Washington Journal of Law, Technology & Arts

Volume 18 | Issue 4 Article 1

6-11-2023

WHAT YOU DON'T KNOW WILL HURT YOU: FIGHTING THE PRIVACY PARADOX BY DESIGNING FOR PRIVACY AND ENFORCING PROTECTIVE TECHNOLOGY

Perla Khattar
Notre Dame Law School

Follow this and additional works at: https://digitalcommons.law.uw.edu/wjlta

 Part of the Computer Law Commons, Entertainment, Arts, and Sports Law Commons, Intellectual Property Law Commons, Internet Law Commons, and the Privacy Law Commons

Recommended Citation

Perla Khattar, *WHAT YOU DON'T KNOW WILL HURT YOU: FIGHTING THE PRIVACY PARADOX BY DESIGNING FOR PRIVACY AND ENFORCING PROTECTIVE TECHNOLOGY*, 18 WASH. J. L. TECH. & ARTS (2023).
Available at: https://digitalcommons.law.uw.edu/wjlta/vol18/iss4/1

This Article is brought to you for free and open access by the Law Reviews and Journals at UW Law Digital Commons. It has been accepted for inclusion in Washington Journal of Law, Technology & Arts by an authorized editor of UW Law Digital Commons. For more information, please contact lawref@uw.edu.

WHAT YOU DON'T KNOW WILL HURT YOU: FIGHTING THE PRIVACY PARADOX BY DESIGNING FOR PRIVACY AND ENFORCING PROTECTIVE TECHNOLOGY

Cover Page Footnote

J.S.D. Candidate, Notre Dame Law School. Many thanks to Professor Patricia L. Bellia for expert input and generous guidance in writing this article, and to Professor Paolo Carozza, Professor John Maciejczyk, and Professor Kathleen Rice Mosier for their helpful comments. The author would like to dedicate this article to the soul of her uncle Jospeh Ajaka that passed away on August 10, 2022. Joseph is the reason Perla went to law school.

This article is available in Washington Journal of Law, Technology & Arts: https://digitalcommons.law.uw.edu/wjlta/vol18/iss4/1

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 18, ISSUE 4 — SUMMER 2023

WHAT YOU DON'T KNOW WILL HURT YOU: FIGHTING THE PRIVACY PARADOX BY DESIGNING FOR PRIVACY AND ENFORCING PROTECTIVE TECHNOLOGY

Perla Khattar[1*]

TABLE OF CONTENTS

[1*] J.S.D. Candidate, Notre Dame Law School. Many thanks to Professor Patricia L. Bellia for expert input and generous guidance in writing this article, and to Professor Paolo Carozza, Professor John Maciejczyk, and Professor Kathleen Rice Mosier for their helpful comments. The author would like to dedicate this article to the soul of her uncle Jospeh Ajaka that passed away on August 10, 2022. Joseph is the reason Perla went to law school.

INTRODUCTION

In 2018, Senator John Kennedy addressed Mark Zuckerberg during the Senate Judiciary Hearing on Facebook, Social Media, Privacy and the Use and Abuse of Data and said: "*your user agreement sucks."*[2] At that time, it felt like Senator Kennedy was voicing the frustrations of internet users who are tired of accepting click wrap agreements titled "privacy policy," and receiving targeted-advertisements that feel like a chip has been implemented in their brain. It only takes initiating a conversation with your next-door neighbor to realize that consumers are not happy with their lack of control over their personal information, yet, they feel helpless.[3] Even the savviest amongst us cannot escape EdgeRank[4] or PageRank.[5] A tech-savvy investigative journalist, Julia Angwin, documented her attempts at avoiding every form of digital surveillance known to man by using burner phones, using cash or credit cards with a fake name, and abstaining from the use of traditional social media.[6] Despite all her hard work, Angwin assessed her efforts as 50% successful.

Although despicable, these results are not shocking. In the cyber information age, the value of data to companies increased exponentially over time due to the possibilities of data mining, data application, and data value enhancements, leading to massive revenues.[7] However, the abundance of this stream of income is contingent on the processing of dozens of *petabytes* of personal information every day. In order to secure the data, companies created ecosystems that normalized the collection of personal data and offered services that heavily rely on consumer input. As a result, consumers started seeing the benefits of giving away their privacy to the tech-giants, reassured that if they ever decide to opt-out, privacy policies are there to protect their right to do so.

With this new reality in place, governments wished to regulate cyberspace, and issued legislations that heavily rely on individual privacy preferences. Instead of mandating the protection of personal information, data privacy laws gave consumers the option to protect themselves as per their personal valuation of privacy. These laws ignore the reality of the privacy paradox: a well-known concept in the field of information privacy that refers to the discrepancy between individuals' stated concern for their privacy and their actual behaviors, which often compromise their personal information.

Daniel Solove argues that individual preferences should not be the focus for establishing the value of privacy, or for determining whether regulation is needed.[8] He explains that the value of privacy is not based on a consumer's particular choice in a particular context.[9] To explain his view, Solove proposes a hypothetical where a consumer shares the name of her favorite book in exchange for a $1 discount from a bookstore online. He then asks what can be concluded from this

---

[2] Transcript of Mark Zuckerberg's Senate Hearing, Wash. Post (Apr. 10, 2018), https://perma.cc/Y7E3-PN5P.

[3] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH 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/.

[4] The algorithm that Meta uses to determine what articles should be displayed in a user's Facebook News Feed.

[5] The algorithm that Alphabet uses to determine the rank of web pages in their Google search engine results.

[6] Jacob Silverman, "*Dragnet Nation" Looks at the Hidden Systems that Are Always Looking at You*, L.A. TIMES (Mar. 6, 2014, 12:00 PM), https://perma.cc/3J4C-HQUS.

[7] Eric Jorstad, *Electronic Commerce in the 21st Century: The Privacy Paradox*, 27 Wm. Mitchell L. Rev. 1503, 1524-26 (2001).

[8] Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 23 (2021).

[9] *Id*. at 24.

behavior and offers 6 options: the person values privacy at only $1; the person values her own privacy at only $1; the person values the privacy of her personal data at only $1; the person values the privacy of her favorite book for only $1; the person values the data about her favorite book at only $1; or none of the above. Solove explains that the only acceptable answer is 'none of the above' because behavior in a particular situation does not reveal a consumer's valuation of privacy.[10] This is because "privacy is a constitutive element of a free and democratic society"[11] and it ought to be protected regardless of its value to specific consumers in a given situation.

The persistence of the privacy paradox is proof that current industry regulation is insufficient to protect consumer's privacy. Although consumer choice is essential, we argue that it should not be the main pillar of modern data privacy legislation. This article argues that legislation should aim to protect consumer's personal data in the first place, while also giving internet users the choice to opt-in to the processing of their information. Ideally, privacy by design principles would be mandated by law, making privacy an essential component of the architecture of every tech-product and service.

I. THE PRIVACY PARADOX: DEFINITIONS AND ORIGINS

"*Secrecy*," "*surveillance*," "*solitude*," "*transparency*," and "*limited access"* – the term 'privacy' has been used across time to mean different things.[12] One of the first scholastic works to define privacy in its contextual dimension was Samuel D. Warren and Louis D. Brandeis' article that called for broad protections against privacy intrusions.[13] In 1890, the authors imagined privacy to be the right to control the extent of one's data and to protect it from the press.[14] Almost 70 years later after the Warren and Brandeis' avant-garde article, William Prosser imagined a compartmentalized approach to privacy torts by grouping causes of action into four distinct categories: intrusion upon seclusion; public disclosure of private facts; publicity of false information; and appropriation.[15] Today, most of the 50 states of the United States recognize some parts of the common law of privacy.

In more recent years, Eric Jorstad defined privacy as "the state of being safe behind a wall which excludes others."[16] Privacy would also include the knowledge to build and maintain said wall and the power to set boundaries.[17] In other terms, privacy is the freedom to define and express one's self as one chooses.[18]

Across times and definitions, privacy has been proved to be valuable to individuals in a democratic society because its value transcends individual choices in specific times and situations. Daniel Solove gives 11 reasons to highlight why privacy is valuable: limit on the power of governments and companies; respect for individual's personhood; reputation management;

---

[10] *Id.* at 31-32.
[11] *Id*. at 34.
[12] Erin Husi, *No Means No: Why a Bright Line Against Data Sharing is The Best Line Forward for Privacy Legislation*, 2021 U. ILL. J.L. TECH. & POL'Y 519, 521 (2021).
[13] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 210-11 (1890).
[14] *Id*. at 196. ("The press is overstepping in every direction the obvious bounds of propriety and decency.").
[15] William Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960). Even though Prosser's four privacy torts were thoroughly litigated in the past decades, his static concept has not translated to the protection of privacy online, in particular, the protection of users from collection and sale of their online data.
[16] Jorstad, *supra* note 6, at 1504-05.
[17] *Id*.
[18] *Id*.

maintaining appropriate social boundaries; trust; control over one's life; freedom of thought and speech; freedom of social and political activities; ability to change and have second chances; protection of intimacy, bodies, and sexuality; and not having to explain or justify oneself.[19]

With the technological revolution of the age of information and telecommunication, more emphasis has been put on consumer's perception of privacy, giving rise to a new phenomenon: the privacy paradox. Although the concept itself is quite complex (and sometimes controversial[20]), defining the privacy paradox is simple: while consumers say that they are concerned about their privacy, they are willing to trade or sell aspects of this privacy for almost nothing.[21] Socially, the privacy paradox is the inconsistency that exists between "individuals' [asserted] intentions to disclose personal identifiable information ("PII") and [individuals'] actual disclosure behaviors."[22] At a granular level, consumers indicate specific personal information that they are not willing to disclose, but then give away the same data regardless of the risks associated with the disclosure.[23]

The first behavioral study to prove the presence of the privacy paradox was Sarah Spiekermann, Jens Grossklags, and Bettina Berendt's work.[24] The researchers compared the consumers' stated privacy preferences to the PII they disclosed to an anthropomorphic chat bot online. The study highlights that "participants displayed a surprising readiness to reveal private and even highly personal information and to let themselves be 'drawn into' communication with the anthropomorphic 3-D bot."[25] Even though the questions were often unimportant and illegitimate, consumers were ready to disclose their PII as long as they were able to perform their shopping activities.[26] Spiekermann and Berendt worked with Oliver Gunther on a study 5 years later where they found that consumers "do not always act in line with their stated privacy preferences, giving away information about themselves without any compelling reason to do so."[27] Another study by Alessandro Acquisti and Jens Grossklags revealed that 87.5% of consumers that had high concerns toward their privacy signed up for a loyalty card using their real information.[28]

The name "privacy paradox" was finally awarded to the disconnect between attitudes and behaviors concerning privacy in an article called "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors."[29]

Amongst privacy experts and enthusiasts, the most common response to the paradox phenomenon is skepticism. In the event of a conflict between what consumers report and what they do, actions are more valuable: simple statements reflect the consumer's aspirations, but

---

[19] Solove, *supra* note 8, at 46-47.
[20] H. Brian Holland, *Internet Expression in the 21st Century: Where Internet and Law Collide: Privacy Paradox 2.0*, 19 Widener L.J. 893, 893 (2010).
[21] *Id.*
[22] Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. Consumer Aff. 100, 100 (2007).
[23] *Id*.
[24] Sarah Spiekermann, Jens Grossklags & Bettina Berendt, *E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior*, in EC '01: Proceedings of the 3rd ACM Conference on Electronic Commerce 38, 38-39 (2001).
[25] *Id*. at 45.
[26] *Id*.
[27] Bettina Berendt, Oliver Gunther & Sarah Spiekermann, *Privacy in E-Commerce: Stated Preferences Versus Actual Behavior*, Commc'ns ACM, 101, 104 (2005).
[28] Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE Sec. & Priv., 26, 28 (2005).
[29] Norberg, *supra* note 21, at 100-01.

actions are an indication of actual intent.[30] This premise is unconvincing since consumers' actions may be heavily influenced by a lack of awareness, absence of options, or the non-belief in the law of large numbers ("NBLLN"). In simple terms, consumers tend to underestimate the amount of data that they are giving away to tech companies and what information this data reveals about their own person when combined with PII from other companies (in the event of a data exchange between tech companies).[31] Consumers are giving away their PII too easily, selling it too cheaply, and underestimating along the way how much tech companies can learn about their private life, and the private life of their acquaintances.[32]

II. ROOT CAUSES OF THE PARADOX

A presumption in classical economy theories is that in the absence of transaction costs, or when a product or service is labeled as "free," exchanges between rational self-interested parties are mutually beneficial and will lead to a beneficial allocation of resources.[33] However, this equation fails to hold due to power imbalance and inequality of the exchanges online: on the one hand, consumers aren't accurately able to estimate the marginal effects that this exchange has on their level of privacy, and often do not have another choice.[34] On the other hand, PII is valued so cheaply while tech giants are profiting billions from it. In 2021, the two biggest technology companies, Alphabet and Meta, earned 324.4 billion dollars in advertising revenue.[35] At this point, Alphabet is not a web-based search engine and Meta is not social networking service ("SNS"): they are simply new-age advertising companies that provide services in exchange for PII. Consumers that undervalue their personal data tend to trust these companies with their PII, leading to the privacy paradox phenomenon.

A. UNAVOIDABLE BYPRODUCT OF HUMAN EXISTENCE

Oscar H. Grandy sees that the creation of PII through the continual process of action and observation is an "unavoidable byproduct of human existence."[36] In a world where surveillance is normalized both online and offline, the indiscriminate production of PII is unavoidable.[37] This article argues that even the most privacy conscious individuals will unknowingly disclose a large amount of PII while doing everyday tasks.

When the PII is produced, it becomes available for collection, storage, use and transfer as a valuable commodity to companies that are in the business of processing PII either for commercial

---

[30] Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 Hastings L.J. 1471, 1488 (2018).
[31] *Id*. at 1489.
[32] *Id.*
[33] *Id.* at 1474-75.
[34] *Id.*
[35] Derek Saul, *Apple Crashes Advertising 'Duopoly': Google and Facebook's Stranglehold Loosening, Report Finds*, Forbes (Sep 6, 2022), https://www.forbes.com/sites/dereksaul/2022/09/06/apple-crashes-advertising-duopoly-google-and-facebooks-stranglehold-loosening-report-finds/?sh=1eb8935a5386.
[36] Oscar H. Grandy, Jr., *Toward a Political Economy of Personal Information*, 10 CRITICAL STUD. MASS COMM. 70, 76 (1993).
[37] Joel R. Reidenberg, *Privacy in the Information Economy: A fortress of Frontier for individual Rights?*, 44 FED. COMM. L.J. 195, 201-08 (1992).

or marketing purposes.[38] And instead of considering the collection, storage, use and transfer of PII an exchange of property, the market in PII is marked by vague consent collection.[39] Consumers cannot sell their PII, because at that stage, no property rights are vested. But once collected, property rights are created over the PII stored on the company's cloud.[40] Consumers can only conceal and manage the disclosure of their collected PII.[41] In short, in today's economy, consumers hold no property rights over their data. Whether they consciously protect their privacy or not, their digital footprint will end up on a BigTech company's cloud somewhere down the line.

Some experts even go the extra mile to assert that consumers not only "have the right to manage privacy trade-offs without regulative intervention, but . . .. individuals can, in fact, use that right in their own best interest."[42] Which means that consumer's concern over privacy is not absolute,[43] since they are willing to trade-off these concerns for economic benefits, convenience, personalization[44] and the mere ability to use a website.[45]

But a consumer's ability to bargain with the companies processing PII is limited to the initial transaction where the user can either disclose or conceal the data[46] as per the terms of the privacy policy.[47] The idea that the privacy paradox is illusory, overstated and optimal[48] disregards the fact that in the absence of effective legislation, the limited choices offered to consumers by monopolies are calculated, and ensure the eventual collection, storage, use, and transfer of PII.

B. HINDERED DECISION-MAKING PROCESS

Alessandro Acquisti and Jens Grossklags consider three factors when explaining why the decision-making process with regard to digital privacy is hindered: "incomplete information; bounded rationality; and systemic psychological deviations from rationality."[49] These factors help explain the existence of the paradox, and why the observed behaviors aren't always rational.

First, consumers possess incomplete information about the online transactions that they are entering in, which translates to a lack of full awareness of the nature and the frequency of privacy

---

[38] Craig D. Tindall, *Argus Rules: The Commercialization of Personal Information*, U. ILL. J.L. TECH. & POL'Y 181, 182-87 (2003).
[39] Hal R. Varian, *Economic Aspects of Personal Privacy, in Internet Policy and Economic Challenges and Perspectives*, U.C. BERKELEY (2009).
[40] Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM, 92, 93 (1996).
[41] Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393-409 (1978).
[42] Acquisti & Grossklags, *supra* note 28, at 26.
[43] Il-Horn Hann et al., *Online Information Privacy: Measuring the Cost-Benefit Trade-Off*, in Twenty-Third International Conference on Information Systems 1, 8 (2002).
[44] Ramnath K. Chellappa & Raymond G. Sin, *Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma*, 6 INFO. TECH. & MGMT. 181, 184-86 (2005).
[45] Kai-Lung Hui & I.P.L. Png, *The Economics of Privacy*, *in* HANDBOOKS OF INFORMATION SYSTEMS: ECONOMIC AND INFORMATION SYSTEMS 471, 489-90 (Emerald Publ., 2006).
[46] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2077 (2004) (in the absence of effective laws that protect this transaction, privacy policies written by companies govern the transaction).
[47] Allyson W. Haynes, *Web Site Visitors and Online Privacy: What Have You Agreed to Share*?, S.C.L., 27, 29 (2008) (in the absence of effective laws that protect these transactions, privacy policies written by companies will be applicable. Both parties are bound by the policy, where no minimum standard of privacy protection is required in most cases).
[48] Richard A. Posner, *The Economics of Privacy*, 71 Am. Econ. Rev. 405, 406 (1981).
[49] Acquisti & Grossklags, *supra* note 27.

infringements.[50] Additionally, consumers may not be aware of the risks associated with data disclosure, the benefits of protecting PII, the probability of a data breach, misuse or infringement until after the fact.[51] Most consumers will not be aware of the existence of protective technologies that can help them manage their privacy preferences.

Asymmetric and incomplete information, often called "lemon market," hinders the decision-making -process of consumers, because this information is often only known to one side of the transaction.[52] In fact, the company processing PII "know[s] a good deal more about how it uses the personal information it collects than [the data subject knows]."[53] In parallel, Paul Sholtz observes that "for most people, it is difficult just to find and understand a company's privacy policy, much less to monitor the company's use of personal information and detect when violations have occurred."[54]

Additionally, as per the bounded rationality concept, consumers are unable to acquire, memorize and process information relevant to the division-making process:[55] in the privacy sphere, consumers are unable to calculate the potential payoffs in privacy-sensitive situations due to the inability to process the stochastic information related to the associated risks.[56]

In this lemon market, we believe that consumers are not deciding freely to sell their PII to be able to browse the internet – to the contrary, consumers do not have another choice in most cases. Quoting Acquisti and Grossklags: "even the most privacy-concerned individuals are not informed and cannot inform themselves about privacy risks, even when that information is available . . . . and instead resort to simplified mental models, approximate strategies, and heuristics."[57]

C. NONNEGOTIABLE CLICK-THROUGH AGREEMENTS

Contracts for the disclosure of PII online are nonnegotiable and standardized,[58] meaning that consumers have to either accept the terms and conditions or go elsewhere due to their lack of bargaining power. [59] Consumers are often presented with a sophisticated version of adhesion contracts called "click-through" or "shrink-wrap" agreements[60] where consent is collected in a non-informed way.[61] This calls into question the legitimacy of these standardized contracts where individualized bargaining and real assent are quasi-absent.

---

[50] *Id*. at 23.
[51] *Id*.
[52] Acquisti & Grossklags, *supra* note 27, at 38.
[53] Paul Sholtz, *Transaction Costs and the Social Costs of Online Privacy*, First Monday (May 2021).
[54] *Id*.
[55] Acquisti & Grossklags, *supra* note 27, at 27.
[56] *Id*. at 23.
[57] *Id*. at 27.
[58] Wayne R. Barnes*, Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. Davis L. Rev. 1545, 1573 (2006).
[59] *Id*. at 1608.
[60] *Id*. at 1573.
[61] *Williams v. Walker-Thomas Furniture Co*., 350 F.2d 445, 449 (D.C. Cir. 1965).

In fact, consumers are no longer reading terms of service and privacy policies due to renegotiation not being possible.[62] Not only that, but courts are unwilling to apply traditional contractual remedies of unconscionability, duress, fraud, etc., to online standardized contracts.[63]

D. SOCIETAL TRANSFORMATION DRIVING PII DISCLOSURE

Social organization evolved "from little boxes to social networks;" Barry Wellman describes that humans went from living in groups, to glocalization and now to networked individualism.[64] According to Wellman, glocalization is the shift from bounded groups such as neighborhoods, to glocalized relationships in households and worksites with interactions based on shared interest rather than shared kinship.[65] However, technology catalyzed a new societal transformation by connecting people all around the world: with networked individualism, people are connected across larger networks via cellphone instant messaging and e-mails.[66] Empirical data supports Wellman's theory: a Pew Research Center study found that "social relationships are not fading away," but rather transforming.[67] The study also shows that "the internet is enabling people to maintain existing ties, often to strengthen them."[68]

To better understand how societal transformation correlates to the privacy paradox, we are going to imagine Facebook as a platform for social production.[69] Facebook is a user-supplied product where consumers are motivated to share their PII due to the accumulation of social capital[70] in the gift economy.[71] Humans' need to preserve communities leads them to stay connected on SNSs. However, for a true connection to be built online, sharing basic identifiers and contact information is not enough to reveal the true expression of one's self.[72] As per James Grimmelmann, the reason why consumers entrust Facebook with their PII is because they have social reasons to do so: consumers want to participate in social life online, which explains the trust in Facebook (and other SNSs) despite the risks, and the underestimation of those risks.[73] With the average consumer spending 147 minutes on social media,[74] the need to participate in social life online seems evident.

---

[62] Holland, *supra* note 19, at 907,

[63] See, e.g., *Bishop v. Washington*, 480 A.2d 1088, 1094 (Pa. Super. Ct. 1984); *Koval v. Liberty Mut. Ins. Co*., 531 A.2d 487, 491 (Pa. Super. Ct. 1987).

[64] Barry Wellman, *Little Boxes, Glocalization, and Networked Individualism*, in Digital Cited II: Computational and Sociological Approaches 10, 10-12 (2002).

[65] *Id*. at 13.

[66] *Id*. at 15-16.

[67] Jeffrey Boase et al., *The Strength of Internet Ties: The Internet and Email Aid Users in Maintaining Their Social Networks and Provide Pathways to Help When People Face Big Decisions*, PEW INTERNET & AM. LIFE PROJECT 42(2006).

[68] *Id*. at 3.

[69] Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, 3 YALE UNIVERSITY PRESS 91-92, 99, 106 (2006).

[70] *Id*.

[71] Steven A. Hetcher, *Hume's Penguin, or, Yochai Benkler and the Nature of Peer Production*, 11 VAND. J. ENT. & TECH. L. 963, 986 (2009). Consumers share their PII because their friends, family and colleagues are sharing their PII, leading to an exchange of social capital.

[72] James Grimmelmann, *Saving Facebook*, 94 Iowa L. Rev. 1151 (2009).

[73] *Id*.

[74] *How Much Time Does The Average Person Spend on Social Media*?, OBERLO (2022), https://www.oberlo.com/statistics/how-much-time-does-the-average-person-spend-on-social-

Brian Holland adds that "just as the transformation of social organization drives us to join these networks, so too does the primary need for community encourage the centralization and distribution of our personal data."[75] The depth of PII shared on social networks is due to the process of identity performance, because traditional personality cues such as accent, style and dress are not by default found online.[76]

The networks are also commercially architected in a way that motivates the contribution of PII by consumers for the accumulation of social capital.[77] For these reasons, individuals are incentivized to share text, images, audio and video online, leading to the processing of this PII by companies.

The paradox exists, it's simply not due to the apparent reasons. Therefore, any privacy legislation that disregards the social dynamics of privacy and online interactions is bound to fail at protecting consumer's PII.[78] For example, ex ante privacy controls whereby consumers set their preferences when first registering with the SNS, although good in theory and on paper, do not account for the nuances of evolving social interactions.[79]

E. NOTICE AND CHOICE MODEL

The creation of Privacy policies started in the early 2000s in an attempt to inform users of the ways companies shared and used this data.[80] At that time, the Federal Trade Commission ("FTC") highly recommended privacy policies to inform consumers of site's data collection practices based on *the principle of notice and choice.*[81]

In today's economy, the continued reliance on privacy policies is influenced by major privacy legislations that continue to require and mandate these policies. For instance, Europe's General Data Protection Regulation ("GDPR"), ratified by the European parliament in 2016 and effective in 2018, requires privacy policies to be concise and written in simple and plain language.[82] With the GDPR, policies filled with technical and opaque language became readable and straightforward,[83] therefore disguising the intricacies of data sharing. The California Online Privacy Protection Act mandates the use of privacy policies to all operators' websites, including mobile phone applications, that are accessible and collect PII from Californians.[84]

---

media#:~:text=your%20free%20trial-,Average%20time%20spent%20on%20social%20media,also%20the%20highest%20ever%20recorded.

[75] Holland, *supra* note 20, at 918-19.

[76] Grimmelmann, *supra* note 72, at 1152-53.

[77] Catherine Dwyer et al., TRUST AND PRIVACY CONCERN WITHIN SOCIAL NETWORKING SITES: A COMPARISON OF FACEBOOK AND MYSPACE, in Ass'n For Info. Sys., 13th Americas Conference on Information Systems (2007).

[78] Grimmelmann, *supra* note 72, at 1178-95.

[79] *Id*. at 1185-86.

[80] Husi, *supra* note 12, at 523.

[81] Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, 21 New Media & Soc'y 1824, 1831 (2019).

[82] *Commission Regulation* 2016/679, 2016 O.J. (L 119) 1.

[83] Deloitte, *A New Era for Privacy* 7 (2018), www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf.

[84] California Online Privacy Protection Act, Cal ALS 829, 2003 Cal AB 68, 2003 Cal Stats. ch. 829. Indirectly, CALOPPA applies to every business operating in the United States because serving one Californian falls within the scope of the law.

However, privacy policies are statements issued by companies to declare their privacy practices to a public of consumers, and do not guarantee any right to privacy.[85] Admittedly, the existence of extensive privacy policies often gives the wrong impression to consumers that think their data is protected.[86] Studies have shown that consumers who actually read privacy policies have a tenuous grasp of the purpose of these policies.[87] Another study highlighted that more than half of the respondents thought that the presence of a privacy policy means that the company keeps confidential the information collected.[88] In fact, privacy policies are corporate disclaimers, designed to maintain regulatory compliance, and they are in no way consumer guarantees. Senator John Kennedy addressed Meta's founder Mark Zuckerberg during the memorable 2018 Senate hearings and confirmed this idea: "[t]he purpose of a user agreement is to cover Facebook's rear end, not inform users of their rights."[89]

To gain consumers' trust, some companies have enacted transparency initiatives.[90] But, similarly to privacy policies, these transparency initiatives are tools that inform consumers on data manipulation practices without giving them any increased control over the collection and sale of their PII.[91]

On this matter, the transformative marketing agency Axciom launched a program called "About the Data" that seeks to disclose to consumers how their data was used in marketing.[92] However, what the modern consumer didn't know was that Axciom only disclosed a portion of the PII that they process, without giving their consumer the right to control, the right to delete, or the right to manage their entire data.[93] These transparency initiatives are more words than actions and they do not increase the protection of consumer's PII.[94]

The notice and choice model makes individual privacy decision-making the main source of protection, even though it has been proven to be ineffective from a practical standpoint.[95] Tsai et al. demonstrated that the mere existence of a privacy policy tends to increase PII disclosure, regardless of whether the consumer reads or understands the contents of the program.[96] In a study conducted by Professor Joseph Turow, it was found that 75% of people incorrectly believed that

---

[85] The same thing could be said about Chief Privacy Officers (CPO) or Data Protection Officers (DPO) mandated by the GDPR. The existence of these positions does not mean that companies are consciously trying to protect the privacy of their consumers. To the contrary, these positions ensure bare minimum compliance required by law to avoid troublesome fines and penalties. Even though consumers might get the impression that their data is in safe hands being handled by a CPO or a DPO, the reality dares to say otherwise.

[86] Draper & Turow, *supra* note 81.

[87] *See* Joseph Turow et al, *The Tradeoff Fallacy: How Marketers Are Misrepresenting Consumers and Opening Them Up To Exploitation* 8 (2015).

[88] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RESEARCH CENTER (Dec. 4, 2014) https://perma.cc/9GBKH4HM.

[89] *Transcript of Mark Zuckerberg's Senate Hearing*, WASH. POST (Apr. 10, 2018) https://perma.cc/Y7E3-PN5P.

[90] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Book and on the Ground*, 63 Stan. L. Rev. 247, 266 (2011).

[91] *Id*. at 301, 302.

[92] Matthew Crain, *The Limits of Transparency: Data Brokers and Commodification*, 20 New Media & Soc'y 88, 92-93 (2018).

[93] *Id*.

[94] Husi, *supra* note 11, at 525-26.

[95] Lindsey Barrett, *Modeling Privacy: Empirical Approaches to Privacy Law and Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 12 (2018).

[96] Janice Tsai et al., *What's it to You? A survey of Online Privacy Concerns and Risks*, NET Inst., Working Paper No. 06-29 (2006), http://ssrn.com/asbtract-941708.

"when a website has a privacy policy, it means the site will not share [their] information with other websites and companies."[97] Additionally, another 2005 study revealed that 41% of individuals who consider themselves concerned about their privacy actually read privacy policies.[98]

These policies fail to provide consumers with a way to manage the processing of their PII due to the inability to engage with these policies.[99] In fact, a study by professor Kristen Martin showed how consumers wrongly interpreted privacy policies to be "more protective of consumer data than the actual notice included in the survey"[100] and "respondents projected the important factors to their privacy expectations onto the privacy notice."[101] These policies became a tabula rasa for consumer's overly-optimistic privacy expectations. This makes privacy policies the most frequently cited indications that individuals do not care about their privacy.[102]

F. THE CONSUMER'S IGNORANCE OF THE TECHNICAL ASPECT

In 2021, WhatsApp released their new privacy policy that indicated how the company was collecting activity, device and connection logs, on top of interactions with business accounts,[103] resulting in a massive outrage due to data accumulation.[104] Earlier in 2018, the revelation of data-sharing arrangements between Spotify, Amazon and Netflix indicated how these giants have access to PII far beyond what has been previously disclosed.[105] Anna Wiener detailed the specificity with which data can be segmented by age, gender, political affiliation, hair color, dietary restrictions, body weight, income bracket, favorite movies, education, sexual kinks, proclivities, country, city, cell phone carrier, device type, and a unique identification code, among others.[106]

Meta also agreed to pay a $5 billion fine to the FTC in 2019 for misrepresenting to consumers: the extent to which consumers can control their privacy settings; the steps consumers could take to implement privacy controls; and the extent to which Facebook shares an individual's PII with third-parties.[107] In the same year, over 5100 publicly disclosed data breaches occurred,

---

[97] Joseph Turow, Lauren Feldman & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline* 3 (2005).
[98] Acquisti & Grossklags, *supra* note 27.
[99] See, e.g., Kristen Martin & Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables*, 18 Colum. Sci & Tech. L. Rev. 176, 180 (2016).
[100] Kristen Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. Pub. Pol'y & Mktg. 210, 219 (2015).
[101] *Id*. at 220.
[102] *Id*.
[103] Daniel Cooper, *WhatsApp Reassures Users It Can't Read Their Messages*, ENGADGET(Jan. 12, 2021), https://www.engadget.com/whatsapp-privacy-policy-changes-statement-encryption-surveillance-172224753.html.
[104] Lily Hay Newman, *WhatsApp Has Shared Your Data with Facebook for Years, Actually*, WIRED(Jan. 8, 2021, 1:52 PM), https://www.wired.com/story/whatsapp-facebook-data-share-notification.
[105] Alexis Madrigal, *Facebook Didn't Sell Your Data; It Gave It Away*, THE ATLANTIC (Dec. 19, 2018), https://www.theatlantic.com/technology/archive/2018/12/facebooks-failures-and-also-its-problems-leaking-data/578599.
[106] ANNA WIENER, *UNCANNY VALLEY: A MEMOIR,* 43 (2020).
[107] Plaintiffs' Consent Motion for Entry of Stipulated Order for Civil Penalty, Monetary Judgement, and Injunctive Relief and Memorandum in Support , at 6, United States v. Facebook, Inc. No. 19-cv-2184 (D.D.C. 2020); United States v. Facebook, Inc., 2020 U.S. Dist. LEXIS 72162, at 10 (D.D.C. 2020).

leading to a total of 7.9 billion exposed records: a 33% increase from 2018,[108] and the latest data is showing a 68% increase.[109]

Gmail, Alphabet's email service, reads emails and pushes out advertisements based on the collected coordinated data.[110] This statement is not based on studies we have consulted or conducted, to the contrary, this fact is spelled out in Google's privacy policy. Consumers provide Gmail a limited amount of PII in exchange for email services. Then, Gmail recedes into the background and gathers PII based on the email exchanges between users. Even though Gmail claims to not pass PII to third-parties except when required by a warrant, advertisements are pushed out to consumers based on the collected data. Yet, consumers are still unaware of Google's data practices that affect 2 billion consumers every year.[111]

The average consumer is not to blame when it comes to privacy literacy: a study at Princeton demonstrated how a consumer could make the deliberate choice to turn off location services on their smartphone, expressing a desire to not have their location communicated to any company. Yet, the geolocation can still be deduced from other sources of publicly available information.[112] Therefore, when consumers are not fully informed and are not taking proactive steps to protect their PII, the outcome is not always desirable.

Some privacy legislation dissenters will still argue that consumers do not care about their privacy, since they are not taking any proactive steps to protect it. Yet, how many consumers actually know that Gmail reads their emails? Or the ins and outs of Facebook's privacy settings? Or the details of every data breach happening around the world? Consumers, for the most part, are ignorant about the technical aspects of tech companies' operations. We will be covering this topic in more details later in the paper.

G. PRIVACY RESIGNATION

In a survey conducted in 2015, 58% of consumers expressed two distinct statements: "[i] want control over what marketers can learn about me online" and "[i]'ve come to accept that I have little control over what marketers can learn about me online."[113] The power imbalance between companies processing PII and consumers is called *privacy resignation*. In other terms, privacy resignation is the reconciliation of the desire to control the information that companies processing PII have with an inability to do so.[114]

In a study conducted by Eszter Hargittai and Alice Marwick, young respondents expressed awareness of many risks associated with disclosing their PII online, but felt resigned to their limited control over their data: "participant comments suggest that users have a sense of apathy or cynicism about online privacy, and specifically believe that privacy violation are inevitable and

---

[108] Rae Hodge, *2019 Data Breach Hall of Shame: These Were the Biggest Data Breaches of the Year*, CNET (Dec. 27, 2019, 4:00 AM), https://www.cnet.com/news/privacy/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/.

[109] Bree Fowler, *Data Breaches Break Record in 2021*, CNET (Jan. 24, 2022, 12:31 PM), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/.

[110] Google, *Gmail Privacy Policy*. https://policies.google.com/privacy?hl=en-US (last visited Jan 24, 2022).

[111] Rande Price, *Consumers Are Unaware of Many of Google's Data Practices*, DIGITAL CONTENT NEXT(April 5, 2019) https://digitalcontentnext.org/blog/2019/04/05/consumers-are-unaware-of-many-of-googles-data-practices/.

[112] Arsalan Mosenia et al., *PinMe: Tracking a Smartphone User Around the World*, 4 Inst. Electrical & Electronic Engineers Transactions On Multi-Scale Computing Systems 420, 420 (2017).

[113] Draper & Turow, *supra* note 81, at 1824.

[114] *Id*.

opting out is not an option."[115] A 2008 study famously estimated that it would take the average American consumer 49 minutes per day to read and examine every privacy policy they came across, which aggregates to a cost of $2,533 to $5,038 a year.[116] From reading privacy policies, terms of service, checking permissions on every website, application or Internet of Things ("Iot") device, consumers are faced with a constant barrage of privacy choices, which makes it challenging to take decisions that accurately reflect their wishes and preferences.[117] Managing one's privacy is complex, vast and virtually impossible at scale.[118]

With these facts in mind, the privacy paradox seems like a logical result of the phenomenon of privacy resignation. In fact, this would explain why consumers that are actively concerned with the protection of their privacy are less likely to engage in privacy-protected behaviors or even risky behaviors.[119] We see that the privacy paradox is an accurate indication of the lack of options to consumers wishing to protect their privacy yet have little to no technical literacy, rather than an affirmation of the idea that consumers do not care about privacy.

Legislation like the California Consumer Privacy Act ("CCPA") and the GDPR rely on a model of self-management that promotes the right to opt-out but fails in application due to lack of consumer awareness.[120] These laws give consumers robust rights to find out about the PII that companies are processing, with the right to opt out of the sale of their PII to third parties.[121] But, these laws do not scale well. Thousands of companies process PII, and expecting consumers to make thousands of requests and to opt out thousands of times is unrealistic.

In short, giving the consumer the right to opt-out of the sale of their data has little to no efficacy if the consumer is encumbered by the burden of sending in requests, or if the consumer simply does not trust the company processing the data.

H. NON-BELIEF IN THE LAW OF LARGE NUMBERS (NBLLN)

The NBLLN phenomenon is the idea that in very large samples, proportions of binary signals might depart significantly from the population mean. First and foremost, the effect of the NBLLN phenomenon is not limited to the online context, but the problem is particularly acute in the digital domain due to the high volume of data that can be collected in the digital sphere compared to the analogue world.[122] This leads individuals that are afflicted by NBLLN and are suffering from information overload to have a hard time grasping how important and valuable their data is and how effective machine learning algorithms are at extracting data.

Stango et al. proved that NBLLN is among the most prevalent behavioral factor in the population: their study proved that 87% of participants exhibited NBLLN.[123] In other terms, a huge

---

[115] Eszter Hargittai & Alice Marwick, *"What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy*, 10 INT'L J. COMM. 3737, 3741, 3752 (2016).
[116] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFOR. SOC'Y 543, 544 (2008).
[117] Barrett, *supra* note 95, at 23.
[118] Solove, *supra* note 8, at 5-6.
[119] Young Min Baek, *Solving the Privacy Paradox: A Counter-Argument Experimental Approach*, 38 COMPUT. HUM. BEHAV. 33, 34 (June 11, 2014).
[120] Solove, *supra* note 8, at 30.
[121] *Id*. at 46-47.
[122] *Cofone & Robertson*, supra note 30, 1490-91.
[123] Victor Stango et et., *The Quest of Parsimony in Behavioral Economics: New Methods and Evidence on Three Fronts*, Nat'l Bureau of Econ. Research, Working Paper No. 23057 (2017), http://www.nber.org/papers/w23057

proportion of the population is vulnerable to the NBLLN bias, as it appears to be the dominant way in which individuals think about information aggregation. Benjamin et al. developed a tractable mathematical model of NBLLN where they proved that individuals tend to underestimate how much a technology company can learn about their behavior by simply analyzing their online social patterns, leading consumers to undervalue their own privacy.[124]

A study conducted by Ignacio N. Cofone and Adriana Z. Robertson proved that consumers have a serious problem accurately estimating the incremental value of their private information online.[125] This same study debunked the idea that the privacy paradox is caused by consumers not paying enough attention online and suggested that any privacy-focused regulation needs to address the NBLLN bias.[126]

III. THE NEED FOR BETTER PRIVACY LEGISLATION

Privacy laws vary depending on the country and jurisdiction in which they are enacted, but in some sense, they're similar because they typically include provisions that establish the rights of individuals to control the collection, use, and disclosure of their personal information by organizations. These laws may also include requirements for organizations to protect the personal information they collect and to provide individuals with access to their own personal information. In some cases, privacy laws may also establish penalties for organizations that fail to comply with their provisions. The common denominator of these laws is that they do not account for the reality of the privacy paradox, and heavily rely on consumer choice.

A. CURRENT U.S PRIVACY LAW FRAMEWORK

Privacy law in the United States is a chaotic landscape due to the sectoral patchwork approach that the federal government adopted. For instance, the Health Insurance Portability and Accountability Act ("HIPAA") is a federal law that seeks to protect sensitive patient health information from being disclosed without the patient's consent or knowledge, therefore regulating the healthcare industry.[127] The Fair Credit Reporting Act ("FCRA") is a federal law that protects consumers from misinformation being used against them in the credit industry.[128] The Gramm-Leach-Bliley Act ("GLBA") is a federal law that requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.[129] The Electronic Communications Privacy Act ("ECPA") is a federal law protecting wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers.[130] The Family Educational Rights and Privacy Act ("FERPA") is a federal law that affords parents the right to have access to their children's education records.[131] The Children's Online Privacy Protection Act ("COPPA") is a federal law that imposes certain

[124] Daniel J. Benjamin et al*., A Model of Nonbelief in the Law or Large Numbers*, 14 J. Eur. Econ. Ass'n 515, 516 (2016).
[125] *Cofone & Robertson*, supra note 30, 1502.
[126] *Id*.
[127] Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320 et seq.
[128] The Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.
[129] Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801 et seq.
[130] Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 3121 et seq.
[131] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232 et seq.

requirements on operators of websites or online services directed to children under 13 years of age.[132] With the absence of a single, streamlined privacy law giving businesses one set of rules to follow, businesses are facing a barrier to innovation in the digital economy, and exorbitant compliance costs.[133]

All these federal statutes have given multiple federal agencies jurisdiction over data privacy regulation. The FTC is particularly active with regards to domestic privacy matters, and the Department of Commerce is active with respect to international data privacy matters.[134]

Additionally, the unauthorized transfer of PII might sometimes trigger liability rules embodied in the four privacy torts: intrusion on a person's seclusion or solitude; public disclosure of embarrassing private facts about a person; publicity that places a person in a false light in the public eye; and appropriation, for the defendant's advantage, of a person's name or likeness.[135] In *Guzman v. RLI Corp*., the plaintiffs were denied an injunction to prevent the defendant from disclosing sensitive immigration because the court found that there was "no emergency shown as to the general claim that there is an immediate, material risk that Defendants will disclose confidential information about the Plaintiff or putative class members in some manner."[136]

Eric Jorstad claims that the world of privacy regulation today resembles the 1960s when legislators were trying to regulate consumer product safety: back then, automation transformed production for customization to mass-production; today the same automation and universalization is affecting the privacy sphere.[137] The patchwork nature of privacy legislation in the United States and the world is presenting a challenge to companies wishing to comply with all these different frameworks. At the same time, consumers are not really protected as discussed earlier in this article.

In short, online transactions involving the disclosure of PII will fall, in the majority of cases, outside of the scope of the mosaic of laws.[138] This reality created a self-regulated industry, where BigTech monopolies enforce limitations such as voluntary privacy seals and privacy policies against the average reasonable consumer.

B. ALARMING STATISTICS AND FINDINGS

A study by Alan Westin established that consumers fall into three categories when it comes to the valuation of their privacy online and offline: fundamentalists (high privacy concern and high distrust in government, business, and technology); pragmatists (mid-level concern and distrust); and unconcerned (no or low concern and distrust).[139] When addressing the United States Congress, Westin stressed that fundamentalists are outliers and cannot be taken as the median, therefore

---

[132] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 et seq.

[133] Ashley Johnson & Daniel Castro, Why Congress Should Pass Data Privacy Legislation in 2022, The Hill (Jan. 24, 2022) https://thehill.com/opinion/cybersecurity/591022-why-congress-should-pass-data-privacy-legislation-in-2022/

[134] Federal Trade Commision Act, 15 U.S.C. 41-57, 57a-c, 58 (1994 & Supp. 1998).

[135] Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. Davis L. Rev. 379, 405 (2003).

[136] *Guzman v. RLI Corp*., No. LA CV20-08318 JAK (ASx), 2020 WL 6815026, at *2 (C.D. Cal. 2020).

[137] Jorstad, *supra* note 6, at 1511–12.

[138] Ilene R. Berson, *Grooming Cybervictims: The Psychological Effects of Online Exploitation for Youth*, 2 J. SCH. VIOLENCE 9, 9-10 (2003).

[139] Kim Bartel Sheehan, *Toward a Typology of Internet Users and Online Privacy Concerns*, 18 INFO. SOC'Y 21, 21 (2002).

policy should be directed toward privacy pragmatists.[140] Westin sees that pragmatists are willing to trade their privacy to receive other goods and services, and therefore need protection.

Chris Hoofnagle and Jennifer Urban conducted research to supplement Westin's theory. They found that people categorized as "unconcerned" or "pragmatists" believed falsely that privacy protections were in place.[141] However, when informed of the reality of legal privacy protections, these individuals made decisions more consistent with those of privacy fundamentalists.

Additionally, Westin's terminology debunks the myth that individuals are willing to give up all of their privacy in order to receive free goods and services, or discounts. According to this line of reasoning, companies processing PII assume that consumers do not care about their privacy and are happy giving it away in exchange for online services. However, the existence of the privacy paradox is nothing but an indication that online platforms make it quasi-impossible for consumers to manage their preferences due to absence of privacy expectations.

From the Consumer's perspective, and as of 2019, 79% of American voters believed that Congress needed to prioritize crafting a law that protects privacy on the federal level.[142] In the same year, 79% of American voters were concerned about the way companies use their data.[143] When it comes to the amount of data that companies process, 81% of American consumers believe that they cannot control that.[144] It was determined in the same survey that 69% of consumers are not confident in ways with which companies use their data.[145] Additionally, 75% consider that companies abusing their data will not be held accountable by the government.[146] A study by the Pew Research Center showed that only 24% of Americans believe that tech firms sufficiently protect PII.[147] 81% of respondents in a study conducted by Kesan et al. had at least once "submitted information online when they wished that they did not have to do so."[148]

With digital privacy law in the United States being molded around the idea of consumer's privacy as an economic good, protection depends on the notice and choice mechanisms and opt-out procedures.[149] However, even though the notice and choice model allows consumers to be informed on how their data is processed, it does not make it easier for a consumer to opt-out of the collection, storage, sale and transmission of data.[150] These long privacy notices filled with complex legal jargon impede consumers from making informed privacy choices that correspond to their

---

[140] What Consumers Have to Say About Information Privacy: Hearing Before the Subcomm. On. Com., Trade and Consumer Protection of the H. Comm. On Energy and Com., 107th Cong. 17–22 (2001) (testimony of Alan K. Westin, Professor Emeritus, Columbia University).

[141] Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 283–84, 302 (2014).

[142] Sam Sabin, *Mot Voters Say Congress Should Make Privacy Legislation a Priority Next Year*, MORNING CONSULT (Dec. 18, 2019), https://morningconsult.com/2019/12/18/most-voters-say-congress-should-make-privacy-legislation-a-priority-next-year/.

[143] *Id.*

[144] *Id*.

[145] *Id*.

[146] *Id*.

[147] *See* Aaron Smith, *Public Attitudes Toward Technology Companies*, PEWRESEARCH. (June 28, 2018), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2018/06/PI_2018.06.28_tech-companies_FINAL.pdf.

[148] Jay P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust and Consumer Autonomy*, 91 Ind. L.J. 267, 271 (2016).

[149] Barrett, *supra* note 94, at 3.

[150] *Id*.

wishes. And with the reality of decision fatigue, learned helplessness and the NBLLN, it is unrealistic to expect consumers to opt-out of the sale of their data (if the law protects this right) every time they use a SNS or website online. This means that a new way of protecting the right to digital privacy is needed.

IV. CONSUMER ORIENTED LEGISLATION: PRIVACY BY DESIGN

The CEO of Apple, Tim Cook, recognizes consumers' right to see where their information is being sold and the right to delete it if need be.[151] In other terms, not every tech company is against strict data protection laws that recognize the consumer's right to privacy and right to choose.

Current legislation relies too heavily on privacy self-management – for example, California's CCPA presents a series of rights where the consumer must take the conscious decision to make use of, such as the right to opt-out of the sale of data.[152] As it has been already discussed in this paper, whenever the law gives consumers control over their PII, and individuals fail to effectively exercise greater control, the behavior valuation argument cites this pattern as a proof that consumers don't care about their privacy.[153] Therefore, privacy regulation needs to be taken in a different direction: instead of focusing on individuals managing their own privacy, privacy regulation should be about regulating the architecture that structures the way PII is collected, stored, used and transferred.

A. THE FAULTY BEHAVIOR VALUATION ARGUMENT

As Eric Jorstad puts it, most people inhabit the space on the continuum between the paranoid retreatists and the utopian ecumenicists.[154] With that in mind, digital privacy legislation needs to provide safe and free communication. And because drafting effective legislation that protects digital privacy is as challenging as writing a jazz mass in Latin, bridging the class of cultural and linguistic differences is essential.[155]

Some privacy commentators rely on the findings of the privacy paradox to assert that less restrictive privacy laws are needed because consumers' behavior indicates that digital privacy is not valued highly.[156] With the behavior valuation argument, experts consider behavior or revealed preferences to be the most accurate measure of how consumers value their privacy (rather than their expressed attitudes or stated preferences).[157] Therefore, since consumers ascribe a fairly low value to their privacy,[158] then privacy laws should not be influenced by what people say, and should be less restrictive. But as discussed above, the existence of the privacy paradox is due to the hindered decision-making process that consumers have to undertake every single day. The

---

[151] Issie Lapowsky, *How Tim Cook's Data Broker Registry Might Actually Work*, WIRED(Jan. 23, 2019, 12:25 PM), https://www.wired.com/story/tim-cook-data-broker-registry/.
[152] Cal. Civ. Code §§1798.100-.1798.199 (West 2020).
[153] Solove, *supra* note 8, at 5-6.
[154] Jorstad, *supra* note 6, at 1518.
[155] *Id*. at 1520.
[156] Gordon Crovtiz, *Opinion, Privacy? We Got Over It*, Wall St. J. (Aug. 25, 2008), https://www.wsj.com/articles/SB121962391804567765.
[157] Wolfram Elsner et. al, T*he Microeconomics of Complex Economies: Evolutionary, Institutional, Neoclassical, and Complexity Perspectives* § 6.4.1, at 139-40 (2015).
[158] Solove, *supra* note 8, at 11-12.

digital world, for the most part, is not designed in a way to give consumers a choice other than selling their PII. Consumer choice is skewed by calculated technological design. Professor Woodraw Hartzog argues in his book, Privacy's Blueprint, that "there are overwhelming incentives to design technologies in a way to maximize the collection, use, and disclosure of personal information."[159] In other terms, SNSs makes it easier for consumers to share their PII without comprehending the consequences.

Privacy by design is the protection of data through technology design. For example, requiring an "opt-in" over an "opt-out" model in modern privacy legislation is a way to honor a consumer's choice to avoid being subject to unconsented-to data sharing.[160] By giving consumers the right to opt-out of the processing (whether processing means in a specific context collection, sale or other) of their PII, companies are essentially creating an illusion of control and a series of obstacles that consumers need to thoroughly research in order to protect their privacy.[161]

Zeynep Tufekci observes that "data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices."[162] We see that there is a need to embed privacy principles into the skeleton of every software that processes the consumer's PII online.

Turning privacy-by-design principles into law will require the coordination of many interests: business, marketing, legal, engineering, risk management, security, policy and design.[163] But transforming a list of legal standards, wireframes and flow diagrams into a software product ready for use is not easy. The process typically starts by brainstorming sessions, followed by rounds of feedback and iterations. Then, the idea will be concretized into a long list of ones and zeros designed specifically for privacy. The final product can then be implemented by companies processing PII in order to comply with the legislated standards of privacy. In conclusion, the combination of a law that imposes privacy by design, and a well written software that was designed for privacy will lead to protection of consumers' PII.

B. FAIR INFORMATION PRACTICES AND PRIVACY ENGINEERING

In order to design products and services with digital privacy in mind, looking at the set of internationally recognized values and standards about personal information known as the Fair Information Practices ("FIP") is essential.[164] In the United States, FIPs are guidelines for notice, choice, access, integrity and enforcement regulated by the FTC that define the rights of consumers

---

[159] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* 5 (2018).

[160] *See* Ana Isabel Segovia Domingo & Nathalie Desmet Villar, *Self-regulation in Data Protection* 2 (2018). The authors explain thoroughly how self-regulation is not working satisfactorily in the United States. This is especially true with the CCPA coming into force and proposing a system of "opt-out" where consumers have to manually opt-out of the processing of their data from every single data provider. This is not only time consuming, but does not take into consideration the reality of the privacy paradox and the behavioral statistics.

[161] Ari Ezra Waldman, *Privacy Law's False Promise*, 97 Wash. U. L. Rev. 773, 811 (2020).

[162] Zeynep Tufekci, *The Latest Data Privacy Debacle*, N.Y. Times (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html

[163] Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 Berkeley Tech. L.J. 1333, 1349.

[164] *Fair Information Practices*, Fed. Trade Comm'n, http://www.ftc.gov/reports/privacy3/fairinfo.shtm

and the obligations of companies processing PII.[165] Most privacy scholars agree that the FIPs are an understanding of privacy as control over PII.[166]

And although there are many different versions and formulations in various jurisdictions, the FIPs coalesce around the following nine principles:

1. Defined limits for controllers and processors of personal information on the collection, processing and use of personal data (in other terms, data minimization);
2. Data quality (accurate, complete and timely information);
3. Limits on data retention;
4. Notice to individual users;
5. Individual choice or consent regarding the collection and subsequent use of personal information;
6. Reasonable security for stored data;
7. Transparent processing systems that affected users can readily understand and act on;
8. Access to one's personal data; and
9. Enforcement of privacy rights and standards (including industry self-regulation, organizational measures implemented by individual firms, regulatory oversight and/or enforcement, and civil litigation).[167]

FIPs have many strengths due to their recognition by privacy experts all around the world as the foundation of modern international privacy law.[168] Due to this wide acceptance, FIPs could become the basis of any local or international law that seeks to describe the rights of consumers and the obligations of companies processing PII. Additionally, due to the open-ended nature of the FIPs, data controllers are able to take account of all relevant factors, which facilitates compliance. And most importantly, the flexible and neutral nature of the FIPs allow for social and technological change. Having principles that can stand the test of time in today's digital world is essential: effective legislation has to account for existing technological advancements and future discoveries as well.

Before the emergence of privacy laws, only 4% of Fortune 500 Companies complied with the measured aspects of the FIPs.[169] However, current privacy laws are built around the FIPs, without really taking these principles as a foundation. For instance, the United States relies on a scaled-down version of the FIPs, often referred to by privacy experts as "FIPs-lite."[170]

Ira Rubinstein and Nathan Good claim that the most reliable way to incorporate privacy by design into product development is to require the inclusion of privacy standards in software

---

[165] *See* Daniel J. Solove & Paul M. Schwartz, Information Privacy Law 699 (4th ed. 2010).
[166] Rubinstein & Good, *supra* note 163, at 1347.
[167] This formulation of the FIPs is the result of the work of Paul M. Schwartz & William M. Treanor. *See* Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 Mich. L. Rev. 2163, 2181 (2003).
[168] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy* (What Larry Doesn't Get) 2001 STAN. TECH. L. REV. 1, P 44 (2001).
[169] Kathy Stweart Schwaig et al., *Compliance to the Fair Information Practices: How are the Fortune 500 Handling Online Privacy Disclosures*? 43 INFO. & MGMT. 805, 808-09 tbl. 4 (2006).
[170] See *Privacy Today: A Review of Current Issues*, PRIVACY RIGHTS CLEARINGHOUSES, http://www.privacyrights.org/ar/privacy-issueslist.html.

specifications and requirements.[171] The product blueprint will have to reflect previously agreed upon standards of privacy that would be reproduced in the final version of the product. Simply, privacy by design requires translating FIPs into engineering principles. However, since not all FIPs are equally relevant, we will be focusing on data avoidance and minimization, data retention, transparency, accountability, and individual choice and access.

1. Protection of PII from Unauthorized Access

Although there is no consensus on exactly what a PII is, scholars and experts agree that the FIPs only apply to PII, and that in the absence of PII, there is no privacy harm.[172] Therefore, the purpose of privacy by design and privacy engineering is to protect PII from unauthorized access and limiting the linkability of collected data to personal identifiers.[173] For example, let's suppose that Company 1 collected Data X about John Doe, and company 2 collected Data Y about John Doe. In the event of a data exchange between Company 1 and Company 2, a well written software should guarantee that these companies would not be able to link Data X and Data Y to John Doe.

This can be done by using anonymity services that delink users from all traces of their online activity: for instance, proxies could be used to shield a consumer's IP address alongside other identifiers,[174] or user-centric identity management systems can be put in place to enable anonymous and pseudo-anonymous credentials while using a service.[175]

2. Data Avoidance and Minimization

Data avoidance and minimization are central principles to the FIPs.[176] In order to support the concept of data minimization, companies processing PII need to minimize the collection of PII at the source. Concretely, this means that engineers will need to consider methods that dissociate functionality requiring PII from activation, recommendation services and other where pseudonyms would suffice.[177]

Feigenbaum et al. argue that companies – specifically data controllers – would need to figure out which piece of data is necessary for different practices, and thereafter build software that can achieve the practice without collecting excessive PII.[178] For example, when it comes to the protection of consumer's geolocation, companies can avoid recording IP addresses, disabling User ID cookies, and or using third-party proxy servers to help strip out IP addresses.

Naturally, serious attention would need to be given to the architecture and management of databases held by companies processing PII: segmenting data into split databases based on common connectors seems like a logical solution.

---

[171] Rubinstein & Good, *supra* note 163, at 1353.
[172] Solove & Schwartz, *supra* note 165.
[173] Rubinstein & Good, *supra* note 163, at 1357.
[174] George Danezis & Seda Gurses, *A Critical Review of 10 Years of Privacy Technology, in Proceedings of Surveillance Cultures: A Global Surveillance Society*? (2010), https://www.researchgate.net/publication/228538295_A_critical_review_of_10_years_of_Privacy_Technology.
[175] *Id*.
[176] Rubinstein & Good, *supra* note 163, at 1357.
[177] *Id*.
[178] Joan Feigenbaum et al., Privacy Engineering in Digital Rights Management Systems, in Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management 79 (Tomas Sander ed., 2002).

3. User Identifiability

User identifiability is the degree to which data can be directly attributed to an individual.[179] Sarah Spiekermann and Lorrie Faith Cranor claim that "the degree of privacy friendliness of a system is inversely related to the degree of user data indefinability."[180] The authors then describe four privacy stages of a privacy-friendly system: at stage 0, privacy is limited and Identifiability is easy.[181] At stage 1, a minimal degree of privacy protection is afforded then at stage 2, non-identifiability is achieved through privacy-by-architecture.[182] Finally, at stage 3, user privacy is protected thoroughly.[183]

4. Data Retention Limits

Data retention limits means that data must be de-identified or erased as soon as it is no longer needed for business purposes. However, question over the appropriate length of retention periods remains unanswered in different parts of the world because the term "business purpose" can be interpreted differently.

According to Feigenbaum et al., addressing data retention is best done through database architecture and management and recommends the erasure of PII before its integration to long-lived data warehouses.[184] Therefore, instead of reducing the risk of reidentification, companies can avoid reidentification in the first place. Additionally, Spiekermann and Cranor propose the "purging of nonidentified data as well, to minimize the risk of reidentification based on the pattern of matching."[185]

5. Notice, Choice, and Access

Privacy policies are not privacy guarantees. In fact, these policies serve as compliance instruments where companies processing PII inform consumers of adopted privacy practices. To fight the paradox, privacy policies need to be understandable, widely disseminated, and timely.[186] Even though its length is imposing, Google's consolidated and comprehensive policy is a notable example.[187]

One of the oldest solutions proposed to create better privacy policies was the Platform for Privacy Preferences ("P3P"). The W3C standards allows companies to encode the practices found in their privacy policies in machine-readable XML format.[188] Consumers can store their privacy preferences, and therefore make automated privacy choices. However, the P3P model has been sharply criticized: when Microsoft implemented the framework in Internet Explorer,

---

[179] Sarah Spiekermann & Lorrie Faith Cranor, *Engineering Privacy*, 35 IEEE Transactions on Software Engineering 67, 74 (2009).
[180] *Id*. at 75.
[181] *Id*.
[182] *Id*.
[183] *Id*.
[184] Joan Feigenbaum et al., *Privacy Engineering for Digital Rights Management Systems*, in Revised Papers from ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management 76, 93 (Tomas Sander ed., 2002).
[185] Spiekermann & Faith Cranor, *supra* note 179, at 76.
[186] Feigenbaum et al., *supra* note 181.
[187] Google, *Privacy Policy,* https://policies.google.com/privacy?hl=en-US (last visited Jun. 1, 2023).
[188] Spiekermann & Faith Cranor, *supra* note 178, at 78.

consumers were only able to know if the website meets the cookie preference after clicking on a small "privacy report" icon on the browser's status bar.[189]

C. A USER-EXPERIENCE APPROACH

To reflect a consumer's real-life experience online, focusing on technical arrangements is not enough, because good software will have to engender social expectations. A complementary approach to translating FIPs into engineering principles would be to embed privacy into the user experience ("UX") design process.[190] This UX approach would seek to develop software that is focused on end-user goals, usability, and aesthetics. This is extremely important because consumers consider privacy controls secondary while completing their primary task: when browsing the internet, for example, privacy controls must be accessible to a broad range of consumers with different skill levels.[191]

Lederer et al. suggest that the improvement of privacy conditions in software happens through a combination of back-end (server, application and database) and front-end (graphic design and user interface) development.[192]

Other notable design standards are the guidelines developed by Lipford et al. that make information more visible in SNS due to their contextual integrity.[193]

Consumers suffering from NBLLN bias do not know how to process and aggregate the information available.[194] In order to achieve an NBLLN-robust privacy legislation, personal data collected from consumers needs to be described in a way that is clear and simple.[195] To address the accumulation problem that the Cofone and Robertson study described, disclosures that are written in unfamiliar terms to the rational individual need to be eliminated.[196]

Additionally, disclosures need to address the significance of the data that is being collected. A consumer's behavior may change if they read "we will collect your geo-location information that will reveal to us where you are accessing the internet from, and it will be combined with geo-locations from other devices that will reveal the coordinates of your home, your work and your hometown" rather than "we will collect your geo-location information."[197] This way, the information asymmetry between the consumer and the company will be reduced significantly, allowing consumers to grasp the concept of information aggregation and the interplay that happens between different classes of information.[198]

---

[189] Tom Spring, *First Look at Microsoft IE 6.0*, PCWorld (Aug. 28, 2001), http://www.pcworld.com/article/59928/article.html.
[190] Rubinstein & Good, *supra* note 163, at 1365-66.
[191] Claire-Marie Karat et al., *Usability Design and Evaluation for Privacy and Security Solutions*, Security and Usability 47, 48-50 (2004).
[192] Scott Lederer et al., *Personal Privacy Through Understanding and Action: Five Pitfalls for Designers*, 8 Pers. & Ubiquitous Computing 440, 445-49 (2004).
[193] Heather Richter Lipford et al., V*isible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Site*s, in Proc. 12th IEEE Int'l Conf. on Computational Sci. & Engineering 985 (2009), http://ieeexplore.ieee.org/.
[194] Cofone & Robertson, *supra* note 30, at 1502.
[195] *Id*. at 1503.
[196] *Id*. at 1502.
[197] *Id*. at 1502.
[198] *Id*. at 1502.

D. EMPOWERING CONSUMERS BEYOND PRIVACY BY DESIGN: PRIVATE RIGHT OF ACTION

By giving consumers the private right of action, businesses will implement reasonable privacy practices to avoid potential liability.[199] While consumers currently have little to no control over the use and dissemination of their data, they maintain weak bargaining power with companies processing their data and bear the risks of poor privacy practices.[200]

Economically speaking, the risk of potential litigation is enough to deter certain behaviors when the costs overweigh the benefits.[201] Currently, companies processing PII are reaping great benefits (including profits) from the collection, sale and transfer of PII. In comparison, they are facing few losses from poor privacy practices.[202] Legislation giving consumers a private right of action would disrupt this cost-benefit analysis, resulting in the adoption of greater protection models by companies wishing to mitigate their risks.[203]

The reality is, privacy practices have morphed into a managerial process of ticking boxes off on compliance checklists, conducting internal audits and keeping up with a mosaic of local and international laws.[204] In the United States, for instance, enforcement mechanisms are weak: the FTC's enforcement is limited by its statute and due to lack of precedent, enforcement is limited.[205] Since companies have no business recognizing a de-facto right to privacy as per human rights standards, a private right of action would incentivize companies to develop and invest in improved data privacy and security to avoid liability in court.

CONCLUSION

The current framework of privacy laws is incapable of protecting consumer's privacy because it ignores the very consumer it is meant to protect. Companies processing PII make it extremely difficult for consumers to manage their digital privacy as per their expectations: for example, privacy policies are often filled with legalese and complicated jargon and click-through agreements are on almost every company's website. In addition to the technical difficulties that the average consumer faces online, internet users may suffer from NBLLN and privacy resignation, thereafter, hindering their choices with regards to the management of their privacy. Instead of taking into account these realities, current digital privacy laws ignore the paradox, and give consumers the responsibility of managing privacy with every company.

---

[199] Wayne Unger, *Reclaiming Our Right To Privacy by Holding Tech. Companies Accountable*, 27 RICH. J.L. & TECH. 3, 11 (2020).
[200] *See* Lee Rainie & Janna Anderson, *The Fate of Online Trust in The Next Decade*, PEW RSCH. CTR. (Aug. 10, 2017) https://www.pewresearch.org/internet/2017/08/10/the-fate-of-online-trust-in-the-next-decade/.
[201] *See generally* Thomas C. Galligan, Jr., *Deterrence: The Legitimate Function of the Public Tort*, 58 Wash. & Lee L. Rev. 1019, 1032 (2001).
[202] *See* Press Release, FT Commissioner Rebecca Kelly Slaughter, Dissenting Statement of Commissioner Rebecca Kelly Slaughter, In the Matter of FTC vs. Facebook (July 24, 2019).
[203] *See, e.g.*, Nick Statt, *Facebook Sets Aside $3 Billion Ahead of Record FTC Fine Over Privacy Violations*, The Vere (Apr. 24, 2019, 4:24 PM), https://www.theverge.com/2019/4/24/18514805/facebook-q1-2019-earnings-ftc-record-fine-privacy-violations-3-billion.
[204] *See* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 Wash. Univ. L. Reb. 773, 776-77 (2020).
[205] Unger, *supra* note 198, at 14-16.

As discussed in this article, having the right to opt-out of the collection and sale of data doesn't mean that consumers are going to use the right with every company that processes PII due to time constraints, and their ignorance of the technical aspect. Therefore, consumer-oriented legislation should be mandating privacy by design principles. By enforcing fair information practice principles through privacy engineering, the right to privacy would be protected across the board, regardless of a consumer's valuation of privacy in a given situation.