2020

A Recent Renaissance in Privacy Law

Margot Kaminski
University of Colorado Law School

DOI:10.1145/3411049

Margot Kaminski

▸ **James Grimmelmann,** Column Editor

Law and Technology
A Recent Renaissance in Privacy Law

Considering the recent increased attention to privacy law issues amid the typically slow pace of legal change.

Until very recently, it was difficult to be an optimist about privacy in the U.S. Privacy laws in the U.S. have been notoriously ineffective. U.S. companies engage in rampant data profiling, from established giants like Google, to shadowy data brokers like Axciom, to headline-grabbing startups like Clearview AI. Edward Snowden's 2013 revelations about the scope of U.S. national security surveillance showed the extensive cooperation, and sometimes even active involvement, of private companies. In 2015, and again in 2020, the top European Union court invalidated the framework that allowed U.S. companies to export E.U. persons' data to the U.S., reasoning that U.S. privacy protections are too weak.

But both privacy talk and privacy law in the U.S. have shifted sharply toward increased protection. U.S. companies now often must comply with both European and California regulations. State after state has enacted new privacy laws, and Congress has been making the most serious attempts at enacting a national privacy law in decades. Former U.S. Presidential candidate Andrew Yang even made data privacy a centerpiece of his campaign.

Privacy isn't dead, it turns out. It is very much alive. We are just learning, finally, how to talk about it.

The Data Privacy Dark(er) Ages

The U.S. has historically had a messy but extensive patchwork of privacy laws. The state privacy tort of "intrusion upon seclusion" prohibits obnoxious snooping like taking surreptitious photos in someone's house, and "public disclosure of private fact" prohibits publishing embarrassing secrets. There are some sector-specific privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA), which protects health data. State-specific laws, like California's anti-paparazzi law, have been adapted to address newer technologies such as drones. There are wiretapping laws, some Fourth Amendment protections against surveillance by law enforcement, and general-purpose consumer protection laws that have recently been interpreted to hold companies to their published privacy policies.[1,9]

Privacy isn't dead, it turns out. It is very much alive. We are just learning, finally, how to talk about it.

What the U.S. does not have, however, is a comprehensive (or "omnibus") national data privacy law. This puts the U.S. out of step with much of the world, most strikingly the E.U., which now famously has the General Data Protection Regulation (GDPR). Unlike the U.S. patchwork, the GDPR applies to all personal data regardless of sector, and does not contain the kind of easy workarounds companies

IMAGE BY ANDRIJ BORYS ASSOCIATES. USING SHUTTERSTOCK

have found in U.S. privacy laws. For example, U.S. companies that process personal health information point out HIPAA does not apply to them, because they do not technically provide health services or insurance. Others have argued they can ignore privacy laws as long as they work with "anonymized" data, even when it is easily reidentifiable.[4]

U.S. privacy law has mostly been built around the concept of "notice and choice," which relies on giving individuals information (notice) about company practices and letting them make a choice (choice) about whether to hand over their data. All of us who regularly ignore privacy notices and click "I agree" to access websites know this does not work. Even broader versions of notice, such as requiring companies to notify consumers of data security breaches, often fail to incentivize good company behavior, since in reality consumers have few choices about which companies to use.

E.U.-style data protection, by contrast, puts in place substantive requirements that "follow the data."[6] That is: under a true *data protection* regime, you can still get access to your information, request a correction or deletion, or require that a company stop processing your information, even if you initially voluntarily handed your information over to the company.

Perhaps the biggest structural weakness in U.S. privacy laws has been the maxim that once you hand your personal data over to somebody else, you assume the risk they will share it further. This rule does not fit everyday expectations about privacy: when you share your personal health information with your doctor, you do not expect that they will go tell your employer.[7] But this reasoning runs throughout U.S. privacy law. It has gutted the privacy torts discussed here—courts have found that people do not have an expectation of privacy in information they have handed over to online platforms.[3] It is only very recently (in a Fourth Amendment case about cellphone location tracking, *Carpenter v. United States*) that courts have started to question this reasoning.

The irony is that we now think of as a "European" approach to privacy is actually very similar to some U.S. data privacy laws from the 1970s, like the Privacy Act of 1974, which regulates government databases. These early laws required transparency about how data is collected and used, restricted some kinds of sharing and use, and gave individuals rights to correct incorrect data and sometimes even have it deleted. In fact, these Fair Information Practice Principles (FIPPs), which now form the backbone of data protection laws around the world, arguably originated in the U.S. These principles were built upon the understanding that data privacy is largely about power, and that without transparency and accountability, the accumulation of data dossiers about individuals by governments and companies leads to huge power imbalances. These imbalances have consequences not just for individuals, but for democratic values and society at large.

So the U.S. does have privacy laws. But there are gaping holes between existing privacy laws; outdated understandings of reasonable expectations of privacy; and plenty of ways for companies to evade, avoid, or challenge the application of what privacy laws do exist.

But recently, things have started changing.

The Beginning of a Renaissance?

A line of Supreme Court cases addressing government surveillance heralds the recent shift in U.S. thinking about privacy: these cases recognize expectations of privacy in public, that we expect privacy even when we hand information over to technology providers, that data analysis can reveal sensitive information from individually innocuous data points.[5] Over the past two years, a majority of U.S. states have either enacted or seriously proposed something more like European data privacy law. Federal lawmakers, too, have gotten in on the debate. What sparked this recent renaissance in U.S. privacy law?

The GDPR went into effect in May 2018. In part the GDPR was adopted to update existing European data protection law. In part, it was a reaction to deepening skepticism about U.S.-based companies and their practices. The GDPR made European data protection law *broader*, *stronger*, and *deeper*: it applies to a wider range of activity (broader), establishes stronger enforcement mechanisms (stronger), and includes additional substantive protections (deeper), compared to previous law.

The GDPR, unlike U.S. laws, covers nearly all processing of all kinds of personal data. It is quintessentially omnibus; it attempts to be both technology neutral and comprehensive. It "follows the data" in the sense that personal data receives numerous protections not just at the point when a consumer transacts with a business. That is, you do not waive the GDPR's protections just by agreeing to let a company collect your data. Approximately half of the GDPR affords individuals a series of rights: of access, notification, correction, deletion, and more. The other half tells companies and government agencies what to do.

The GDPR, in short, establishes a data privacy compliance program, like the kind of thing one sees in highly regulated sectors such as banking. For example, many companies have to appoint a Data Protection Officer (DPO), who is responsible for ensuring compliance with the GDPR. Companies conducting "high risk" projects, such as extensive monitoring of public places, must conduct impact assessments and under some circumstances get government approval before proceeding. Companies must keep records about data processing, and build new technologies with data privacy in mind. These and other requirements establish a compliance system that aims to change both companies' infrastructure and the substance of their decisions around data processing.

The GDPR has clearly had a global effect. It intentionally reaches data processing around the world, including companies that target European users on the Internet, or monitor the behavior of Europeans in Europe. The intentionally global reach of the GDPR, coupled with its threat of huge fines, has led companies around the world to adjust their privacy practices—and countries around the world to update their privacy laws.[8]

One theory of what has recently been happening in the U.S., with the startling uptick in proposed state and federal data privacy laws, is that the GDPR has spawned a host of imitators. When California enacted the California Consumer Privacy Act (CCPA) in June 2018, many journalists referred to it as "GDPR-lite." To some extent this is true. Both the CCPA and recent state and federal proposals are fundamentally different from U.S. privacy laws that came before. Like the GDPR, they aim at *all* data processing, not just processing in particular sectors.

Also like the GDPR, many of the U.S. proposals follow the data. The CCPA, for example, famously allows California residents to opt out of the sale of their personal data, even when they have voluntarily given it over to a company. It also allows individuals to make access requests for personal data, providing an unprecedented degree of transparency over private sector data processing in the U.S.

But claiming the CCPA and follow-on state and federal proposals are the consequence of the GDPR is largely inaccurate.[2] The E.U. has long had data protection laws, and the U.S. has long decided to ignore them.

The CCPA was not enacted in response to the GDPR; it was enacted when a real estate billionaire, Alastair Mactaggart, coordinated with other privacy activists to put forward a data privacy law as a California ballot initiative. At the last minute, California's lawmakers begged for a compromise (it is very, very difficult to amend a law passed by ballot initiative), and passed the CCPA in order to get Mactaggart to withdraw his proposal.

The CCPA is also substantively different from the GDPR. First, and importantly, it exists against the backdrop of U.S. law, which prioritizes free speech and does not have constitutional protections for data privacy, unlike Europe, where data protection is enshrined as a human right. The CCPA is still largely an American-style transparency law, one that amplifies the "notice" in "notice and choice." The hope is that true transparency about data practices might lead consumers to behave differently, or lead to public outrage and new laws.

While it echoes a number of individual rights from the GDPR, the CCPA does not create structural requirements for companies. It does not require a data privacy officer, or records of data processing activity, or that companies minimize privacy violations and bake data privacy into the design of their technologies. The CCPA might obliquely trigger some changes in corporate practices, but mostly it relies on individuals to invoke their rights, rather than requiring companies to behave in particular ways.

Other states' proposals largely mimic the CCPA, not the GDPR. Some states just copy and paste it; others have established legislative committees specifically to study the CCPA in action. Other states are pushing forward with yet more sectoral privacy laws, rather than omnibus protections. These new laws address cybersecurity, biometric surveillance, and ISP privacy.

The flurry of state activity (with its risk of a high degree of variation) has driven numerous privacy law proposals in Congress. There seems to be bipartisan agreement that there should be new federal privacy law. There is substantial disagreement, however, about whether that law should preempt (override) state laws, whether it should allow people to sue on their own behalf versus rely on government enforcement, and of course what should actually be in it.

The story of U.S. privacy law is not yet at happily ever after. It is, however, meaningfully improving.

The story of U.S. privacy law is not yet at happily ever after. It is, however, meaningfully improving. Major hurdles still remain, including significant First Amendment challenges (do privacy laws violate rights to free speech?). But in a very short time period, compared with the usually glacial pace of legal change, the paradigm has shifted. Data privacy law is no longer a matter of whether, but what and when. C

References

1. Bamberger, K.A. and Mulligan, D. Privacy on the books and on the ground. *63 Stan. L. Rev. 247* (2010).
2. Chander, A., Kaminski, M.E., and McGeveran, W. Catalyzing privacy law. *105 Minn. L. Rev.* (forthcoming 2020).
3. Citron, D. Mainstreaming privacy torts. *98 California Law Review 1805* (2010).
4. Hartzog, W. and Rubinstein, I. The anonymization debate should be about risk, not perfection. *Commun. ACM 60*, 5 (May 2017), 22–24; DOI: 10.1145/3068787
5. Joh, E. Increasing automation in policing. *Commun. ACM 63*, 1 (Jan. 2020), 20–22; 10.1145/3372912
6. McGeveran, W. Friending the privacy regulators. *58 Ariz. L. Rev. 960* (2016).
7. Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford Law Books, First edition, 2009.
8. Schwartz, P.M. Global data privacy: The EU way. *NYU L. Rev. 771* (2019), 94.
9. Solove, D.J. and Hartzog, W. The FTC and the new common law of privacy. *Colum. L. Rev. 583* (2011), 114.

Margot Kaminski (margot.kaminski@colorado.edu) is Associate Professor at the University of Colorado Law and the Director of the Privacy Initiative at Silicon Flatirons, Boulder, CO, USA.