From: Rose Lee
To: privacyrfc2018
Subject: Comments on Developing the Administration's Approach to Consumer Privacy
Date: Friday, November 9, 2018 2:46:29 PM

The question of data privacy has become increasingly important and complex. We have the authority to choose what we share online, whom we share it with, and how it is shared, but every time we do so, we turn over important, valuable, and potentially quite personal information to seemingly omnipotent tech companies. Though most people understand this phenomenon vis-à-vis social media, many people do not understand that a massive and rapidly expanding body of data is being generated about each individual through the nearly ubiquitous Internet of Things ("IoT"). Within this new paradigm, our legal system has failed to keep up and respond adequately. Tech companies now give us more perceived control over personal information, which on its surface may look like a fair exchange, until we realize the harsh truth: all the focus on excessive control distracts us from what really affects our privacy in the modern age.

As Congress grapples with this issue, it should not make the mistake of demanding a muddled array of superficially important choices; rather, it should follow the example of the California Customer Protection Act (CCPA), but do so in a manner designed to achieve the overarching principle of preventing substantial injury to users who share information based on trust. Importantly, the law must address notice, consent, access, data minimization, portability, and deletion, while also requiring the Federal Trade Commission (the "FTC") to interpret, implement, and enforce these measures guided by the principle that consumer privacy is a right not to be harmed by the collection and use of information that users entrusted to the company.

In working through this topic, this paper advances five core arguments. First, as we assess these questions, it is important to begin by acknowledging that our embodied experience with information privacy is bound up with our concept of trust, which in turn invokes an obligation on the part of companies to prevent harm and act according to the interests of the users. Second, our current conceptualization of harm is too limited, focusing as it does on tort. This approach fails to encapsulate and acknowledge remote, diffuse risks that arise from privacy harm as real and actual harm. Within the context of privacy, harm should be defined as a result that arises from the invasion of privacy. Third, giving users excessive control and notice-and-choice is not an effective framework to address such harms. Fourth, users who make themselves vulnerable by trusting companies with their information should have more effective means of mitigating harm through privacy by design. Fifth and finally, as lawmakers and regulators work toward a solution with these guideposts in mind, they must also acknowledge some foreseeable shortcomings in executing such principles, while also recognizing that prudent solution to them do likely exist.

The concept of 'privacy-as-trust' asserts that data collectors are obligated to act in a trustworthy manner because they are information fiduciaries with respect to user data. Uber, Facebook, and Google are all information fiduciaries for the same reasons that doctors and lawyers are considered fiduciaries. By voluntarily placing sensitive information such as bank account data, personal preferences, and health in their hands, we become absolutely dependent on their services. In return, companies learn a great deal about us as they monitor and trace every step we take online and employ specialized analysts to predict, for example, our future spending habits based on our search histories. The appetite for data is voracious, and tech companies have become increasingly adept at procuring and monetizing our personal information by marketing themselves as experts in what they do and holding themselves out as trustworthy. The tradeoff -which is rarely made explicit- is that consumers gain access to highly useful information from the Internet, and in return tech companies acquire our information. In such an exchange, we unconsciously make ourselves vulnerable vis-à-vis our fiduciaries. Such absolute dependence on these technologies invokes a special obligation for companies to act in a manner aligned with basic precepts of loyalty and trustworthiness with regards to our information. The great fear, as Balkin writes, is that information fiduciaries might use our data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norms.

One particularly vexing challenge -which, importantly, has very real legal consequences- is how do

we measure such privacy harm information fiduciaries impose on us? At present, privacy law is founded in basic tort law, and thus looks for concrete harm. Unfortunately, privacy torts' limited conceptualization of harm makes this approach unsuited for most modern privacy problems. Though what constitutes a "concrete" injury remains an open question, courts have consistently held that only "concrete" privacy injuries are legally cognizable, and that mere speculation about possible future injury is insufficient to maintain a claim. Within the present paradigm of social media and massive data collection and monetization, this framing has become quite antiquated. Many modern privacy problems are not concentrated, outrageous, or concrete enough in a singular instance to be considered the kind of "harm" required to invoke a particular legal remedy. Under our current outdated thinking, people whose information has been misused usually must demonstrate some kind of discrete financial or even physical harm to recover, but doing so is exceedingly difficult. Indeed, the reason most data breach lawsuits are dismissed is a failure to demonstrate a particularized individual "harm." For example, the betrayal of trust and emotional distress a victim feels in the wake of being subjected to revenge porn is purely subjective and makes it difficult to articulate a clear, cognizable, and individualized injury that meets the higher standard of harm courts require. Yet, the law is reluctant to recognize adverse effects from data breaches simply because they do not immediately result in identity theft or financial harm.

However, let us not forget these privacy harms are also as real as any tort or criminal injuries. Some adverse effects from loss of privacy stem from the inability to negotiate boundaries, trust others, and assess risk. This differs from traditionally recognized harms such as financial costs or the infliction of extreme emotional distress. When our privacy is invaded, we are forced to watch our own backs, cover our tracks, and self-censor. Collectively and over time, these burdens can weigh significantly upon individuals. This is doubly true when the law continuously fails to recognize privacy harms as real harms. It is only a matter of time until it saddles the victims with the full burden of protecting themselves, recovering from breaches, and preventing future harms from past breaches. In return, those who cause such harm will have little incentive to change their behavior or invest in protections for users simply because the law does not consider it a "real" harm.

To prevent data collectors from inducing trust among us and then using it against our interest, we must craft national privacy laws that clarify and define privacy harm arising from breach of trust. The concept on harm should be broad enough to include deception, financial injury, health and safety injuries, unwanted intrusion, and reputational damage. Companies should be penalized for misleading consumers with materially false claims or omissions about a product or service. Users could be financially harmed when fraudsters use personal data to steal money or commit identity theft. Injuries to health and safety may arise, for example, when the unauthorized disclosure of personal information exposes people to harassment and unwanted surveillance from stalkers and abusive spouses. Revenge porn provides a stark example of wrongdoers being punished or penalized lightly relative to their misdeeds just because the court was not satisfied with the proof of harm. But, whereas tangible properties can be returned or financial losses can be remedied with legal restitution, victims of revenge porn are scarred for life because it is impossible to recollect nude pictures that have already been widely spread on the Internet. With privacy harm, there is no going back; victims can only either suffer or tolerate it. Unwarranted intrusion into people's private lives through the installation of spyware on computers that enable the recording of users engaged in private activities will not only leave the user traumatized, but disrespects one of the most fundamental human rights protected under the Fourth Amendment. Such abusive conduct can also cause reputational damage and lead to job loss. The law should acknowledge the heavy reality that once privacy is lost, it cannot be restored.

Any law or regulation that places excessive burdens on users is misguided. When the EU crafted its General Data Protection Regulation (GDPR), it placed too much emphasis upon notice-and-choice. This approach hinges upon the expectation that giving users every conceivable option and every possible relevant piece of information will lead to better use of consumer data. This improperly shifts the burden onto people who are less equipped than the information fiduciaries to handle it. Control over personal information might sound attractive in isolation, but we should also remind ourselves that such power comes with a substantial obligation. If users do not exercise that control themselves, users are at risk. Companies can take users' inaction as acquiescence. Privacy scholar Woodrow Hartzog emphasizes two main problems with elevating control. First, control does not scale. Hartzog notes that

the sheer number of choices that inundate users creates a control regime that is so overwhelming to the point of futility. Unsurprisingly, most users never read 50-page privacy policies and are more apt to disregard them when presented on small screens. Second, the other FIPs become subservient. The fixation on control sidelines other important principles, such as limiting data collection in the first place. Therefore, any sound approach to privacy in furtherance of autonomy must ensure the right amount of control and structured choice for people that is easy to comprehend and follow. Merely ticking "I Agree" is a traditional and archaic mechanism that does not add any meaningful protection.

Instead of pinning virtually everything on the notion of control, user interests should be the center of the design agenda. This is because design significantly affects how something is perceived, functions, and is used. Designers should utilize *signals* to embed trust in users and effectuate *transaction costs* to make certain tasks more difficult or easy to proceed. Companies that emphasize and excel at personal data collection typically manipulate users into revealing their personal preferences by designing the platform in a way that sends subtle *signals* to users that the platform is intimate, confidential, and safe. Facebook Newsfeeds, for example, prioritizes our closest friends or those with whom we have had more online interactions. This is because Facebook understands that people are more willing to share their personal information only with those they deem trustworthy. Transaction costs, on the other hand, focus more on the intensity of labor in performing a certain task. In another words, companies require people to invest more resources and effort to perform a certain behavior that companies want to discourage. Again, Facebook has a 'reply' feature for its private messages, but no forwarding feature. While you could still cut and paste your private conversation with a friend into a separate message box for other users, that takes more time and effort than simply pressing 'forward' and typing in a name. While the cost might be slight, it adds up over time and works as a nudge against sharing content privately. This similar methodology can be adapted to protect information users subjectively feel the need to conceal. Design affects our perceptions of relationships and risks while also influencing our behavior; thus, design provides a powerful tool for facilitating the proper use of consumer data.

In approaching design, it is vital to remain cognizant of obscurity. Obscurity as a privacy value is the notion that when our activities or information is *unlikely* to be found, seen, or remembered it is, to some degree, safe. This is because when our activities and information are designed to be hard to come by, the only people who will seize upon it will be those with sufficient motivation to expend the necessary effort and resources. Even if obscure information is found, if it is contextually vague and hard to understand, then the only people who will grasp it are those with sufficient motivation to push past the layer of opacity protecting it, such as a journalist investigating a story. If it is too hard to understand information, people can come to faulty conclusions or grow frustrated and give up on their investigation. Such effort serves as a deterrent, just as if the information were not readily available.

Evan Selinger, Fred Stutzman, and Woodrow Hartzog proposed key factors that could be used as functions of transaction costs such as search visibility, unprotected access, identification, and clarity. The presence of these factors diminishes obscurity, whereas their absence would enhance it. For example, access protection covers technologies and methods for controlling access to specific content, such as passwords. Although access controls do not allow users to technologically restrict who can view the information, they are significant and effective in a way it serves as a normative signal indicating the private nature of the information. Different kinds of access controls such as biometrics, encryption, privacy settings, and passwords can provide users control over several variables, including the content shared or the specifics of the potential audience. According to Hartzog, access controls are one of the most important factors in creating online obscurity. The best design would prioritize control where it is most important and useful without becoming a burden.

However, even if users obscured their identity by using pseudonyms and ID variants, social media presents challenges to such identity management. Social media can instantly pull up the user's networked connections, search history, interests, and education which, when aggregated, can reveal with near certainty the user's identity. One potential countermeasure would be to replace identifying information such as names, dates of birth, and addresses with data that looks the same but does not reveal significant details about the real person. Rabobank, a Dutch firm, spent the past year pseudonymizing payment data so that names, account numbers, and dates of birth retained their form but lost the identifying information they contained. The result was a new dataset that contains no

personal information, but retains the format, and statistics of the original.

Though our present legal structure for online privacy certainly falls short, lawmakers must also recognize that any regulation that prevented harms completely would present an undue burden and immense structural challenge. Like all other laws, we need to acknowledge the inherent limitations of regulatory prescriptions. Design protections can at most mitigate harmful behavior and attempts to go beyond that would likely be perceived as too tangential to address privacy harms. However, as sharing information within trusted friend group with no risk is not the same as broadcasting to the wide public on purpose, laws that focused too much on the differentiation of what information is considered intimate and what is not would be misguided and impractical. Modest incremental privacy protections might be one effective way of protecting information that users consider private while balancing competing values like free speech, innovation, transparency, and security. Privacy cannot coexist with other conflicting values if we attempt to provide absolute protection at all times.