Privacy RFC 2018
Julianne Bagley

According to a January 2017 Pew Research Center Report, about "half of Americans do not trust the federal government or social media sites to protect their data."[1] Additionally, this research examined several types of cybersecurity issues affecting Americans and found that 64% have experienced at least one of them.[2] This illustrates the need for a single, comprehensive privacy policy to provide uniformity and a structured approach to embedding privacy within organizations. In response to the Department of Commerce's Request for Comments (RFC) on the Administration's approach to consumer privacy, I will address specific principles which should be emphasized in the proposal as well as further interpreting the proposed privacy principles.

Need for Education

To establish the importance of data privacy and the risks associated with violating privacy, it must begin with education. Education consumers on privacy risks and educating organizations so they grasp the need for privacy and think beyond their own business and economic needs while implementing their products or services. This need for education addresses goal 6 of the proposal: incentivize privacy research.[3]

This education should begin as early as ethics courses in engineering programs and ethics courses or seminars within organizations who utilize consumer data. It needs to be a part of the corporate structure and the companies need to hire engineers, product development teams, and privacy professionals who have this in mind and collaborate together to make a product or offer a service that consumers can trust. Education should also be implemented within the company culture.

This focus on education was highlighted in the 2014 Report to President Obama on Big Data and Privacy submitted by the President's Council of Advisors on Science and Technology[4]. In section 5.2 of the report, five recommendations are presented, two of which focus on education and research on data privacy.

Recommendation 3 focuses on coordinating with the other agencies (they specifically note the OSTP and NITRD) to strengthen research in privacy related technologies and the areas of social science that shed light on how to best apply these technologies while Recommendation 4 focuses on partnering with educational institutions and professional societies to provide education, training programs, and new career paths pertaining to privacy protection.[5] The latter

[1] Aaron Smith, *Americans and Cybersecurity*, Pew Research Center, (last visited Nov. 8, 2018), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.
[2] Aaron Smith, *Americans and Cybersecurity*, Pew Research Center, (last visited Nov. 8, 2018), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.
[3] *Request for Comments on Developing the Administration's Approach to Consumer Privacy*, NTIA, (Sept. 2018), https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf
[4] *Report to President Big Data And Privacy: A Technological Perspective*, The White House President Barack Obama, (May 2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf
[5] *Report to President Big Data And Privacy: A Technological Perspective*, The White House President Barack Obama, (May 2014),

recommendation supports my point above that education and training should be made at the educational institution level and the need for privacy centered careers is more pertinent than ever.

Consent and Privacy by Design

The RFC aims to "refocus on outcomes of organizational practices, rather than on dictating what those practices should be."[6] It seems idealistic and ambiguous to solely base privacy principles on desired outcomes rather than providing guidance and specific criteria to achieve those outcomes. It would be difficult for organizations and enforcement to distinguish the threshold of compliance and noncompliance. Organizations will still run the risk of being retroactive, with companies experimenting and gaging what works and what doesn't, just to fix it after the fact. Furthermore, with an outcome-based approach, many organizations will remain complacent in doing the minimum to protect consumers. Without specificity, it leaves the organizations open to interpreting what is enough and will cause subjectivity.

A first step would be to develop a clear definition of what constitutes "private sector organizations that collect, store, use, or share personal data."[7] A new approach should require organizations to be transparent about who is collecting data, what data they are collecting, how they are collecting it, and why. It should also explicitly state the rights of data subjects v. the rights of the controller and processor.[8] The GDPR and the California Consumer Protection Act (CCPA), although different in many respects, have established specific practices to achieve a higher standard of consumer privacy, some of which should be incorporated into U.S. policies. Although the GDPR is viewed as stringent, Europe is ahead of the U.S. in terms of consumer privacy legislation. If the U.S. wants to be a leader in data privacy as the RFC emphasizes, we will have to take into account parts of their proposal because the GDPR is far reaching and has long armed outside its borders.

The Fair Information Practice Principles (FIPPs) have provided a general basis for privacy principles within the U.S., which should be incorporated and developed further. As referenced in the RFC, the principles should shift away from a Notice and Choice system which derived from the FIPPs and has become known as a "privacy policy" based standard. This standard is no longer sufficient enough for consent, especially for transparency and control-based outcomes. While privacy policies are unlikely to be erased as the standard. Organizations need to do more and there needs to be a comprehensive definition for what constitutes consent.

---

https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdfpot

[6] *Request for Comments on Developing the Administration's Approach to Consumer Privacy*, NTIA, (Sept. 2018), https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf

[7] *Request for Comments on Developing the Administration's Approach to Consumer Privacy*, NTIA, (Sept. 2018), https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf

[8] General Data Protection Regulation (GDPR), Art. 3 - 4

"The conceptual problem with notice is that it fundamentally places the burden of privacy protection on the individual, resulting in an unequal bargain, a kind of market failure."[9] Furthermore, "privacy policies today do not convey information in a way that reflects the embodied experience of internet users because they are designed without the needs of real people in mind."[10]

Current privacy policies are confusing and inconspicuous while providing little protection for consumers. If the notice is unclear, transparency cannot be achieved. Similarly, if a user does not know what they are agreeing to, consent cannot be achieved. Moreover, many users do not even read privacy policies, resulting again in a lack of consent. This is largely due to the design of privacy policies. They are often long, written in "legalese", typically in small font, and inconspicuous. Instead, organizations need to incorporate art, marketing, and design strategies to manipulate the audience's eyes and movements to evoke emotional or behavioral responses.[11] Websites are designed to manipulate users into following a certain pattern, hovering over and clicking on certain links; so why are companies incorporating their privacy policies in a way that is deceptive and deters consumer attention?

Many organizations currently use an "opt-out" model for consent. The default rule is that companies can decide to disclose your personal data as long as the customer does not indicate otherwise. However, this does not take into account that an individual can consent during the first instance but not necessarily consent to future data sharing. This especially becomes an issue when a privacy policy changes and an individuals' initial consent remains valid. The CCPA operates on a right to "opt out", while the GDPR is based off affirmatively "opting in." "Consent cannot be implied and must always be given through an opt-in, a declaration or an active motion, so that there is no misunderstanding that the data subject has consented to the particular processing."[12] This gives the consumer control over their data and their choice to participate in information collection, sharing, and overall use. Another benefit deriving from the GDPR and the CCPA is the right for individuals to not be discriminated against for choosing not to opt in. Organizations are still required to offer the baseline service regardless of whether an individual refuse to consent to data collection and sharing.[13] Organizations should use a mixture of both opt-in and opt-out to ensure that consent is given.

Other provisions from the CCPA and GDPR that should be considered in the U.S. to further consumer privacy protection are the right to be forgotten[14] (a right for the consumer to request information deletion) and a right to access their collected data and make corrections[15]. Again, this facilitates the control-based outcome allowing consumers to choose at any point to have their

[9] Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today and How to Change the Game*, Brookings.edu, (last visited Nov. 7, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-and-how-to-change-the-game/
[10] Ari Ezra Waldman, Privacy, Notice, and Design, 21 Stan. Tech. L. Rev. 74, 77 (2018)
[11] Ari Ezra Waldman, Privacy, Notice, and Design, 21 Stan. Tech. L. Rev. 74, 78 (2018)
[12] General Data Protection Regulation (GDPR), Key Issues: Consent, (lasted visited Nov. 7, 2018), https://gdpr-info.eu/issues/consent/
[13] California Consumer Protection Act (CCPA) §1798.103
[14] California Consumer Protection Act (CCPA) §1798.105(a); General Data Protection Regulation (GDPR) Art. 17
[15] California Consumer Protection Act (CCPA) §1798.100; General Data Protection Regulation (GDPR) Art. 15

data erased and no longer accessible as well as receiving full reports of what data any given organization has on them.

Shifting away from Notice and Choice, Article 25 of the GDPR turned to Privacy by Design (PbD), a principle developed by Ann Cavoukian.[16] There is this idea of regulation on consumer privacy as a negative concept which stymies innovation but we need to transform this rhetoric into thinking of privacy protection as Tabriz pointed out: a business strategy. Any business operating in good faith should have consumer protection in mind and want to create the best product or service that incorporates a safe, enjoyable, and successful result.

Privacy must be considered at the earliest stages of the design process alongside aesthetics, functionality, budget, and efficiency. Companies should be required to adhere to data minimization, use of data only for the length of time necessary, and protection against or consent before sharing with third parties. These organizations are in better positions both financially and knowledgeably, to address privacy concerns.[17] The overall outcome-based approach by companies should not be thought of as company interest versus consumer interest because the better outcome encapsulates both. Based on a January 2018 report by Cisco, there is evidence that prioritizing the consumer and their privacy needs is likely to benefit a company's own interests as well. Cisco reported "65% of organizations have had delays in their sales cycles and the delays were heavily correlated to the privacy maturity level of the company. The privacy mature companies experience less delays and less costs and losses during data breaches.[18]

There should be a focus on the first three principles of PbD, where companies are proactive instead of reactive, privacy is the default in any business model, and privacy is embedded into design.[19] Rather than launching a business or product with the idea of making corrections after the issues occur, companies need to take into account all possible outcomes, especially any privacy related issues that could occur from the start. Once the data is breached it cannot be undone and changing a password or implementing new privacy protections after the fact do not eliminate or adequately remedy the harm that has occurred.

Information Fiduciaries and Private Action

[16] Josh Manion, *Marketers' Balancing Act Between Value And Privacy*, Martech Today (Last visited Nov. 8, 2018) https://martechtoday.com/balancing-act-value-privacy-120517
[17] General Data Protection Regulation (GDPR) Art. 25
[18] *Privacy Maturity Benchmark Study*, Cisco, (2018), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/privacy-maturity-benchmark-study.pdf?_ga=2.208332442.902572385.1517245138-1302553340.1517245138
[19] Ann Cavoukian, *Privacy by Design*, Information and Privacy Commissioner of Ontario, (Jan. 2011) https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Parisa Tabriz humanized the issue with consumer privacy and [emphasized] that "privacy is so personal and so specific to culture and your specific situation."[20]

In protecting consumers from data breaches and harm as a result, the U.S. needs a less rigid way of defining privacy. It should not limit it to privacy as secrecy but, recognize that information that is shared with others in secrecy or as part of a fiduciary relationship is still private. A narrow view on privacy stymies individuals from bringing successful privacy claims. In Dupont, the court concedes that they recognize that there are exceptions to the general rule where a duty to exercise reasonable care will arise. "We have held that such a duty may arise because: (1) a special relationship exists; (2) special circumstances exist; or (3) the duty has been voluntarily assumed."[21] Because of this, a fiduciary relationship between organizations and consumers should be recognized to allow for private action when organizations breach their duty.

If "trust is at the core of the United States' privacy policy formation"[22], as is stated within the RFC, then the relationship of information fiduciaries should be recognized under the common law and tort principles. The fiduciary relationship between a company and a consumer is one of trust and confidentiality. Information that is shared in a situation of trust can and should still be considered private and "under the law of information fiduciaries, online data collectors would not be allowed to share the data they collect with third parties that do not comply with the same data privacy obligations"[23] For example, in Dwyer v. American Express, the plaintiffs failed in their tort claim of intrusion upon seclusion because in doing business with Amex, they had already shared their information with the company, therefore making it no longer private.[24] If this were considered a fiduciary relationship the privacy factor would remain because the information was shared in a confidential relationship.

"Tort and fiduciary law assume that professionals and their clients do not stand on an equal footing. Professionals have special skill and knowledge that clients often lack. Clients are usually dependent on professionals to perform important tasks for them."[25] Because consumers are clients who trust these companies with valuable, sensitive, and personally identifiable information, and organizations know more about their data subjects than the consumers know about them, there is an unfair bargaining power. Consumers are confiding in these companies to use their data to provide them with the best possible service which the consumer otherwise cannot provide for themselves. In this respect, there is an imbalance and the companies should be held to the higher standard of professional fiduciary relationships similar to doctors and lawyers.

Consumers should be able to bring private actions against companies. The CCPA allows consumers to sue businesses for security breaches of their data, "even if consumers cannot prove

[20] Josh Manion, *Marketers' Balancing Act Between Value And Privacy*, Martech Today (Last visited Nov. 8, 2018), https://martechtoday.com/balancing-act-value-privacy-120517
[21] Dupont v. Aavid Thermal Techs., Inc., 147 N.H. 706, 709, 798 A.2d 587, 590 (2002)
[22] *Request for Comments on Developing the Administration's Approach to Consumer Privacy*, NTIA, (Sept. 2018), https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf
[23] Ari Ezra Waldman, *A Trust-Based Approach to Privacy and Information Law, in* Privacy as Trust: Information Privacy for an Information Age 77-147 (2018).
[24] Dwyer v. Am. Exp. Co., 273 Ill. App. 3d 742, 746, 652 N.E.2d 1351, 1354 (1995)
[25] Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. Davis L. Rev. 1183, 1216 (2016)

injury."[26] This should be permitted in addition to FTC's enforcement of unfair and deceptive practices. Additionally, there needs to be a comprehensive definition for "personally identifiable information" to adhere to under privacy claims while assessing the reasonableness of intrusion, which is another tort claim hurdle. In comparing the GDPR and U.S. state data privacy laws, the definition varies throughout. For example, Michigan's definition is broader and addresses the basic forms of personally identifiable information, such as social security number, driver's license number, and financial account numbers.[27] The GDPR's definition is also very broad, listing categories such as location data, physiological, and genetic.[28] CCPA takes it a step narrower in listing specific types for some of the broader categories.[29]A broader definition may be beneficial for enforcement because it allows for a case-by-case and contextual analysis.

Additional challenges in tort privacy claims are causation and injury. In many instances it is difficult to find the precise proximate cause and the injury may be intangible. However, in FTC v. Wyndham, the court adopted from tort principles and determined that "a company may be held accountable for negligent behavior that results in injury to a company and a consumer, even if the harm is precipitated by the criminality of a third party and "that a company's conduct was not the most proximate cause of an injury generally does not immunize liability from foreseeable harms."[30] This determination is crucial in analyzing data breach cases where third parties intercepted or leaked information. It recognizes that companies should still be liable for their own breach of duty and failure to impose adequate security measures. The court further analyzed §5 of the FTC Act and established that the standard as a cost benefit analysis "that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[31]

Lastly, the U.S. needs to rethink the penalties on organizations who violate privacy principles. It should be considered upon the context, evaluating factors such as the type of information shared, the type of company, and size of the company. However, the slight penalties that have been issued thus far are not enough. In FTC v. Wyndham, the settlement stipulated Wyndham to essentially create an information security program, perform annual audits, and submit a compliance report annually. These stipulations are retroactive and should already be in place before a data breach occurs. Similarly, there should be explicit requirements in regard to notifying the FTC and consumers when a data breach occurs. These companies are holding important information and breaching the confidence of their consumers by leaving it vulnerable for dissemination and need to be incentivized into taking privacy seriously from day one.

[26] Initiative 17-0039 (Amdt. #1), State of California Department of Justice, (Dec. 18, 2017), https://oag.ca.gov/system/files/initiatives/pdfs/Title%20and%20Summary%20%2817-0039%29_0.pdf
[27] Identity Theft Protection Act, §445.63(q), Michigan Compiled Laws (2004)
[28] General Data Protection Regulation (GDPR) Art. 4(1)
[29] California Consumer Protection Act (CCPA) §1798.106(3)
[30] F.T.C. v. Wyndham Worldwide Corp. (Wyndham II), 799 F.3d 236, 246 (3d Cir. 2015).
[31] Wyndham II, 799 F.3d at 255-56.