Legal Backgrounder

Vol. 36 No. 3 March 12, 2021

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

The Fraught Path to a Federal Privacy Law Businesses Can Live With

by Corbin K. Barthold

Congress Wants Privacy

Although the wait for federal data-privacy legislation continues, Republicans and Democrats generally agree on what such a law should look like. The two most prominent bills are the Consumer Online Privacy Rights Act (COPRA), introduced by Senator Maria Cantwell (D.-Wash.) in November 2019, and the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act, introduced by Senator Roger Wicker (R.-Miss.) in September 2020. Both bills would empower a user to see what data a business has about her. Both would give a user the right to have the data corrected or deleted. Both would empower a user to obtain a copy of the data in portable form. And both would provide the right to opt out of various forms of data transfer or collection.

Are each of these provisions a good idea? Perhaps not. It's been argued, for instance, that a right to data portability will *reduce* data security: someone who steals your identity can then steal your data.[1] And a right to opt out is, in effect, a right to freeride on other users. Too many freeriders could lead to fewer free (or, if you insist, pay-with-data) services on the Internet. It appears, however, that these qualms have fallen by the wayside, and that the core of any federal privacy law will be access, correction, deletion, portability, and a right to opt out.

What's in the Way?

So why the deadlock? There are two main sticking points. First, federal preemption. The SAFE DATA Act preempts all state data-privacy laws, while COPRA preempts only those that "directly conflict" with it. Under COPRA, businesses would remain subject to strict state laws, as well as to state laws that conflict. And because it's difficult if not impossible to tailor Internet service by state — it's hard even to know where a given Internet user resides — each state could potentially use its privacy law to dictate data practices for the country as a whole.

Second, private rights of action. Although both bills provide for enforcement by the Federal Trade Commission and state attorneys general, only COPRA provides for suits by private actors. COPRA says, in fact, that a person may sue for a violation of *any* provision; that *any* violation qualifies as an "injury in fact"; and that a plaintiff may obtain statutory damages of at least $100 per violation per day. In effect COPRA invites class actions that allege a minor infraction, multiply it across millions of users and hundreds of days, and thereby assert a damages calculation in the billions or even trillions of dollars.

---

[1] Alec Stapp, *GDPR After One Year: Costs and Unintended Consequences*, Truth on the Market, May 24, 2019, https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/.

Corbin K. Barthold is Internet Policy Counsel at TechFreedom.

To pass legislation, the parties will have to compromise on these two overriding issues. The simplest path forward is for one side to cede ground on preemption, the other on private suits. The Democrats, of course, control the House, the Senate, and the White House. They have the whip hand. They can tilt the compromise in their favor. But so long as there's a filibuster, they'll need Republican votes in the Senate. So if legislation is to pass, compromise there must be.

A Rock and a Hard Place

Say you run a business that will have to comply (as most businesses will) with whatever law ultimately passes. Pick your poison. Do you want greater preemption, or less private enforcement? There is no good option.

Without preemption, problems abound. First and most obviously, state laws can make incompatible demands. Any user that can confirm her social-security number may access her data, might say one state. Only a user who completes a multi-factor authentication may do so, might say another. To whom should the company listen? On other issues, meanwhile, states can race to the top, with the strictest law becoming the *de facto* national standard. If some states have an opt-in system for data collection, for instance, while others require only that a user have a chance to opt out, opt-in will become the nationwide default. And finally, even where their terms are identical, state laws can be applied by different states in different ways. Portability, for instance, could mean one thing in one state's courts, another thing in another's. All in all, businesses gain little, absent preemption, from even having a federal law.

Yet giving way on private federal suits is hardly better. Government actors are expected to prosecute in the public interest. They have reason, at least in theory, to pursue the worst offenders, rather than the deepest pockets. And they will, at least in theory, be held to account by voters if they're too aggressive. Plaintiffs' lawyers, by contrast, have next to nothing holding them back. Seekers of profit, they are only too ready to exploit each loophole, to enlarge each vagueness, to push each boundary, that a statute's words present them. Language being the flawed tool that it is, moreover, every statute will present them many sections, clauses, and lines worth testing.

Consider COPRA. The Act bars data practices that are "likely" to cause, among other things, a "reputational" or "other substantial" injury to a person. Yet it does not define "likely," "reputational," "substantial," or "injury." The Act gives entities latitude, assuming they take "reasonable measures," to deal in data that can't "reasonably" be used to form "infer[ences]" about, or "link[s]" to, specific people, households, or devices. Yet it does not define "reasonable measures," "reasonably," "infer," or "link." The Act entitles a plaintiff to "not less than $100 and not greater than $1,000 per violation per day," but it does not define "violation."

It is no answer that the Act authorizes the Federal Trade Commission to issue regulations expounding on what these terms mean. An agency can issue all the rules (and guidance papers, circular letters, and memoranda) it wants. The written word, that imprecise instrument, is typically no match for a sharp plaintiff's lawyer determined to press each opening to the full. If anything, adding page upon page of rules and guidance simply creates more complexities, confusions, and contradictions for that lawyer to feed on.

The combination of a private right of action, a statutory damages provision, and an ill-defined concept of "violation" is especially destructive. Some courts have let plaintiffs' lawyers use a statutory-damages remedy to certify a class without showing much in the way of commonality among the class's members. The uncertainty over what counts as a violation, meanwhile, enables those lawyers, by drawing the finest imaginable lines among infringements, piling one supposed category of infringement on another, and then aggregating across a large number of class members, to generate fantastic damages calculations. This immense figure then serves as the starting point in the negotiation over a class settlement and fee award.

Large companies that deal with lots of customers, such as Google, can face, and have faced, privacy suits where the plaintiffs' damages calculation equals the GDP of a small European country.[2] There have been some hefty payouts. Take one recent class action brought under the Illinois Biometric Privacy Act. Facebook used facial-recognition software to identify when a user's friends appear in an uploaded photograph. Although the named plaintiffs admitted that this feature had caused them no harm, their lawyers sought tens of billions of dollars in statutory damages for the class. Facebook settled the suit for $650 million.

Uniformity or Bust

Forced to choose between avoiding state law and avoiding federal private suits, companies are likely to decide that preemption is what they can't live without. Imagine trying to comply with fifty states' distinct, sometimes idiosyncratic, often conflicting notions of what it means to collect, package, transfer, safely store, provide access to, correct, or delete data. Left to themselves, states will not even define "data" consistently. And of course, many state laws will contain that most open-ended, most ambiguous, most litigated of all legal terms: "reasonable." It's hardly surprising that, as Cameron F. Kerry, a Brookings Institution fellow, reports, "some businesses are considering what [private] remedies they might be able to live with if meaningful preemption is on the table."[3]

With preemption in hand, companies could turn to trying to blunt a private right of action's sharper edges. Ideally private suits would be limited to individual (rather than class) actions and actual (rather than statutory) damages. In place of the class mechanism, federal law could offer a streamlined, arbitration-like procedure for small claims. These measures would deprive plaintiffs' lawyers of their fee-heavy class-action settlements, and, for that reason among others, Democrats will strongly oppose them. (COPRA, for its part, bans arbitration.) Businesses should remind legislators of the havoc wrought by the trial bar, yet be ready, given the balance of power in Congress, for their pleas to fall on closed ears.

Standing Questions

There is another reason why preemption should be the paramount goal. With just a federal law in play, companies that handle data might have a stroke of luck in court. Recall how COPRA asserts that a violation of any of its provisions, no matter how vague, obscure, or technical, is an injury in fact. "A violation of this Act or of a regulation under this Act with respect to the covered data of an individual," it says, "constitutes a concrete and particularized injury in fact to that individual." COPRA says this, of course, because only a person who has suffered an injury in fact has standing to sue in federal court. COPRA's authors want the bill's private right of action to have the broadest possible scope.

But Congress can't simply declare a bare statutory violation to be an injury in fact. Nor can it concoct such an injury by attaching statutory damages to conduct that causes no real-world harm. Although the Supreme Court gives weight to Congress's views on what qualifies as an injury, it reserves for itself the power to decide which purported injuries are too abstract to confer standing. "The requirement of injury in fact," Justice Scalia once wrote for the Court, "is a hard floor of Article III jurisdiction that cannot be removed by statute."[4]

If a credit reporting company sends you your credit file in two mailings instead of one, have you been injured? The Court will grapple with that question this term in *TransUnion v. Ramirez*. No one disputes that the plaintiff alleged an injury under the Fair Credit Reporting Act. He was allowed to represent a class, however, with many people who were subjected to (at most) a mere procedural infraction: they received their credit file in two letters. The class includes even those who never opened the envelopes.

---

[2] *See, e.g., In re Google Referrer Header Privacy Litig.*, 2014 WL 1266091 (N.D. Cal. Mar. 26, 2014).

[3] Cameron F. Kerry, *Game on: What to Make of Senate Privacy Bills and Hearing*, TechTank, Dec. 3, 2019, https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/.

[4] *Summers v. Earth Island Inst.*, 555 U.S. 488, 497 (2009).

ISBN 1056 3059

Google, Facebook, and other tech companies filed an *amicus* brief urging the Justices to confirm that every member of a class must have standing, and to hold that a small *risk* of concrete harm is not an injury in fact.[5] If two mailings instead of one is no injury — and, for that matter, even if it is — some technical violations of a federal privacy law would not confer standing to sue.

Limiting a federal private right of action would be an uphill fight. The judiciary is likely to find that even minor mishandlings of data inflict concrete harm. (An intangible injury can still be concrete.) But a federal privacy law that combines preemption and a private right of action would at least let firms use the requirements of Article III to defeat insubstantial suits that allege trivial mistakes.

What Next?

With so much else to occupy Congress — climate change, race relations, a pandemic, a recession, infrastructure, health care, and pushes for labor, tax, broadband, and antitrust reform — it would be all too easy to let privacy legislation continue to languish.

But tech companies have become a favorite target of activists, journalists, and lawyers, a cultural development that politicians have not failed to notice. Although there are clamors for reform, many paths to legislation are illusory. There is much talk, for instance, of amending or repealing Section 230, the law that protects websites from liability for the speech of their users. But the parties have opposite goals: Democrats want to encourage more content moderation, Republicans less. Unable to agree elsewhere, the legislators might spot that on privacy, at least, they can compromise, pass a law, and say they've tried to curb Big Tech.

And as Congress dithers, the states are moving forward. California, Illinois, New York, Washington, Virginia, Florida, Utah, and Oklahoma have passed, or are close to passing, major privacy legislation.[6] More states are sure to follow. Businesses are starting to face the very tangle of disparate privacy laws that only a federal law can unwind. There is growing pressure to act.

[5] Brief for eBay, Inc., *et al.*, as *Amici Curiae* Supporting Petitioner, *Trans Union LLC v. Ramirez*, No. 20-297 (U.S. Feb. 8, 2021), https://bit.ly/2OgSuE0.

[6] Rebecca Klar and Chris Mills Rodrigo, *New State Privacy Initiatives Turn Up Heat on Congress*, The Hill, Feb. 10, 2021, https://thehill.com/policy/technology/538122-new-state-privacy-initiatives-turn-up-heat-on-congress.

ISBN 1056 3059