Regulatory Transparency Project

Unlocking Innovation & Opportunity

Modern Privacy Advocacy: An Approach at War with Privacy Itself?

Cyber & Privacy

Justin "Gus" Hurwitz

Jamil N. Jaffer

This paper was the work of multiple authors. No assumption should be made that any or all of the views expressed are held by any individual author. In addition, the views expressed are those of the authors in their personal capacities and not in their official/professional capacities.

To cite this paper: Justin Hurwitz, et al., "Modern Privacy Advocacy: An Approach at War with Privacy Itself?", released by the Regulatory Transparency Project of the Federalist Society, June 12, 2018 (https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper-Incoherent-Privacy.pdf).

12 June 2018

Privacy is one of the defining policy issues of our time. In the digital era, privacy concerns are omnipresent. From advertisers and online platforms seemingly tracking our every move online, to ongoing discussions about law enforcement's need for access to encrypted communications to protect us against terrorists and other violent criminals, to the geopolitics of countries spying on one another's citizens, concerns about individual privacy arise constantly in the public and private spheres, both domestically and abroad. But while concerns about privacy may be a defining issue of our time, that does not mean that privacy – at least as understood today by its most fervent advocates – is itself a well-defined concept. To the contrary, privacy, as it is promoted today by well-heeled lobbyists from all manner of three-letter NGOs and often funded by Silicon Valley tech companies guiltily worried about their own massive data collections, is a fundamentally incoherent concept. This incoherence is a defining characteristic both of privacy as a concept and the modern debates around that concept. Specifically, we are concerned that privacy advocates often discount the impact of their ostensibly privacy-supporting activities on other privacy-related values and, more often than not, take positions that while appearing on the surface to protect privacy actually serve to undermine it (or aspects of it) in the long-run.

This incoherence matters quite a bit. We should all be deeply concerned about privacy as a general matter, and we should be prepared to protect it against depredations by private entities seeking commercial gain, governments seeking to snuff out political dissent and free speech, and individuals promoting agendas that we may not support. After all, our nation was founded by men and women who rightly had a healthy skepticism of overweening executive power, particularly as it intersected with the private sphere of the home and where it sought to intrude upon those core liberties that our framers sought to codify in the first ten amendments to our Constitution. But the privacy claims made by modern advocates overreach. This overreach pushes the privacy values they mean to defend to incoherency and risks undermining the very privacy rights that need defending. We owe it to ourselves to check these over-ambitious claims so as to not undermine our legitimate efforts to protect our privacy, or worse, create actual poor outcomes, net-net, for individual privacy.

Consider, for example an issue from an earlier technological iteration of today's fights: caller ID. Caller ID today is considered a basic feature of telephone calls and, indeed, most would consider it privacy enhancing, akin to allowing individuals to know who is at the door before allowing them into their home. Just as the peephole allows you to guard your home from all manner of visitors, including the now-fairly rare door-to-door salesperson or evangelist, so too caller ID protects the iPhone in your pocket from the modern war dialers and solicitors.

But when Caller ID was introduced in the early 1990s, many of today's most prominent privacy advocates were among its fiercest opponents. From their perspective, Caller ID was a forced disclosure of personal information about the person initiating the call. To be fair, these advocates were generally concerned about legitimate cases where disclosure of that information could prove problematic: whistleblowers, for instance, being unable to make anonymous calls; abuse victims unable to receive phone calls from shelters without their abusers being aware of the call's origin. But hindsight teaches us that these advocates' concerns about these specific issues were, at best, the

tail wagging a much larger dog of an issue; a dog, by the way, that ended up being much better for individual privacy.

The story of Caller ID is a classic demonstration of one of the basic challenges of privacy: namely, its reciprocal nature. My right to know who is calling me (that is, who is seeking to invade my privacy) comes at the expense of the caller's right to control disclosure of their identity. There is no reason to assume, at the outset, that one or the other of these values is necessarily the more important to protect. No matter the general merits of a given rule, there will always be specific cases in which the general rule gets things wrong. As a result, the general efficacy of such a rule can wax or wane as technology, social values, and political realities change. One lesson from this is that we can (and should) be cautious about adopting rules that are prescriptively rigid. With Caller ID, for instance, the market has responded with technologies and services that allow legitimate blocking of Caller ID information when needed to preserve sensitive information. This flexibility, supported and fostered by policies that were initially derided by the so-called "privacy community," has ultimately led to a world that largely supports both sides of the privacy value proposition.

We see similar incoherence in more contemporary examples. Consider the long-running Wiretap Act litigation against Google's Gmail service. When Gmail receives an email for one of its users, it electronically scans the contents of that email in order to target focused advertising to that user. This includes emails sent to Google's users, even by people who don't use Gmail. Over a decade ago a group of consumers – who were not Gmail users – sued Google, arguing that Google's scanning of their emails violated their privacy rights, as protected by the Wiretap Act.

The suit was ultimately settled after more than a decade of litigation. But it settled on terms that once again demonstrate the incoherence of the underlying privacy construct crafted by modern privacy groups. Google agreed to stop scanning the contents of emails at the time they were received by its email services. Instead, Google agreed that it would wait until those emails had been delivered to the intended recipient's email inbox. Then, Google, relying on the explicit consent of the owner of the inbox could conduct the exact same scan it had previously done and deliver the exact same ad it would have previously.

As a result of this change – which literally amounts to requiring that Google's email scanning systems wait a fraction of a second longer before scanning emails – the privacy advocates and plaintiffs' lawyers who brought suit take the view that Google is no longer violating the privacy rights the of non-Google users. No matter that nothing of substance has changed from a practical or a privacy perspective. In many ways then, one might reasonably ask whether the privacy claims being raised here are merely a charade designed to raise funds for advocates and line the pockets of trial lawyers all the while agitating average Gmail users and making Google reorganize its otherwise perfectly acceptable technology, all for naught.

Or consider another suit against Google, in which the Google StreetView vehicles were WiFi-enabled and recorded not only images of houses taken from the public streets but also the names and locations of wireless networks being broadcast from those houses. Once again the Wiretap Act was invoked, this time by lawyers (including, to be fair, one of the authors of this piece for at least a

short time) and privacy advocates arguing that Google had violated the privacy rights of homeowners by recording the network names their routers were broadcasting over the public airwaves. Never mind that the Wiretap Act expressly exempts information broadcast over public airwaves from protection under the Act; and never mind that wireless networks can be configured expressly not to broadcast their names by privacy-concerned users.

Amazingly, in this case, the Ninth Circuit held that WiFi's public broadcasting of packets on public radio spectrum was *not* covered by the Wiretap Act's exemption of broadcasts on radio spectrum, despite the signals being *broadcast on radio spectrum*. Oddly, at least one implication of this opinion is that each one of us violates the Wiretap Act any time our computer displays to us a list of WiFi networks available in the local area because we are obtaining and recording – at least temporarily – the broadcast packets from these WiFi networks. Once again, while there is no coherent (or practical) distinction between Google intercepting those packets as part of its mapping service and your computer intercepting them to display it to you, other than perhaps the ephemeral timeframe for which you hold the relevant data. Of course, in one instance privacy advocates claim the sky is falling, while in the other ordinary citizens go about their business happy to be able to get on the local airport WiFi without having to find a kiosk to ask for the network name. Privacy, it seems, is very much in the eye of the beholder.

And, of course, there's the never-ending debate between the privacy groups and the national security and law enforcement communities over encryption. As demonstrated all too well in the aftermath of the 2015 San Bernardino terrorist shooting, companies like Apple have taken steps – ostensibly in an effort to protect user privacy – to encrypt data in a manner that makes it virtually impossible for law enforcement to access, even with a lawful court order. While on its face this might seem like a purely privacy enhancing move, consider both the short- and long-term ramifications of Apple's decision to pick a fight with the government and to refuse to assist it with its completely sensible (and lawful) request to access the work phone – owned by the county government – of the San Bernardino shooter. In that case, even though Apple had the consent of the owner of the phone and the FBI had obtained a court order from a judge requiring Apple to provide assistance to the government, Apple fought back, aggressively taking the position that providing such assistance would be inappropriate to do so and would undermine the privacy of its (in this case, terrorist) user(s). The FBI was ultimately able to access the terrorist's phone by obtaining an exploit from a private company that took advantage of a heretofore undisclosed vulnerability in Apple's encryption system. Of course, Apple immediately demanded that the FBI hand over this vulnerability so that Apple might protect its users from further such hacks, and, not surprisingly, having faced down a completely unreasonable Apple in court, the FBI refused. The net outcome of this fight: law enforcement got access to the data on the phone, Apple played no role in assisting with (or potentially limiting) such access, and tens of thousands of iPhone users became instantly more vulnerable, with both a private company and the FBI having access to an exploit that rendered their hardware-based encryption ineffectual. Hardly a privacy-enhancing outcome.

And worse still, this incident, with Apple and privacy groups backing the most extreme position possible – that they wouldn't help law enforcement access the work phone of a known terrorist after

over a dozen people were brutally murdered in broad daylight – will almost certainly be cited down the road when the government seeks to obtain legislation mandating lawful access to encrypted data in the aftermath of a mass-casualty terrorist attack. This is because if privacy advocates and technologists of all stripes continue to stamp their feet, scrunch up their eyes, and remain unwilling to work on potential options for lawful access to encrypted data ahead of time, we are likely to see a solution imposed by political leaders that will at once be insufficient to do the job, while excessively costly both from both the financial and privacy perspectives.

At the end of the day, there are a few things that perhaps ought to be said about modern privacy advocacy. First, as a general matter, it comes from a good place. These are advocates genuinely committed to protecting and defending a critically important right of individuals. Second, protection of individual privacy is something that we all ought to cherish as it is a cornerstone of our system of democratic governance, and it is at the heart of the very ideals that our framing generation sought to uphold in crafting our Constitution. Third, and perhaps most important, privacy is not an incommensurable good that ought not be weighed against other values, but rather, one that must be protected in light of the larger dynamics and threats that might ultimately result in worse outcomes. After all, our framers never once thought that our private spaces were forever invulnerable against government access; to the contrary, they specifically provided for such access, setting up a system of neutral, third-party magistrates and specific legal standards to be met before the government might obtain such access. The final lesson we've learned about modern privacy advocacy is that privacy overreach – of the variety practiced by most (if not all) of today's modern advocacy groups – is often likely to result in worse outcomes for privacy, regardless of the noble intent of those promoting such efforts.

The bottom-line, therefore is this: while privacy is a critical value that we all must fight to defend, when we engage in that fight without an eye towards the bigger picture and the short- and long-term consequences of our privacy claims, we may often end up doing more harm than good for this critical value that we all seek to protect.