2021

Beware of Giant Tech Companies Bearing Jurisprudential Gifts

Kiel Brennan-Marquez

BEWARE OF GIANT TECH COMPANIES BEARING JURISPRUDENTIAL GIFTS†

*Kiel Brennan-Marquez**

Giant tech companies are not a brooding omnipresence in the sky,[1] but mostly because their rapacious approach to data surveillance leaves little time for brooding. They are certainly omnipresent, and their role in contemporary life has an eerie, ethereal quality — not unlike the nineteenth-century projections of legality that so disquieted Justice Holmes and his allies. It took the realists a generation to dismantle the *mythos* of formalism.[2] This case requires nothing so grand, but we could still use a healthy dose of realism. Giant tech companies are not our advocates. They are not our friends. They are giant companies. Their concerns about consumer privacy run exactly — and only — to the extent of their business interests. Everything else is just peripheral noise.

In *Privacy as Privilege*, Professor Rebecca Wexler argues that courts should stop construing the Stored Communications Act[3] (SCA) to block criminal defense–side subpoenas for communication records.[4] She has woven a narrative in which communication privacy collides with the ability of criminal defendants to mount a robust case. This story is not wrong; such collisions occur. The more important story, however, is a slightly different one. It originates from the same facts, and it also features disadvantaged criminal defendants. But they are not the main characters. Rather, the main characters are the giant tech companies that have routinely been served with defense subpoenas (under the SCA), appeared in court to contest those subpoenas, and won — securing "privacy victories" for their users. And the moral of the story, boiled down, is that we should beware of these victories; for they are not quite what they appear. A system in which the boundaries of communication privacy are negotiated at the behest of the very entities whose profit model relies on their erosion is not a healthy one. It may be preferable

† Responding to Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721 (2021).

* Associate Professor of Law and William T. Golden Scholar, University of Connecticut School of Law. The author would like to thank Michael Fischl, Brendan Maher, Julia Simon-Kerr, Doug Spencer, and Rebecca Wexler for helpful feedback. Additionally, Morgen Barroso and Ryan Coleman provided invaluable research assistance.

[1] *See* S. Pac. Co. v. Jensen, 244 U.S. 205, 222 (1917) (Holmes, J., dissenting) ("The common law is not a brooding omnipresence in the sky but the articulate voice of some sovereign or quasi-sovereign that can be identified . . . .").

[2] *See, e.g.*, Lon L. Fuller, *American Legal Realism*, 82 U. PA. L. REV. 429, 429–30 (1934).

[3] 18 U.S.C. §§ 2701–2712.

[4] Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721 (2021).

to a system in which *no* communication privacy is protected. But it merits little praise beyond that.

In terms of genre, Wexler's narrative is tragic. It conjures to mind a world in which two relatively powerless actors — criminal defendants and consumers — are pitted against one another, a conflict fated for zero-sum resolution. Longer term, however, the more important narrative is not a tragedy. It is a polemic. And its focus is not on the less powerful characters, but the more powerful ones: the surveillance state and its corporate handmaidens, both of whom would prefer all of us, as subjects of power, to imagine their relationship in oppositional rather than synergistic terms.

* * *

The problem animating Wexler's Article is easy to see. Trials depend on informational abundance,[5] whereas privacy laws create pockets — some small, some vast — of informational scarcity.[6] And more specifically, the SCA, as a privacy law, limits access to communication records in ways that can thwart the presentation of a robust defense. By construing the SCA to bar defense-side subpoenas, Wexler argues, courts have created a de facto evidentiary privilege, one that "shield[s] an ex ante category of [possibly exculpatory information] from [compulsory legal] process."[7] In Wexler's view, this outcome is lamentable; the point of *Privacy as Privilege* is that courts should reverse course.

I find little to disagree with in Wexler's core claim. As a value, exculpation is quite important. And, as a tool for shoring up this value, compulsory process is likewise.[8] Furthermore, the SCA seems like an odd legal instrument for counteracting these principles, and the court decisions canvassed by Wexler appear, accordingly, to suffer from a profound lack of imagination — to say the least.

The lingering question, if we take Wexler's account seriously, is where privacy ultimately stands. As she acknowledges, open-ended discovery and admissibility — as ingredients of the trial process — are at

---

[5] *See, e.g.*, Babette Boliek, *Prioritizing Privacy in the Courts and Beyond*, 103 CORNELL L. REV. 1101, 1128 (2018) (explaining trial courts' reluctance to limit discovery on privacy grounds).

[6] *Cf.* Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235, 258 (2015) ("[P]rivacy harms cannot be completely ignored simply because a civil case is pending. Rather, even civil discovery has limits — limits that necessarily draw on important privacy-based principles.").

[7] Wexler, *supra* note 4, at 2746.

[8] *See, e.g.*, Chambers v. Mississippi, 410 U.S. 284, 297–98 (1973) (holding that the Constitution limits the extent to which generally applicable exclusionary rules could hamper the ability of a criminal defendant to mount the defense of his choosing).

some level *necessarily* at odds with privacy.[9] For privacy is an antiaccuracy value.[10] That is the source of both its precariousness and its grandeur; to speak in the language of privacy is to highlight aspects of human flourishing that transcend, and can in principle justify setting aside, our collective commitment to the discovery of truth.[11]

As such, it is only to be expected that privacy protections — like those in the SCA — would operate, at times, to the detriment of fact-finding in particular cases. The question is whether the tradeoffs are worth it. Wexler thinks not, and she offers two intertwined arguments in service of that view. The first is a procedural argument about the *route* by which courts have limited defense-side access to communication records. The second is a substantive argument about why barring such access may, on balance, be unwise. I will briefly discuss these arguments in turn.

The procedural argument, which comprises the heart of Wexler's Article, concerns the relationship between statutory interpretation and evidentiary rules. Statutes designed to constrain information flow can, in principle, impact the trial process by limiting the latter's inputs; in light of this restraint, the interpretation of such statutes always runs a risk of thwarting the goals of evidence law. In Wexler's view (and I agree), that is exactly what rigid interpretations of the SCA do: they frustrate the ability of criminal defendants to develop a maximally persuasive defense. Furthermore, she argues (and once again, I agree), statutory interpretations that bar access to an entire category of information, creating a de facto privilege, should be subject to a strict construction rule.[12] The SCA contains no such statement, so it should be read permissively.

Even if all this is right, however, it does not tell us whether a privilege along the lines enacted by courts — an "Internet privilege," in Wexler's phrase[13] — is warranted on the merits. In fact, as Wexler acknowledges, lawmakers and judges have myriad tools at their disposal *apart* from rigid statutory interpretation to arrive at the same essential endpoint. In her words:

> [I]f legislators or courts are displeased with the result, options are available to them. Congress could amend the SCA to enact a novel statutory eviden-

---

[9] *See generally* Robert D. Keeling & Ray Mangum, *The Burden of Privacy in Discovery*, 20 SEDONA CONF. J. 415 (2019); Boliek, *supra* note 5; McPeak, *supra* note 6.

[10] *See, e.g.*, Stephen E. Henderson, Commentary, *A Few Criminal Justice Big Data Rules*, 15 OHIO ST. J. CRIM. L. 527, 537 (2018) ("[I]n considering these norms [of privacy values] we must remember — and not shy away from — the fact that limited government norms, such as the Fourth Amendment, tend to be *anti*-accuracy norms.").

[11] McPeak, *supra* note 6, at 286.

[12] Wexler, *supra* note 4, at 2763–68.

[13] *Id.* at 2790.

> tiary privilege that unqualifiedly bars criminal defendants from subpoenaing technology companies for the contents of online communications. Or, courts could rely on their common law authority to craft such a privilege from whole cloth, provided they first undertake the required balancing of the competing interests.[14]

To this list, I would add that the rulemaking committee for the Rules of Evidence could propose a new specialized relevance rule — Rule $409^{3/4}$ — that limits the admission, and perhaps also the discovery, of communication records for specific purposes.[15]

Given all this, the question becomes substantive. Wexler's complaint is not merely about interpretive hijinks; it runs to the merits. In her view, the legal system ought not to deprive criminal defendants of access to exculpatory evidence contained in communication records, period — whatever the instrument of deprivation. At one point, in fact, she characterizes the worry about communication privacy that underwrites the status quo approach to the SCA as an argument "dressed in privacy clothing" but bereft of a real core.[16] In reality, Wexler maintains, lifting the bar on defense-side subpoenas for communication records "would impose zero cost to privacy."[17]

If true, this would be a devastating objection to existing law, because it would mean that courts have not only distorted the SCA but done so gratuitously. Yet is it true? Here, Wexler's argument boils down to two claims.[18] The first is that individuals "with legitimate privacy interests" — in other words, people who do not want enormous batches of records about their private communications to be accessible at any time

---

[14] *Id.* at 2786–87 (footnotes omitted).

[15] Although specialized relevance rules, at least in the federal system, limit only admission of evidence at trial, not pretrial discovery, *see* FED. R. EVID. 407–411, some courts have construed the rules more expansively to bear on access as well as admissibility, *see, e.g.*, *In re* Teligent, Inc., 640 F.3d 53, 58 (2d Cir. 2011) (holding that a heightened showing is required for discovery of materials whose admission would likely be barred by Rule 408); Vardon Golf Co. v. BBMG Golf Ltd., 156 F.R.D. 641, 651 (N.D. Ill. 1994) (same for Rule 407); Kakule v. Progressive Cas. Ins. Co., No. 06-4995, 2008 WL 1902201, at *5 (E.D. Pa. Apr. 30, 2008) (barring discovery outright because of concern about admissibility under Rule 407). *But see* Doe No. 1 v. United States, 749 F.3d 999, 1008 (11th Cir. 2014) (holding that Rule 410 "governs the admissibility of plea negotiations, not the discoverability of them"). Details aside, the conceptual point is that specialized relevance rules are yet another mechanism by which criminal defendants are denied the capability to marshal potentially exculpatory evidence at trial. *See, e.g.*, GEORGE FISHER, EVIDENCE 132 (3d ed. 2013) (providing a factual scenario in which a specialized relevance rule would clearly operate to the detriment of a criminal defendant).

[16] Wexler, *supra* note 4, at 2779.

[17] *Id.* at 2780.

[18] To be fair, Wexler also gestures toward the possibility that some people may "[lack] legitimate privacy interests in subpoenaed information" under the SCA. *Id.* at 2779. Although this is theoretically possible — and may be true in certain narrow circumstances — the strong default presumption is that communication records are *paradigmatically* privacy sensitive. Because Wexler has, for good reason, offered no grounds to dislodge this presumption, I will say no more about this particular argument.

by all defense lawyers — could move to quash defense "subpoenas . . . served on technology companies."[19] For a variety of reasons that have been thoroughly expounded in the privacy literature, and which I will list here only briefly, this solution is unlikely to have much bite in practice. The reasons include problems with notice,[20] a regressive political economy of legal "self-help,"[21] the hardship of having to assess the privacy sensitivity of enormous quantities of communication data,[22] and, most fundamentally, the fact that the motion-to-quash tool, even when accessible and effective, is simply not that protective of privacy.[23]

Perhaps out of an implicit sense of these difficulties, Wexler quickly pivots to her second argument. Namely, even if many people would be unable to effectively avail themselves of this protection in practice, it does not matter; the countervailing benefits for criminal defendants are still greater. "Concededly," Wexler writes, there will be a group of individuals "whose privacy interests are unknown because, for instance, they cannot be located or contacted" — or I would add, because they move to quash subpoenas for communication records but are simply unsuccessful — who:

> stand to lose control over information with unknown privacy value. . . . But protecting such speculative privacy interests with the current, unqualified SCA bar on criminal defense subpoenas is wrong. As an initial matter, it is overbroad; it blocks access to private and nonprivate evidence alike. Additionally, any hypothetical privacy interests in this category of communications are, by definition, unjustified by any legal showing, and should thus be considered waived. Speculative privacy interests that no one has raised

---

[19] *Id.* at 2780.

[20] *Compare* Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, NEW AM.: OPEN TECH. INST. (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy [https://perma.cc/TR6T-DYB8] ("Notice and consent is too weak in practice to meaningfully shield individual privacy."), *with* Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 371–72 (2014), *and* Facebook, Inc. v. Superior Ct. (Chan), 417 P.3d 725, 728 (Cal. 2018), *and* Facebook, Inc. v. Wint, 199 A.3d 625, 628 (D.C. 2019).

[21] Indeed, this is one of the reasons why "self-help" approaches to privacy protection have been notoriously unsuccessful. *See, e.g.*, Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71, 76 (2016).

[22] Imagine if you were served with a defense-side subpoena for "all emails related to X, Y, Z over a year-long period," and you had to decide which of those emails were sufficiently privacy sensitive to cause concern (and to merit a potential legal challenge to prevent compliance). It might literally require months of full-time work to determine.

[23] Indeed, this concern is why there has been such a protracted, high-stakes fight about the importance of warrants in the Fourth Amendment context: it seems insufficient for law enforcement to rely on subpoena power alone. *See, e.g.*, Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 128; Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 826 (2005).

> in court should not outweigh the sober need for relevant evidence in criminal proceedings.[24]

On what evidence does this final assertion — that the interests of criminal defendants are more important, in aggregate, than countervailing interests in communication privacy — come to rest? Wexler may, of course, believe the assertion to be true. And she may ultimately be right. But the essence of the privacy argument, the one Wexler denigrates as merely "dressed in privacy clothing,"[25] is that her claim is backward.

In other words, the privacy argument here *just is* that the privacy interests in this realm are more important, in aggregate, than the countervailing interests of criminal defendants. And this is hardly an unfamiliar or outlandish argument. In fact, it is the same argument, in form, that underpins the Fourth Amendment's approach to digital privacy. There, of course, the interests on the "legal process" side of the ledger run to the state, not to defendants. But the *privacy* interests are virtually identical — and the Supreme Court has recently made clear, echoing decades of scholarly agitation, that subpoenas provide insufficient accommodation of those privacy interests.[26] Instead, warrants are necessary.[27] This does not necessarily mean, of course, that warrants (or the equivalent) should be required for defense-side discovery. With different interests at stake, the balance may net to a different equilibrium.[28] But it does give us prima facie reason to doubt that a subpoena regime, standing alone, suffices to accommodate the relevant privacy interests — foundational as they are to the health of our democratic culture.[29] And, at a minimum, it means that waving the problem away, designating it a matter of fashion rather than substance, cannot be the right answer.

* * *

There is, however, a different sense in which Wexler is right to characterize the legal arguments in favor of an SCA bar to defense-side subpoenas as "dressed in privacy clothing," despite being, in the last analysis, about something else entirely. That something else is corporate power. Giant tech companies *do* cloak their arguments about the SCA

---

[24] Wexler, *supra* note 4, at 2782–83.

[25] *Id.* at 2779.

[26] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

[27] *See Carpenter*, 138 S. Ct. at 2217; Riley v. California, 573 U.S. 373, 403 (2014).

[28] *See, e.g.*, Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1043–44 (2014) (outlining the argument that we ought to be more concerned about defense-side errors — and by extension, limited access to information — than the prosecutorial equivalent).

[29] *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012); *see also* Allen, *supra* note 21, at 71–72.

in the rhetorical garb of privacy. The wrinkle, however, is not (as Wexler would have it) that their arguments genuinely fail to implicate privacy. It is that privacy values are, so to speak, the argument's incidental beneficiaries. The primary beneficiary is a radical, deregulatory — even antinomian — vision of information capitalism.

This point echoes one of Wexler's own. Ultimately, she writes, the main "effect of the current SCA privilege is not to protect privacy but, rather, to exempt technology companies from the administrative burdens of complying with judicial compulsory process."[30] And it is quite "unclear," she continues, "why these companies should receive this special treatment when other companies and private individuals all must shoulder the public duty of supplying relevant evidence to the courts."[31]

In spirit, I wholeheartedly agree — but I would use a less measured tone. In my view, not only is it unclear why tech companies should receive "special entitlements" with respect to legal process; it is quite clear they should not. Giant tech companies may differ from other powerful corporations. But if they do, it runs exclusively in the direction of *bearing* duties, not avoiding them. For instance, it may be, as I and many others have argued, that giant tech companies have fiduciary obligations[32] — in a manner roughly analogous to doctors, lawyers, and financial advisors — to their users, above and beyond the baseline duties of contract, tort, and property law.[33] Similarly, some have argued (so far unsuccessfully in court) that giant tech companies have *constitutional* obligations, given the totalizing role they play in our expressive and political lives.[34] Yet even if these "heightened duty" arguments fail to carry the day, their plausibility only goes to show that giant tech companies are distinctive, if at all, in ways that call out for greater restriction, not greater license.

In fact, take a step back. Why would anyone think giant tech companies deserve special legal treatment? The answer lies, I think, in an elaborate, dismayingly successful PR campaign. For decades now, giant

---

[30] Wexler, *supra* note 4, at 2783–84.

[31] *Id.* at 2784.

[32] *See* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 617 (2015); Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 7 (2018); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://perma.cc/E9KY-K447]; *cf.* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 501 (2019) (questioning whether fiduciary obligations are sufficient to address problems of information asymmetry and market dominance).

[33] *See* Brennan-Marquez, *supra* note 32, at 616–38 (unpacking the doctrinal implications of this idea).

[34] *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017) (discussing information companies as the "public square"); Prager Univ. v. Google LLC, 951 F.3d 991, 998 (2020) (declining to apply Marsh v. Alabama, 326 U.S. 501 (1946), to social media).

tech companies have been cultivating an aura of renegade independence, a riff on the famous Marlboro Man aesthetic — charismatic, world weary, flirting with anarchy[35] — but reimagined through a cyber-punk lens.[36]

The PR campaign has also infused litigation strategy. For example, as Wexler notes, Facebook and Google recently submitted a petition for certiorari about the SCA issue, arguing against "prioritiz[ing] a criminal defendant's desire to obtain communication [records]" over "trust in the privacy of electronic communications."[37] And this is just the tip of the iceberg. In the last few years, Microsoft has argued (1) that provisions of the SCA allowing the government to seek an order limiting disclosures to users about records requests violates the First and Fourth Amendments,[38] and (2) — more famously — that it need not comply with properly issued warrants for user data, so long as the data is being "stored" outside the jurisdictional territory of the United States.[39] Similarly, Facebook has argued against compliance with warrants, not just subpoenas, on user-privacy grounds.[40] What is more, giant tech companies are not alone in making these arguments; they are routinely supported by prominent, well-heeled, progressive advocacy organizations like the ACLU[41] and the Electronic Frontier Foundation (EFF).[42]

Politics, they say, can make for strange bedfellows — and that may be part of the explanation here. But I cannot help but detect a sense of resignation as well. If privacy politics have devolved into a prolonged negotiation of the terms of surrender to the titans of information capitalism, these developments make some sense; they represent a rational strategy by a weaker party, trying to pull as much potential value as

---

[35] *See* Barry Vacker, *The Marlboro Man as a Twentieth Century David: A Philosophical Inquiry into the Aristotelian Aesthetic of Advertising*, 19 ADVANCES CONSUMER RSCH. 746, 753–54 (1992).

[36] *See* David Mayer, *Why Google Was Smart to Drop Its "Don't Be Evil" Motto*, FAST CO. (Feb. 9, 2016), https://www.fastcompany.com/3056389/why-google-was-smart-to-drop-its-dont-be-evil-motto [https://perma.cc/K2ME-GYG5].

[37] Petition for a Writ of Certiorari at 10, Facebook, Inc. v. Superior Ct., 417 P.3d 725 (Cal. 2018) (No. 19-1006), *cert. denied*, 140 S. Ct. 2761 (2020).

[38] Microsoft Corp. v. U.S. Dep't of Just., 233 F. Supp. 3d. 887, 896 (W.D. Wash. 2017).

[39] United States v. Microsoft Corp., 138 S. Ct. 1186, 1187 (2018) (per curiam).

[40] *See In re* 381 Search Warrants Directed to Facebook, Inc., 78 N.E.3d 141, 150 n.8 (N.Y. 2017).

[41] *See, e.g.*, Brief of *Amici Curiae* New York Civil Liberties Union & American Civil Liberties Union in Support of Appellant's Opposition to Appellee's Motion to Dismiss at 1–2, *In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23 (App. Div. 2015) (No. 14014), 2014 WL 12672712.

[42] *See, e.g.*, Brief for *Amici Curiae* Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, the Constitution Project, & Electronic Frontier Foundation in Support of Appellant at 3–4, *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) (No. 14-2985), 2014 WL 7277562 [hereinafter EFF Brief].

possible out of the negotiation. This is certainly the sensibility on display in recent legal scholarship, which emphasizes the "intermediary" role that giant tech companies can play in keeping the surveillance state at bay.[43] Tech companies, the logic goes, may not have the public interest — or indeed, *any* normative interest — at heart. But they can at least be counted on, consistent with their business model, to run interference.[44]

From a mercenary perspective, the "surveillance intermediary" model may be attractive. For reasons both substantive and procedural, digital privacy rights have proven difficult to secure through direct litigation.[45] The Supreme Court has, of course, long been hostile to class actions[46] — an especially important vehicle in the privacy context, where injuries are typically small and diffuse.[47] But that is only the beginning. In recent years, the Court has expressed doubt about Article III standing for privacy claims, even in settings where Congress has sought to create private rights of action,[48] and at least one member of the Court has signaled that *cy pres* remedies — another important tool in privacy litigation — may soon be on the chopping block.[49] Put all this together, and it is not hard to see the appeal of having giant tech companies litigating on behalf of their users. It may be nothing more than a stopgap measure. But the gap it aims to stop is significant.

From a more aspirational perspective, however, the status quo looks more discouraging. It seems like an unambitious rallying cry, putting the point rather mildly, to demand simply that giant tech companies comply with normal legal process. Normal legal process is not perfect, of course. It has blemishes and lacunae; it evolves very slowly. Particularly in the context of digital records, historical tools have proven

---

[43] *See, e.g.*, Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665, 669 (2019); Riana Pfefferkorn, *Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?*, 49 CONN. L. REV. 1393, 1408–09 (2017); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 105 (2018); Steven Song, *Keeping Private Messages Private: End-to-End Encryption on Social Media*, B.C. INTELL. PROP. & TECH. F., 2020, at 1, 11; *see also* Ian Samuel, *The New Writs of Assistance*, 86 FORDHAM L. REV. 2873, 2888–90 (2018) (arguing intermediaries will ultimately be limited by government power).

[44] *See Developments in the Law — More Data, More Problems*, 131 HARV. L. REV. 1714, 1724 (2018); Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 2 GEO. L. TECH. REV. 275, 290–91 (2018).

[45] *See* Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 656–57 (2019).

[46] *See generally* Robert H. Klonoff, *The Decline of Class Actions*, 90 WASH. U. L. REV. 729 (2013).

[47] *See* Scholz, *supra* note 45, at 681–83.

[48] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1552–53 (2016) (Thomas, J., concurring) (explaining — as applied to the privacy setting — that standing rules serve separation of powers principles that fall beyond the reach of legislative reconfiguration).

[49] *See* Frank v. Gaos, 139 S. Ct. 1041, 1047–48 (2019) (Thomas, J., dissenting).

to be largely ineffective, and reconfiguration — of just the sort we are beginning to see in the Fourth Amendment context[50] — is needed.

But the reconfiguration ought to be a political and jurisprudential process in which the public, as the main interest holder on both sides of the ledger — concerned about both the fate of communication privacy and the operation of the criminal justice system — should have the final say. It should not be a reconfiguration for the primary benefit of private business interests, even if those interests happen to align, contingently and temporarily, with the public good. In terms of shorter-term tactics, it may be tempting to capitalize on such alignment. But the winds of alignment are fickle, and longer term, the better strategy — the genuinely democratic strategy — must lie elsewhere.

On this front, *United States v. Microsoft*,[51] the "extraterritorial warrant" case from 2018, is exemplary. Microsoft was served with a warrant to turn over communication records related to one of its users.[52] In response, the company argued that the relevant records were held in Ireland, so they fell beyond the warrant's territorial scope.[53] The case made its way up the appellate chain, and Microsoft litigated relentlessly.[54] It focused especially on the geopolitical implications of compliance — what precedent would it set to have one sovereign (in this case, the United States) compel the cross-border extraction of data via ordinary legal process?[55] According to the company, it would spell the end of digital privacy worldwide.[56] And — just as in the SCA cases canvassed by Wexler — the ACLU, EFF, and other privacy-oriented advocacy organizations agreed.[57]

There is an important sense, however, in which the entire litigation was built on unsound foundations. That the case persisted so long is beside the point; it goes to show only the sheer quantity of resources Microsoft was willing to commit to the process. In fact, the case had

---

[50] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018); Riley v. California, 573 U.S. 373, 403 (2014).

[51] 138 S. Ct. 1186 (2018).

[52] *In re* a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467–68 (S.D.N.Y. 2014).

[53] *Id.* at 470.

[54] *Microsoft*, 138 S. Ct. at 1187 (per curiam) (describing procedural history).

[55] *See, e.g.*, Brief for Respondent at 3, *Microsoft*, 138 S. Ct. 1186 (2018) (No. 17-2), 2018 WL 447349 (arguing that a ruling for the government — requiring compliance with the warrant — would invite a situation in which "foreign government[s]" could "unilaterally seize[] . . . personal documents stored [anywhere in the world] — whether in a home, safe-deposit box, or computer server").

[56] *Id.*

[57] *See* Brief for Brennan Center for Justice at NYU School of Law, American Civil Liberties Union Foundation, Electronic Frontier Foundation, Restore the Fourth, Inc. & R Street Institute as *Amici Curiae* in Support of Respondent at 22–26, *Microsoft*, 138 S. Ct. 1186 (2018) (No. 17-2), 2018 WL 555814.

little — in some sense, nothing — to do with privacy. The underlying warrant had been issued on probable cause. Probable cause is a mechanism of privacy protection. It may be imperfect. It may be subject to erosion.[58] But it is nevertheless, and axiomatically, the main legal tool we use to enforce privacy interests against the government.

Accordingly, for Microsoft to resist compliance with a validly issued warrant on privacy grounds was, at bottom, to thumb its nose at the agreed-upon mechanisms of legal process. It was to play the role of jurisprudential vigilante. As Professor Paul Ohm put it:

> Microsoft's entire course of conduct — from setting up its remote datacenters in a way that permits users to select where to place their data to suing the federal government for seeking a warrant to investigate a drug crime — could be cast as a gambit that isn't about respecting the rules of Ireland or the United States or the rights of the Irish or the Americans. It is perhaps part of a much more cynical and pernicious move to declare independence from [sovereign governments] . . . . This seems more East India Company than Thomas Paine. Revolutions should not be declared by corporations, they should reflect the will of the people, in this case, the users.[59]

Ohm is right: revolutions should not be declared by giant companies.[60] But in some sense, this gives Microsoft too much credit. The company was not making a revolutionary claim. Like the other companies discussed in Wexler's Article who have invoked the SCA to resist compliance to subpoenas, Microsoft was making a deregulatory claim. All it *really* sought to do was fend off the state. The idea was not to upend sovereignty or to facilitate a grand rebalancing of geopolitical power. It was to proceed, business as usual, with all the benefits of a world defined by sovereign power — but without the hassle of compliance or the downsides of enhanced visibility into corporate operations.

This "gambit," as Ohm rightly describes it,[61] should be resisted. It is a gambit characteristic of gilded economies: a strategy adopted by powerful economic actors to convince those lesser off that everyone's interests are, on a deeper level, aligned against an overreaching state. The gambit comes in many shapes and sizes, but its core is always the same. And its paradigm case, in the American legal imagination, is plain. Joseph Lochner was not a baker; he was a bakery owner.[62] But

---

[58] *See* Kiel Brennan-Marquez, Search and Seizure Ceilings 2 (unpublished manuscript) (on file with the Harvard Law School Library) (arguing that suspicion standards like probable cause are, in essence, information-processing burdens — requiring police to build a "mini case" against their targets in advance of intrusion — that become more dilute as technological change makes information easier to process).

[59] Paul Ohm, *The Microsoft Design Decisions That Caused This Mess*, JUST SEC. (Feb. 21, 2018), https://www.justsecurity.org/52805/microsoft-design-decisions-caused-mess [https://perma.cc/6AAB-NCEK].

[60] *See* Eichensehr, *supra* note 43, at 685.

[61] Ohm, *supra* note 59.

[62] *See* Lochner v. New York, 198 U.S. 45, 46 (1905).

still he managed, through deft legal representation, to get the Supreme Court to focus on the way in which "limiting the hours in which grown and intelligent men may labor to earn their living [represents a] meddlesome interference[] with the rights of the individual."[63] Mr. Lochner had a vanishing fraction of the resources giant tech companies do. Imagine where they could focus — or have already focused — the judiciary's attention.

[63] *Id.* at 61.