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

Justin "Gus" Hurwitz*
Jamil N. Jaffer*

Abstract

This Article argues that the modern concept of privacy itself, particularly as framed by some of its most ardent advocates today, is fundamentally incoherent. The Article highlights that many common arguments made in support of privacy, while initially seeming to protect this critical value, nonetheless undermine it in the long-run. Using both recent and older examples of applying classic privacy advocacy positions to key technological innovations, the authors demonstrate how these positions, while seemingly privacy-enhancing at the time, actually resulted in outcomes that were less beneficial for consumers and citizens, including from a purely privacy-focused perspective. As a result, the authors advocate for a privacy approach that focuses on the long-term results of particular proposals rather than the immediate results in a given circumstance.

---

* Associate Professor of Law, Director of the Nebraska Governance and Technology Center, and Co-Director of the Space, Cyber, and Telecom Law Program, University of Nebraska College of Law; Director of Law & Economics Programs, International Center for Law & Economics; Program Affiliate, NYU School of Law Classical Liberalism Institute; Visiting Fellow, Antonin Scalia Law School National Security Institute. JD, University of Chicago, 2007; MA, George Mason University (economics), 2010; BA, St. John's College, 2003. This Article originally appeared on the website of the Federalist Society's Regulatory Transparency Project.

* Assistant Professor of Law, Founder and Executive Director of the National Security Institute, and Director of the National Security Law & Policy Program, Antonin Scalia Law School at George Mason University; Affiliate, Center for International Security and Cooperation, Stanford University. JD, University of Chicago, 2003; MA, United States Naval War College, 2006; BA, UCLA, 1998.

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,[1] to ongoing discussions about law enforcement's need for access to encrypted communications to protect us against terrorists and other violent criminals,[2] to the geopolitics of countries spying on one another's citizens,[3] 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 is because the way privacy is talked about publicly is often at odds with privacy-enhancing outcomes. This incoherence is a defining characteristic both of privacy as a concept and the modern debates around that concept. Indeed, it is this very incoherence that leads privacy advocates to often discount the impact of their ostensibly privacy-supporting activities on other privacy-related values and, more often than not, to take positions that, while appearing on the surface to protect privacy, actually undermine aspects of it in the long-run.

This incoherence matters quite a bit. As a general matter, we should all be deeply concerned about privacy and ought 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 malign agendas. After all, our nation was founded by men and women who rightly had a healthy skepticism of overweening executive

1. *See, e.g.*, Gabriel Weinberg, *Google and Facebook are watching our every move online. It's time to make them stop*, CNBC, https://www.cnbc.com/2018/01/31/google-facebook-data-privacy-concerns-out-of-control-commentary.html (last updated Feb. 1, 2018, 12:30 AM) (according to Princeton Web Transparency & Accountability Project, "76 percent of websites now contain hidden Google trackers, and 24 percent have hidden Facebook trackers[.]").

2. *See, e.g.*, Tom Ridge, *Law Enforcement's Encryption Dilemma*, HILL (Sept. 16, 2019, 11:30 AM), https://thehill.com/opinion/cybersecurity/461558-law-enforcements-encryption-dilemma.

3. *See, e.g.*, Alissa J. Rubin, *French Condemn Surveillance by N.S.A.*, N.Y. TIMES (Oct. 21, 2013), https://www.nytimes.com/2013/10/22/world/europe/new-report-of-nsa-spying-angers-france.html.

power,[4] particularly as it intersected with the private sphere of the home as well as where it sought to intrude upon the core liberties codified in the first ten amendments to our Constitution. Unfortunately, the privacy claims made by modern advocates often overreach and push the privacy values they mean to defend to incoherency, all the while undermining the very privacy rights that need defending. We owe it to ourselves to check these overambitious claims so as to not undermine our legitimate efforts to protect our privacy, or worse, create actual poor outcomes, 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 (or the modern doorbell cam) allows you to guard your home from all manner of unwanted 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 dialing robocallers and other solicitors.

But when Caller ID was introduced in the early 1990s,[5] some of today's most prominent privacy advocates were among its fiercest opponents.[6] From their perspective, Caller ID was a forced disclosure of personal information about the person initiating the call.[7] To be fair, these advocates were generally concerned about legitimate cases where disclosure of that information could

4. *See, e.g.*, THE FEDERALIST NO. 47 (James Madison).

5. Rules and Policies Regarding Calling Number Identification Service–Caller ID, 59 Fed. Reg. 18318 (April 18, 1994), https://www.fcc.gov/document/rules-and-policies-regarding-calling-number-identification-service-3.

6. *See, e.g.*, Cindy Skrzycki, *Caller ID: Grappling With Issues of Privacy*, WASH. POST (June 21, 1991), https://www.washingtonpost.com/archive/business/1991/06/21/caller-id-grappling-with-issues-of-privacy/8fffd9cb-a14a-4ed7-9286-8cba7637b39d/; States News Service, *'Caller ID' Stirs Debate on Phone Privacy*, N.Y. TIMES (Feb. 11, 1990), https://www.nytimes.com/1990/02/11/nyregion/caller-id-stirs-debate-on-phone-privacy.html (quoting Marc Rotenberg, who a few years later founded EPIC); Anthony Ramirez, *Caller ID: Consumer's Friend of Foe?*, N.Y. TIMES (Apr. 4, 1992), https://www.nytimes.com/1992/04/04/news/caller-id-consumer-s-friend-or-foe.html; Mark Calvey, *Caller ID: Is Anybody Out There?*, S.F. BUS. TIMES (Oct. 13, 1996 9:00 PM), https://www.bizjournals.com/sanfrancisco/stories/1996/10/14/focus4.html (discussing Caller ID privacy concerns and noting the Privacy Rights Clearinghouse, which published a "Privacy FAQ" about "Caller ID and My Privacy"); *see also Fact Sheet 19: Caller ID and My Privacy*, PRIVACY RIGHTS CLEARINGHOUSE (Aug. 2000), https://web.archive.org/web/20110524111020/http:/www.privacyrights.org/fs/fs19-cid.htm.

7. Skrzycki, *supra* note 6.

prove problematic: whistleblowers, for instance, being unable to make anonymous calls and abuse victims unable to receive phone calls from shelters without their abusers being aware of the call's origin.[8] 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, in many ways, is a classic demonstration of one of the basic challenges of privacy: namely, the reciprocal nature of privacy claims and rights. 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.[9] There is no reason to assume, at the outset, that one or the other of these values is necessarily more important to protect. No matter the general merits of a given privacy rule, there will always be specific cases in which the general rule gets things wrong. As a result, the general efficacy of such a privacy rule can wax or wane as technology, social values, and political realities change. One lesson to be taken from this inherent feature of privacy claims is that we can (and should) be cautious about adopting privacy 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 (and benefits from) both sides of the privacy value proposition.[10]

We see similar incoherence in more contemporary examples. Consider the long-running Wiretap Act litigation against Google's Gmail service.[11] When Gmail receives an email for one of its users, it electronically scans the contents of that email to target focused advertising to that user.[12] This includes emails sent to Google's users, even by people who don't use

8. *See* States News Service, *supra* note 6.

9. *See* Skrzycki, *supra* note 6.

10. *See, e.g.*, Ernie Smith, *Know Who's Calling*, TEDIUM (Dec. 5, 2019), https://tedium.co/2019/12/05/telephone-caller-id-history/.

11. *See generally* 18 U.S.C. § 2511 (2018); *In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 WL 5423918, at *1 (N.D. Cal. Sep. 26, 2013).

12. *Google Inc.*, 2013 WL 5423918, at *1.

Gmail.[13] Nearly 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.[14]

The suit was ultimately settled after nearly a decade of litigation.[15] 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.[16] Instead, Google agreed that it would wait until those emails had been delivered to the intended recipient's email inbox.[17] Then, Google, relying on the explicit consent of the owner of the inbox, could conduct the exact same scan it had previously conducted and deliver the exact same ad it would previously have served up.[18]

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 of the non-Google users.[19] No matter that nothing of substance has changed from a practical or a privacy perspective. Given this episode, and many others like it, 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 Wi-Fi-enabled Google Street View vehicles (those responsible for the detailed local images available in Google Maps) recorded not only images of houses taken from the public streets, but also the names and locations of wireless networks being

13. *See* Matera v. Google Inc., No. 15-CV-04062-LHK, 2016 WL 5339806, at *1 (N.D. Cal. Sep. 23, 2016).

14. *See id.* at *4.

15. *See* Mot. Prelim. Approval Class Action Settlement and Mem. P. & A., *Matera*, No. 5:15-cv-04062 LHK.

16. *See id.* at 5.

17. *Id.*

18. *Id.*

19. *Id.* ("Class Counsel believes that these technical changes are substantial and that these changes, once implemented, will bring Google's email processing practices in compliance with Class Counsel's view of the California Invasion of Privacy Act . . . and the Electronic Communications Privacy Act . . . .").

broadcast from those houses.[20] 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.[21] Never mind that the Wiretap Act expressly exempts information broadcast over public airwaves from protection under the Act,[22] and never mind that wireless networks can be configured expressly not to broadcast their names by privacy-concerned users.[23]

Amazingly, in this case, the Ninth Circuit held that the public broadcasting of packets on public radio spectrum with Wi-Fi routers was *not* covered by the Wiretap Act's exemption of broadcasts on radio spectrum, despite the signals being broadcast on radio spectrum.[24] 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 Wi-Fi networks available in the local area because we are obtaining and recording—at least temporarily—the broadcast packets from these Wi-Fi 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, 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 Wi-Fi without asking around 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.[25] As demonstrated all too well in the aftermath of the 2015 San

20. *See* Joffe v. Google, 746 F.3d 920, 922–23 (9th Cir. 2013).

21. *Id.* at 922.

22. 18 U.S.C. § 2511(2)(g)(i) (2018).

23. *See Joffe*, 746 F.3d at 931 ("[T]he recipient of those communications [can decide] to secure her wireless network . . . [by] tak[ing] care to encrypt her own Wi-Fi network.").

24. *Id*. at 929–31.

25. *See, e.g.*, Katie Benner, *Barr Asks Apple to Unlock Pensacola Killer's Phones, Setting Up Clash*, N.Y. TIMES (Jan. 13, 2020), https://www.nytimes.com/2020/01/13/us/politics/pensacola-shooting-iphones.html; *see also* Charlie Savage, *Justice Dept. Revives Push to Mandate a Way to Unlock Phones*, N.Y. TIMES (Mar. 24, 2018), https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html.

Bernardino terrorist shooting, and more recently in the case of the Saudi military shooter in Pennsylvania, 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.[26] 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 county-owned work phone 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, and that to do so would undermine the privacy of its (here, terrorist) user(s).[27] 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.[28] Of course, Apple immediately demanded that the FBI hand over this vulnerability so that Apple might protect its users from further hacks; not surprisingly, having faced down a completely unreasonable Apple in court, the FBI refused.[29] 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.[30]

And worse still, this incident with Apple and privacy groups backing the

26. *See* Benner, *supra* note 25 and accompanying text.

27. *Id.*

28. Ellen Nakashima, *FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone*, WASH. POST (Apr. 12, 2016), https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

29. *See id.*

30. *See, e.g.*, Jamil N. Jaffer & Daniel J. Rosenthal, *Why Apple's Stand Against the F.B.I. Hurts Its Own Customers*, N.Y.TIMES (Apr. 8, 2016), https://www.nytimes.com/2016/04/09/opinion/why-apples-stand-against-the-fbi-hurts-its-own-customers.html; Jamil N. Jaffer & Daniel J. Rosenthal, *How Apple's Fight with the FBI Will Hurt Our Privacy*, POLITICO (Feb. 26, 2016), https://www.politico.com/agenda/story/2016/02/how-apples-fight-with-the-government-hurts-our-privacy-000055/.

most extreme position possible—that they wouldn't help law enforcement access a known terrorist's work phone after more than 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.[31] 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 being excessively costly from both the financial and privacy perspective.[32]

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.[33] 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

31. *See* Jamil N. Jaffer & Daniel J. Rosenthal, *Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge*, 24 CATH. U. J. LAW & TECH. 273, 278–81 (2016), https://scholarship.law.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1012&context=jlt.

32. *Id*.

33. *See, e.g.*, U.S. CONST. amend. IV.

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.

***