it may appear that legislators are getting the hint, the proposed Act still lacks a sense of reality.

The proposed DETOUR Act addresses user interfaces designed to obscure, subvert or impair individual autonomy, decision making, or choice; behavioral or psychological experiments on us-

146 *Carpenter*, 138 S. Ct. at 2223 (stating that the third factor of the *Carpenter* test requires that the information is collected in an "inescapable and automatic nature."); *see also* discussion *supra* Section III.B (discussing wearing down by design).

147 *See* COGNIZANT, *supra* note 104, at 4 (discussing the cost-effectiveness of TB). *See also* Ohm, *supra* note 140, at 366–69 (applying the fourth factor of the *Carpenter* test: society does not expect that the information processed leads to a gain in efficiency to RTB); *see generally Carpenter*, 138 S. Ct. at 2223.

148 Associated Press, *Kagan: Court Hasn't 'Gotten to' Email*, POLITICO (Aug. 20, 2013, 4:06 PM), https://www.politico.com/story/2013/08/kagan-supreme-court-email-095724.

149 Makena Kelly, *Big Tech's 'Dark Patterns' Could be Outlawed Under New Senate Bill*, VERGE (Apr. 9, 2019, 1:13 PM), https://www.theverge.com/2019/4/9/18302199/big-tech-dark-patterns-senate-bill-detour-act-facebook-google-amazon-twitter.

150 *Id.*

ers; and user interfaces that cultivate compulsive usage in users under the age of 13.[151] Interestingly, though the Act defines informed consent, the definition only appears to apply to behavioral or psychological studies.[152]

Similar to the CCPA, large online operators have a duty under the DETOUR Act to disclose certain information to consumers. They have a duty to "disclose to its users on a routine basis . . . any experiments or studies that user was subjected to or enrolled in with the purpose of promoting engagement or product conversion," and a duty to "disclose to the public on a routine basis . . . any experiments or studies with the purposes of promoting engagement or product conversion being currently undertaken, or concluded since the prior disclosure."[153] These disclosures must be presented in a "clear, conspicuous, context-appropriate, and easily accessible" manner, and must not be "deceptively obscured."[154] Unfair or deceptive acts are treated the same as under the Federal Trade Commission Act and are determined as having "the purpose, or substantial effect, of subverting or impairing user autonomy, decision-making, or choice to obtain consent or user data."[155]

The Act is framed as imposing a duty on large online operators instead of relying on consumer control. Framing the Act in the context of user interfaces that are designed to manipulate users suggests that these operators are acting in ways that are beyond the consumer's control and that the consumer cannot effectively consent to any of these behaviors. The Act rightfully takes into account that consent regimes do not work. While this is a step closer to the ePrivacy Regulation by seemingly assigning positive rights to consumers, there are two main problems this note argues (among many others) with regulating privacy by design that should be mentioned, though thorough discussion of each topic would be outside the scope of this note.

Acts such as the DETOUR Act, which seek to regulate and close the gap on information asymmetries, may be limited by commercial speech. Regulating privacy policies, notices, and interfaces

151 Deceptive Experiences to Online Users Reduction ("DETOUR") Act, S. 1084, 116th Cong. § 3(a)(1)(A)-(C) (as introduced to Senate Apr. 9, 2019) [hereinafter DETOUR Act].

152 DETOUR Act, *supra* note 151, at § 2(5)(A).

153 *Id.* at § 3(b)(1)–(2).

154 *Id.* at § 3(b)(3).

155 *Id.* at § 3(d)(2)(A).

interferes with the way online operators conduct their business and is highly paternalistic. For commercial speech to be protected by the First Amendment, according to the test proscribed by *Central Hudson*, it must, at a minimum, concern lawful activity and not be misleading.[156] Large online operators could attempt to argue that their privacy policies, notices, and interfaces are not misleading—possibly arguing that it is unreasonable to expect them to substantially modify their practices in order to predict the implicit biases or education of every potential consumer. Next, the government's asserted interest, providing transparency for consumers to provide informed consent while operating in the largely opaque online market, must be considered insubstantial or otherwise must not directly advance the asserted interest in a manner that is not more extensive than necessary.[157] If an online operator's practices are truly non-misleading, commercial speech issues should not arise. However, since there is little judicial interpretation of the FTC's guidelines for determining what is unfair and deceptive,[158] navigating this territory may require large online operators to conduct risk analyses to determine if their policies are appropriate. "There is, of course, an alternative to this highly paternalistic approach. That alternative is to assume that this information is not in itself harmful, that people will perceive their own best interests if only they are well enough informed, and that the best means to that end is to open the channels of communication rather than close them."[159]

The second problem about regulating privacy by design is on equal protection grounds. When certain types of advertisements are more heavily regulated than other types, an equal protection ar-

156 Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980) (establishing a four-part test for commercial speech: 1) whether the speech "concerns lawful activity and [is] not . . . misleading;" 2) "whether the asserted governmental interest is substantial;" 3) whether the regulation directly advances the governmental interest asserted;" and 4) "whether it is not more extensive than is necessary to serve that interest.").

157 *Id.* (holding that to be protected under the First Amendment, commercial speech must be related to a substantial governmental interest).

158 While the FTC has issued over 170 privacy related complaints, only three resulted in judicial opinions: FTC v. Accusearch Inc., 2007 U.S. Dist. LEXIS 74905 (D. Wyo. 2007); FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D. N.J. 2014); and LabMD, Inc. v. FTC 2014 U.S. Dist. LEXIS 65090 (N.D. Ga. 2014). Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L.R. 583, 611 (2014).

159 Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, 425 U.S. 748, 770 (1976).

gument by large online operators may arise. Privacy by design regulations tend to differentiate between data collection practices for advertising products online and offline.[160] The large online operators would argue that the basis of this distinction is not rationally justified by the purpose of the regulation, and violates the Equal Protection Clause of the Fourteenth Amendment.[161] It could be said that online advertisements are no less harmful to consumers than mailed coupons or advertisements for products. A classic example of this is when Target sent baby coupons to customers based on their "pregnancy scores," and was able to figure out a teen was pregnant before the teen's parents did.[162] Every time a consumer swipes their credit card or provides their zip code while checking out at a retail store like Target, the retailer collects the consumer's name and zip code and then purchases additional information about the consumer from a data broker, "including [their] age, marital status, education level, political leanings, hobbies and income level," to predict the consumer's next purchases.[163] Based on their predictions, the retailers mail consumers customized print advertisements and coupons.[164] Purchasing information from a data broker and using it to tailor advertisements to a particular consumer is not unlike how large online

160 *Compare* DETOUR Act, *supra* note 151 (regulating only certain online deceptive advertising practices), *with* Lara O'Reilly, *Walgreens Test Digital Cooler Doors with Cameras to Target you With Ads*, THE WALL STREET JOURNAL (Jan. 11, 2019), https://www.wsj.com/articles/walgreens-tests-digital-cooler-doors-with-cameras-to-target-you-with-ads-11547206200 (stating that Walgreens is testing a type of in-store advertising that would use similar techniques prohibited by the DETOUR Act. This technology would give companies "the ability to dynamically influence the shopper at the point of purchase and get them to add [their products] to the basket."); *see also* Ry. Express Agency, Inc. v. New York, 336 U.S. 106, 109–10 (1946) (holding that New York state could discriminate between different forms of advertisements, when the state had a legitimate governmental interest in protecting the safety of its citizens).

161 *See Railway Express Agency, Inc.*, 336 U.S. at 109 (stating petitioner's argument that "the classification which the regulation makes has no relation to the traffic problem since a violation turns not on what kind of advertisements are carried on trucks but on whose trucks they are carried.").

162 Kashmir Hill, *How Target Figured Out a Teen Girl was Pregnant Before her Father Did,* FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2526293e6668.

163 Melanie Hicken, *What Your Zip Code Reveals About You*, CNN: MONEY (Apr. 18, 2013, 9:59 AM), https://money.cnn.com/2013/04/18/pf/data-privacy/index.html.

164 *Id.*; *see also* Hill, *supra* note 162.

operators practice behavioral real-time marketing.[165] Yet once these tactics that are accepted for print advertising move online, privacy by design based regulations treat these practices differently. Although large online operators might argue that this unequal treatment violates the Fourteenth Amendment, as long as the "classification has relation to the purpose for which it is made and does not contain discrimination against which the Equal Protection Clause affords protection" their claims will face many challenges.[166]

While the DETOUR Act hits all the right points, it still lacks a sense of reality that is seen in much of the United States' regulations. In order to ensure that a national privacy law in the United States is enduring and realistic, it cannot be based on human rights or positive rights, as the United States interprets privacy as a property and negative right. So, while looking to Europe can provide useful ideas, privacy by design in the United States needs to be drawn in terms that are familiar to us and in terms that do not rely on our consent.

VI. Conclusion

Informed consent is meaningless in the area of privacy law when companies exploit consumers' irrational behaviors and inabilities to accurately and completely assess the tradeoffs of privacy disclosures. When companies manipulate consumers and use practices such as information asymmetries and the paradox of choice, wearing down by design, and nudging and dark patterns, consumers lack any real ability to consent in a meaningful way. They do not and cannot understand all the information that is relevant to their decision-making process and cannot properly evaluate the risks and benefits of disclosure. By inundating consumers with notices of consent, the quality of consent downgrades, making consent an inefficient and subpar mechanism for a regulation to rely upon when seeking to protect consumer privacy and companies' data collection practices.

165 *See* discussion *supra* Section III.B.

166 *See Railway Express Agency, Inc.*, 336 U.S. at 110 (holding that classifications of different types of advertising should take into account "practical considerations based on experience rather than [] theoretical inconsistencies that the question of equal protection is to be answered." They further found that "the fact that New York City sees fit to eliminate from traffic this kind of distraction but does not touch what may be even greater ones in a different category, such as the vivid displays on Times Square, is immaterial. It is no requirement of equal protection that all evils of the same genus be eradicated or none at all.").

While the CCPA, ePrivacy Regulation, and DETOUR Act function as prototype legislations for privacy law, they are imperfect. The CCPA still frames privacy as something within the consumer's control, by requiring privacy policies to be understandable to the reader. While it does require companies to outline certain rights and responsibilities, it falls flat by relying on informed consent, and there is no precise way to measure what constitutes a privacy policy that is reasonably accessible to consumers. In comparison, the ePrivacy Regulation relies heavily on clear, prominent notices that require affirmative consent, which may yield similar results to the opt-in GDPR notices that ultimately wore consumers down by design. It also relies on regulating a technology that is already slowly becoming obsolete, i.e. cookies, and does not necessarily anticipate the future of RTB and beyond. Consent regimes do not work. The DETOUR Act highlights that consumers do not and cannot have all the information and assigns responsibility to the large online operators. However, acts like this one, which legislate privacy by design, also must take into account first amendment and equal protection issues.

Consumers deserve a right to know how and why Facebook knew Bali was a dream destination of theirs or that their partner was going to propose, because what privacy really means is a right to be left alone—to choose to keep these things private. The surveillance of our most personal life is creepy because it's invasive and inevitable; corporations create monopolies by commodifying the thoughts, movements, and feelings of consumers. It's inescapable. Deleting your account doesn't work. And consumers have one option: accept the regime. This is not a norm that we can accept. I, for one, do not consent.