UNIVERSITY OF WASHINGTON TECH POLICY LAB
In partnership with MICROSOFT

PUBLIC PANEL
"REDRESSING PRIVACY VIOLATIONS: A CONVERSATION WITH EXPERTS"

REPORT

MARIA P. ANGEL | ALEX BOLTON
Authors

RYAN CALO | LAURA GARDNER
Editors

December 2020

Table of Contents

Introduction

On December 10th, 2020, the University of Washington Tech Policy Lab and Microsoft hosted a public panel exploring the broad range of potential options available for providing redress when an individual's privacy is violated. During a 60-minute conversation, Professor Ryan Calo moderated a frank and illuminating discussion between three current and former Commissioners of the Federal Trade Commission and a noted scholar of privacy remedies. The panel featured Microsoft executive and former Commissioner of the Federal Trade Commission Julie Brill; Covington & Burling LLP partner and former Commissioner Terrell McSweeny; current FTC Commissioner Noah Phillips; and Florida State University College of Law Professor Lauren Scholz.

Discussion

Professor Calo formally opened the discussion with the question that gave rise to the panel: "Why is this question of privacy redress such an important piece of the puzzle when it comes to having a federal privacy law?" For Brill, it came down to privacy as a fundamental right: people own their data, and they need to be able to control it and to have some kind of redress in case a company does not give it to them, or they are unable to speak to a company to get control of it.

BUT WHO IS THE RIGHT AUTHORITY TO ENFORCE THIS NEW LAW?

Commissioner Phillips was clear his agency was up to the task. Due to its experience, the capacity the agency has built up, and its understanding of both the legal issues that surround privacy and the economics of privacy, the FTC is in the best position to serve as the federal watchdog for consumer privacy. In fact, Phillips considers that despite the lack of a general consumer data privacy law in the United States, in terms of enforcement and remedies the FTC remains today the leader in privacy enforcement worldwide. "I think there is not any other agency, even armed with GDPR, that has been more effective than the FTC has. So it would be a pity to lose that institutional knowledge and capability moving forward," he said. However, Phillips also recognized that as of today, the FTC does not have enough personnel, budget, etc., and that with an eventual new federal privacy law, the agency will need much more resources.

According to McSweeny, an important key to privacy redress is trying to assess the scope of a privacy harm and the value to attach to it. This isn't easy. In Professor Scholz's view, courts seem to have a particular worry about the standing for privacy plaintiffs, which seems to be rooted in a fear of ending up with very high, unfair, and uncertain awards. Therefore, if by means of a federal privacy law we can make more predictable what happens when there is a privacy violation, we can get courts less scared about vindicating that right. Phillips suggested that the fear in The Hill is to get privacy violations that are so massive that we are not going to be able to handle them. And according to Brill, both types of fears are real, and come from the recognition that, if a federal privacy law is enacted, we will have millions of companies that will not only be subject to robust requirements about how they collect, use and share data for the first time, but also to strong enforcement and penalty authority, and eventually, to the ability of individuals to bring very large class actions against them.

SO HOW TO REDRESS PRIVACY VIOLATIONS IN A WAY THAT ADEQUATELY PROTECTS CONSUMER PRIVACY BUT STILL SATISFIES WHATEVER OTHER INTERESTS MIGHT BE PUSHING BACK?

- **Restitution**

One idea, proposed by Scholz, is restitution (also called "unjust enrichment"). According to Scholz, instead of measuring what is received by a successful plaintiff in terms of its losses, the privacy harm could be measured by what the defendant gained with the privacy violation. "Although the amount of the restitution is not necessarily

always larger than a compensation or other measures, in a lot of consumer privacy cases the dollar value of the harm to the consumer is probably smaller than the benefit of, let's say, a database divided in the number of units in there." In that sense, in comparison to compensation, restitution goes more with intuition and can get around standing problems. Besides, Phillips added, one of the interesting distinctions between compensation and restitution is that the former tends to deter conduct that is more harmful, so you pay more when you endanger people more. In contrast, restitution may also deter conduct that despite being less harmful, is still very profitable.

- **Injunctive relief**

Another idea, for those cases in which the consumer is looking for the harm to stop, or for someone to tell them that they are right, is for courts or agencies to grant an injunction. In Brill's words, "in my almost three decades doing enforcement work in privacy, consumer protection, and competition, mostly what people want is to have the violations to stop, and it is a dignity issue. Sometimes it is restitution, but sometimes it is just to get this practice to stop." However, Brill, Scholz, and McSweeny all encouraged regulators not to entirely dismiss the power of strong monetary fines. According to Scholz, "money fines are very powerful, by making practices prohibitively expensive." Likewise, McSweeny pointed to the deterrent effect that high fines can have. For her, companies' decisions about what kind of compliance program to put in place, how much risk to take about consumer data, and the design of products, are definitely informed by how much a violation would cost.

- **Safe harbors**

The panel also discussed the possibility of creating FTC-approved safe harbors as a defense against violations of the law. More than a redress mechanism, a safe harbor is a way in which a company can have some assurance it is complying with the regulatory framework, while also giving some ability to enforcers to verify that compliance. For McSweeny, while perhaps not a complete solution, it is useful to think about safe harbors as a potential compromise. For Phillips, the first question is which rights you are enforcing, because it is around those rights that you want to build a set of remedies, including the redress that people may have, and then think about safe harbors as a way to ameliorate enforcement or drive companies in the right direction as part of a package. In that sense, while privacy rights are the fundamental issue, redress is a secondary issue, and safe harbors a tertiary one. Brill agreed that safe harbors "can be very helpful for the entire ecosystem: consumers as well as companies" if accompanied by transparency and accountability.

- **Private right of action**

The creation of a private right of action (PRA) was the subject of a heated debate. While several panelists expressed openness to a PRA as one potential tool, Phillips was emphatic in describing the PRA as a bad idea. According to the Commissioner, we think about PRAs as an additional approach to deterrence, a mechanism to do what law enforcement cannot. However, a PRA and the high penalties that can come along with it can end up doing a lot more than just deterrence, by also chilling innovation. Besides, if a PRA is created, enforcement will be driven by economics rather than addressing the worst harms. Phillips added that the political economy that a PRA creates makes it very hard to course correct the law afterwards. "So if you get it wrong, you are sort of stuck."

Brill highlighted that, if the substantive provisions of the federal privacy law are strong, it would be better for the ecosystem to start out with other redress options, such as companies developing internal redress mechanism; giving individuals the ability to go to the state AGs or a new federal program that would mediate their concerns; or perhaps giving individuals the possibility to go to court for injunctive relief. In contrast, a "full PRA" (with actual damages, punitive damages, and attorney's fees) runs the risk of ending up with a large number of companies that will suddenly be facing cases in court with judges that are not prepared to handle these new laws. Therefore, she argued, it would be better to take this slower and let the ecosystem get used to it, giving individuals some kind of redress. Because if we get it wrong, we can end up damaging innovation and potential data use that can responsibly use individuals' data to solve problems.

In contrast, Scholz clearly expressed her position in favor of a PRA. For Professor Scholz, when it comes to this debate there are two mistakes that we should try to avoid: first, thinking that PRAs are only there because we expect public resources to be underfunded; and second, being afraid that an underprepared judge will get things wrong. According to Scholz, in comparison to public actors, actors in the private sphere are the ones who will likely have unique access to information on problematic data use in a highly innovative tech environment. Thus, providing avenues of recourse to the private sphere is important. Likewise, Scholz considers that the only way to deal with the underprepared judges is to have actual cases hitting the courts. And if judges make mistakes, legislators will have to be there to correct those mistakes, which is an ongoing process.

Conclusion

Before adjourning, Professor Ryan Calo asked the participants about their predictions for a 2021 federal privacy law. Although none of them dared to assure that in 2021 the law will be a reality, Commissioner Phillips and former Commissioners Brill and McSweeny showed optimism, while Professor Scholz closed the panel with a plea for more discussion. Overall, the Tech Policy Lab and Microsoft received excellent feedback for the discussion, which is still available to view at this link: http://techpolicylab.uw.edu/resource/redressing-privacy-violations/.