UNIVERSITY OF WASHINGTON TECH POLICY LAB
In partnership with MICROSOFT

PRIVACY REDRESS OPTIONS WORKSHOP

REPORT

MARIA P. ANGEL | ALEX BOLTON*
Authors

RYAN CALO | LAURA GARDNER
Editors

December 2020

* We are indebted to Savannah J. McKinnon for providing us with excellent notes as a record of one of the discussion groups held during the workshop.

Table of Contents

Introduction

On December 10th, 2020, the University of Washington Tech Policy Lab and Microsoft hosted a two-hour workshop on options for privacy redress. Based on a set of four hypothetical enforcement approaches for a federal privacy law, the organizers invited participants representing different perspectives—industry, academia, civil society, and government—to come together to compare and contrast various remedies, mechanisms, and components of privacy redress. The ultimate goal of the workshop was to leverage expertise to help Congress and stakeholders move past privacy legislation gridlock.

Takeaways

Workshop participants were divided into two groups, each focusing on at least two scenarios, and reconvened for discussion. Here are some of the main takeaways of the discussions, presented in terms of possible enforcing authorities, remedies, and other mechanisms available to balance competing interests. Given that the discussions here were held under the Chatham House rules, neither the identity nor the specific affiliation of the participants will appear.

WHO CAN CHALLENGE A PRIVACY VIOLATION?

- **The Federal Trade Commission and the State Attorneys General**

Most of the participants of the workshop agreed that the enforcement of the federal privacy law by both the Federal Trade Commission (FTC) and the State Attorney Generals (AGs) is the bare minimum (described as "table stakes" in one of the discussion groups). In particular, having a strong central regulator that puts out rules and guidance and helps with interpretation was highlighted as critical for newer companies and for the enforcement of systemic privacy requirements.

Participants generally agreed that these agencies have to be endowed with adequate resources in terms of funding, personnel, and expertise. However, some of the members of one of the discussion groups had concerns about the FTC not being up to the task, even if expanded. Others pointed out that the existence of an enforcement agency supplemented by state AGs would necessarily require consistency of what is allowed and what is not, and therefore, would need both clearer rules and a body of caselaw. Finally, many participants agreed that a well-resourced process needs to be created, to allow State AGs and/or FTC to respond to individual complaints. Nevertheless, there were disagreements on what should this process look like.

- **Private right of action**

The source of least agreement was the prospect of a private right of action (PRA). Some participants highlighted the utility of a PRA both in general (to give individuals a remedy to enforce their own rights) and in particular (for people skeptical of government enforcement and for individuals affected by privacy violations in very intense ways). But many questioned the political viability of PRAs. A participant suggested that in deciding about the creation of a PRA, the expansive nature of American jurisprudence and law should be taken into account: legislators should be mindful of the fact that very few causes of action have gone away once established, whereas they can always come back and add more. In contrast, another participant argued there needs to be some degree of private enforcement, because by itself the new built-up regulator is not going to be able to enforce the law. Yet another participant invited colleagues to take into account the importance that PRAs have played for traditionally marginalized communities, who may not entirely trust institutions to vindicate their rights.

With regards to the reach and scope of the individual enforcement, there was greater consensus around a limited PRA. For example, a participant from a nonprofit organization suggested that a PRA could be limited to asking injunctive relief. An industry participant proposed a PRA where a consumer could prove that they suffered cognizable actual damages from the violation of the law. A third participant offered that, based on this participant's research, the recovery of a limited PRA should be measured in terms of gains.

- **Class actions**

Most of the participants of the workshop held concerns regarding a class action. In one of the discussion groups, an industry participant observed that, due to the way in which data is collected in the United States and is utilized by companies, a national class action for violation is likely to end up having tens of millions of people in that potential class. This, added to a given level of statutory damages, can turn out to be a massive dollar amount of damages. Despite this, class actions do not really benefit the class monetarily. Similarly, another participant highlighted the difference of contexts that exist in Europe and in the United States in terms of class actions. Thus, while in the context of the European General Data Protection Regulation (GDPR), which does give individuals the right to sue, there is not a tradition of class actions, in the United States there is a really robust class action culture and framework.

An academic participant highlighted research suggesting a lack of efficacy of class actions to change corporate behavior, taking into account that they are focused on money rather than remedies. According to this participant, when structuring the different remedies there needs to be a matrix of considerations and an explicitness as to what each remedy is trying to achieve, whether it is to achieve a change in corporate behavior or to put money in people's pockets. Other participants rejected the option of class actions out of hand because of concerns over abuse of discovery or because class actions would be a political non-starter.

- **Expanded rights of nonprofit organizations to bring suit on behalf of consumers**

Where it was discussed, expanding the rights of nonprofit organizations to bring suit on behalf of consumers was generally considered by participants as a viable avenue. The public tends to understand that government enforcement entities only bring very large cases over long periods of time, so nonprofit organizations could help to fill the gap. However, a member of a nonprofit organization conditioned this possibility on the FTC carefully choosing what kind of nonprofits are allowed to bring cases. Also, someone from academia was curious about the standing questions that could be raised by allowing non-profit organizations to bring cases on behalf of individuals. Therefore, despite considering it to be better for the articulation of the harm as a group, the participant wondered about how different this would be from other cases in which non-profits bring suit.

KINDS OF REMEDIES

- **Statutory penalties**

An industry participant supported something like the monetary fines included in the GDPR (e.g. percentages of revenues), which could potentially be a deterrent for companies. Expanding on that issue, another participant considered that if that is the case, then it has to be decided whether those statutory penalties are going to be calculated with a cap (like the GDPR), or if there should be a different definition of statutory damages, or no definition at all. For this participant, this is especially important in the context of a possible class action, where it is likely to have tens of millions of people suing. Pushing back, a participant from a nonprofit organization was doubtful about the power of financial penalties. In this participant's view, despite the great amount of manpower and fining authority given to the Data Protection Authorities (DPAs) by the GDPR, they are often paralyzed (citing the UK's Information Commissioner's Office (ICO) as an example). Yet another participant disagreed, observing that the DPAs tend to approach fining very differently, and bringing as examples both the French DPA, which just issued large fines against both Google and Amazon for advertising practices (cookies), and the Irish DPA, which in the next few months is expected to impose large fines in multi-jurisdictional actions.

- **Injunctive relief**

An industry participant suggested that if we want companies to change their behavior and do things in litigation that actually benefit those harmed, then it is necessary to admit that monetary compensation back to class members is a model that just does not work very well, and that injunctive relief should be preferred. A member of a nonprofit organization endorsed that point, further adding that sometimes you just want someone to recognize that something was wrong, even without the need for economic damages. In particular, this participant described injunctive relief as being key for core privacy concerns that we can conceptualize as human rights rather than data protection issues. In those cases, injunctive relief turns to be powerful for challenging undesirable business models. In contrast, one of the academics endorsed the use of injunctive relief as a remedy available for failures to offer meaningful access, correction and deletion rights. However, as a matter of legislative drafting, an academic advised drafters not to label those violations as "procedural violations," but rather as "all other violations for which economic harm is difficult to prove," to avoid the risk of drafting a provision that could be eventually considered unconstitutional under *Spokeo v. Robins*.[1] Finally, two members of nonprofit organizations reacted saying that even though they all agree that injunctive relief is important, so is the ability to have some monetary damages. Absent that, one added, there needs to be some sort of private recourse to courts.

- **Attorneys' fees**

Attorneys' fees were briefly highlighted in one of the discussion groups by a member of a nonprofit organization, as a powerful tool to allow small plaintiffs' attorneys to bring cases without needing massive class actions and massive penalties.

ADDITIONAL MECHANISMS

- **Well-resourced process to allow the FTC to respond to individual complaints**

Only some of the participants reached a discussion of enforcement resources. One proposal, brought up by a member of a nonprofit organization, was to expand the FTC Administrative Law Judge (ALJ) process to allow for someone to bring a case and issue an injunction. This would create a judicial forum for individuals to mandate privacy, and would go beyond hearing and processing complaints, and trying to meet with a mediator. Another idea, proposed by a participant from industry, was to give the FTC the ability and resources to establish consumer mediation programs, like the ones that currently exist in most States. In that sense, the FTC would offer a program where it would take every complaint about and send it off to the business involved and try to get to a solution. However, unlike the GDPR model, where DPAs do this under statutes, having no choice about whether or not to look at every complaint, this should not be considered as a mandatory FTC mediation.

This second proposal caused various reactions among the group participants. On the one hand, some participants highlighted the similarities of the proposed mediation model with the US Equal Employment Opportunity Commission's and with the Shield Ombudsperson procedure. On the other hand, a member of a nonprofit organization pushed back on the proposal, arguing that the State-like mediation model would often be helpful to help consumers get paid back (e.g. "I got ripped off buying a camera"), but not necessarily to challenge fundamental data practices (e.g. "I want Facebook to stop tracking me around the web" or "I want Google to stop driving its car around photographing cul-de-sacs"). For this participant, in the latter case there would need to be a mandate for a judge or judge-like object to determine that the practice violated the statute.

As a response, the proponent of the mediation model countered that the proposed process was mainly for the inattention of "procedural claims" (e.g. "I wanted to delete my data but the company didn't delete it," or "I wanted to access my data but I didn't see all of it"), without prejudice to the fact that the agency could decide to pick up and

[1] Ever since Lujan v. Defenders of Wildlife, all injuries to have jurisdiction in federal court have to be actual. In addition, in Spokeo v. Robins Justice Alito stated that a bare "procedural violation" is not actual. Therefore, just as a matter of legislative drafting it is very dangerous to talk about "procedural violations" because a good lawyer defending a lawsuit can say that that is outside the scope of Article III.

run with the action on a broader basis. Besides, the author of the proposal added that even in the example of the Google Maps car, an individual who did not want to have their home part of a video/mapping program could ask that this practice be stopped, and the data deleted –assuming the practice was inappropriate. However, the member of the nonprofit organization once again pushed back, highlighting the need for a declarative statement that "photographing cul-de-sacs is illegal (or not)," rather than just the company agreeing to stop photographing someone's house. In other words, although it is nice if the agency decides to take up the case, consumers need a vehicle to force a determination.

- **Safe harbors**

Some participants were especially skeptical about allowing the creation of FTC approved safe harbors as a defense against violations of the law. For example, a participant highlighted how consumer advocates tended to have problems with safe harbors because of their lack of transparency and clear oversight. In contrast, other participants agreed on allowing safe harbors. However, an academic participant argued that self-certification should be avoided. Instead, a minimum of necessary annual or bi-annual examination / audits, alongside a publication requirement, should be required to come with any safe harbor, to ensure that the entity is living up to its compromises. Similarly, a participant from industry suggested that safe harbors should be carefully structured, setting up criteria about their content and ensuring that they are FTC-approved. Under those conditions, a safe harbor could be something that small entities could definitely avail themselves of. Specially—added a member of a nonprofit organization—, because they see them (e.g. the COPPA safe harbor programs) as the place where they can get all their legal advice on how to comply with the law.

- **Public disclosure of independent 3rd party audits**

Interestingly, opinions about the usefulness of publicly disclosing the results of independent 3rd party audits of companies were very similar in both discussion groups. Both a member of a nonprofit organization of one of the groups and someone from industry – large tech in the other group emphatically claimed that the public disclosure of those results would not help anybody ("would be less than worthless"). However, in one of the groups a member of the academy pushed back on this previous characterization, arguing that being able to see the results of these audits could be useful, so if they were going to be required, it would be better to have them published rather than not.

Several industry participants were unified in suggesting a system where there were requirements for companies of an appropriate size to have a 3rd party independent audit of their data collection and usage (similar to bank supervision). For one of the proponents, this would elevate the industry, increase compliance, and make a shift from the old paradigm of just self-regulation, to something that would substantially enhance the compliance with whatever the federal law is. For the other proponent, this would allow the intervention of experts, who unlike the general public, know the right questions to ask and the formulas to apply.

- **Internal appeal mechanisms**

In one of the discussion groups, a member of a nonprofit organization considered that it would be interesting to require companies to provide internal appeal mechanisms for some of the things that are "more procedural" (e.g. access, correction, deletion, and transparency), where you don't want to look at the nature of the right, but for the consumer to be able to correct, access, delete or be able to get the proper transparency. In that sense, internal appeal mechanisms would be useful for cases where what you want is to vindicate your right, not to punish the company. However, some members of the other discussion group were more skeptical about this mechanism. For example, one of the academics contended that, given that many people face small intrusions in their privacy which do not really care about, it is very likely that very few people will actually end up utilizing the internal appeals mechanism. Similarly, someone from industry – large tech highlighted that even though companies take these complaints very seriously in order to avoid litigation, the majority of individuals do not have the time to exercise these mechanisms. For those reasons, someone from industry – large tech suggested that for the internal appeal

mechanisms to count as a prerequisite of litigation, there should be some rules (e.g. as part of a safe harbor) as to what an internal appeal process and an ideal resolution timeline, should look like.

- **Notice and right to cure**

Only some participants discussed a notice and right to cure. A participant proposed that in case of "procedural issues" it could also be helpful for companies to have an opportunity to fix the problem before it went to court. This idea, commonly known as a "notice and cure provision," was also supported by another person from and by a member of a nonprofit organization. However, the latter wondered if there would be a way to get a "right to cure" with enforcement discretion, to be able to override it for things that were willful by the company, or where the company has been really irresponsible. Similarly, another member of a nonprofit organization stressed that it would be highly problematic if companies get a free bite of the apple, or can violate the law until they are specifically told not to. Therefore, although there is usually no scienter requirement in consumer protection law, this participant thought that companies' moral culpability should be considered by regulators and judges in determining appropriate remedies or whether to intervene. Finally, two academics highlighted that there is a difference between (a) not intending the harm and (b) not intending the act, and would push against (a) hiding in (b). In fact, one of them even anticipated some companies ("the Wyndham of privacy perhaps") doing nothing, only responding to the complaints made and ignoring the rest, but telling regulators how hard they are working responding so diligently to consumer complaints.

Therefore, and as one of the academics noted, in addressing this mechanisms the participants of this group—like the two political parties in Washington D.C., ultimately diverged on who the law is intended for. Thus, while corporate types were worrying about well-meaning companies getting burned, consumer types worried about bad companies getting away with wanton harm infliction.

Conclusion

It seems to be clear that redress for individual violations of privacy is one of the core issues that must be addressed if we want to be able to move forward with comprehensive privacy legislation in the United States. However, redress is not a binary choice. Who can challenge the violations of the comprehensive privacy law? What kind of remedies should exist? Are there any additional mechanisms to balance interests? Each of these three areas of discussion drove participants of the workshop to both agreements and sticking points.

For example, there seems to be consensus on the central enforcement role of the FTC and the State AGs, as well as on the need to expand their authority and resources. Likewise, there appears to be a common understanding about the current inconvenience of allowing the introduction of class actions and about the reduced impact that the publication of independent 3rd party audits could eventually have. However, when it comes to the PRA, the statutory penalties, the safe harbors, the internal appeal mechanisms, and the notice and right to cure provision, there are still disagreements with regards to their convenience. Likewise, conflicts persist on the ideal reach and scope of other mechanisms, such as the rights of nonprofit organizations to bring suit on behalf of consumers, the injunctive relief, and the well-resourced process that needs to be created in the State AGs and/or FTC to respond to individual complaints.

This conversation has to keep going. Yet now it is clearer than before that the FTC enforcement and the PRA are not the only two available options. Rather, there is an ample set of different elements that we can build into redress and enforcement, to ensure that the federal privacy law offers consumers a real possibility of remedy for privacy violations.