2023

Toward Stronger Data Protection Laws

Margot E. Kaminski
University of Colorado Law School

Citation Information

Margot Kaminski, *Toward Stronger Data Protection Laws*, 68 Democracy: A Journal of Ideas (2023), https://democracyjournal.org/magazine/68/toward-stronger-data-protection-laws/

DEMOCRACY

SYMPOSIUM | DEMOCRACY AND TECHNOLOGY: ALLIES OR ENEMIES?

Toward Stronger Data Protection Laws

BY MARGOT KAMINSKI FROM SPRING, NO. 68 – 10 MIN READ

TAGGED DEMOCRACY INTERNET TECHNOLOGY

If there is one thing we have learned from around 30 years of the U.S.-style wait-and-see approach to data privacy, it's that companies that aren't regulated will behave badly. From lax security and massive data breaches to data-driven consumer manipulation to discriminatory profiling, to surreptitious location-tracking, examples

abound. But the tide has been shifting, especially at the state level. We are now inching, however cautiously, toward American data protection law.

What does it mean to talk about data protection, as opposed to privacy? In Europe, which largely leads the world on data protection law, the two concepts are separate but related. Privacy refers to unwanted information flows, typically of highly sensitive personal information or information gathered from a protected location, or in a particularly intrusive way. This includes gathering such information intrusively, or sending it to an unintended audience, often via one-to-many media like a newspaper, television, or the internet. Nonconsensual pornography, for example—the sharing of a graphic sexual image without consent—constitutes a modern-day example of a fairly classic violation of privacy.

Data protection is, by contrast, often about what can appear to be innocuous information, like what groceries you buy or how long you spend on a particular website. Data protection aims to establish the rules of the road for processing and using personal information that has typically already been shared, often voluntarily. Like privacy, data protection is ultimately about power: the power of the entity that holds the information to manipulate, coerce, influence, or just change the life outcomes of an affected individual. Unlike privacy, data protection is also centrally concerned with fairness: the procedural rights of an affected individual, including a right to know that data has been gathered and processed and a right to challenge inaccurate data, among other things. The core principles of data protection—the Fair Information Practice Principles—emerged close to simultaneously in the United States and the UK, over concerns about what to do about increasingly large databases of personal information held by both the government and private actors, and used across increasingly broad contexts. In the United States, these principles, which emerged in a government agency report, came to form the backbone of a number of narrower U.S. privacy laws protecting things like health information and children's information, but never evolved into a general catch-all data protection law—until, potentially, now.

If the paradigmatic privacy problem is having a piece of private information published for all to see, the paradigmatic data protection problem is having one's information collated from across many sources into a so-called "digital dossier." As early as the 1970s, people recognized the power such a dossier could have in

determining one's life choices, and the due-process-like concerns that arise when one can neither see the data nor challenge its accuracy or use.

Initially, starting in the mid-1970s, America was all for data protection. We passed a number of sectoral laws and one general government law (the Privacy Act) built on data protection principles. And then by 2000 we stalled. In the name of permissionless innovation, our lawmakers underplayed the by-then known harms of unfettered data collection and aggregation. The Supreme Court downplayed data privacy harms that could not readily be measured. Personal data was widely characterized as both the currency of the free internet and valueless to the people from whom it was extracted.

In the United States, data protection principles were watered down to the infamous "notice and choice." This occurred both as lawmakers failed to enact new, broader data protection law, and as the Federal Trade Commission began enforcing data privacy under its authority to regulate against unfair and deceptive practices. Characterized as emphasizing individual liberty, "notice and choice" in fact stripped individuals of meaningful autonomy by requiring neither particularly effective notice nor particularly meaningful choice. As every internet user knows, websites (and now apps) are full of consent streams that don't involve real consent: the contractual terms embedded in small print on the bottom of a webpage, the terms of service boxes you check for every company with which you interact. Making the use of basic online resources contingent on data sharing and then characterizing that sharing as meaningful consent marked an almost willful blindness to the principles of data protection. Rather than triggering a set of legal protections, sharing personal information was found in many areas of U.S. law to waive privacy protection entirely.

So what changed? Or really, what is still changing? The scope of platform-related harms, the potential and real impact of surveillance and personalized manipulation on our democracy, the ways in which data-driven decision-making increasingly impacts people's lives and even restricts their choices, the realization that Europe put in place tougher laws and the internet didn't break, the fact that many of our largest companies are already in compliance now with European data protection law and would love to impose the same costs on their competitors—all of these things and more have been driving a wave of state-by-state privacy legislation, and the closest bipartisan push for federal data protection-style law that we have seen in decades. Perhaps, too, data

protection principles now resonate even across our country's deepening political divides: from the worker fearing repercussions for her political views in the workplace to the woman seeking an abortion and fearing prosecution and harassment across state lines.

Despite the impasse at the federal level, data protection law has begun to emerge at the state level. Its success will hinge on how much it empowers individuals while also including effective governance, how well it is backed by enforcement, and the extent to which it is coupled with other backstops, including more traditional privacy law.

When California first passed its consumer data privacy law, the California Consumer Privacy Act (CCPA), a few years back, many termed it "the American GDPR." The GDPR, or General Data Protection Regulation, is the massive data protection law in the European Union. California's initial law, to be clear, in many ways had similar bones to the GDPR: an expansive definition of "personal data," a similar set of foundational individual rights, and a focus on using transparency to reveal data practices and restore some power to individuals in the face of gaping power imbalances.

But there were also glaring differences. Europe has a constitutional right to both privacy and data protection, and a human rights court eager to enforce those rights. It has, whatever their weaknesses, longstanding data protection regulators, who are experts in this area of law and whose task is to focus on it. California, by contrast, put data protection in the hands of its busy attorney general. It gave individuals only a limited right to sue, in the context of data security breaches. And strikingly, the first version of California's law lacked the second half of the GDPR: the part that focused primarily on corporate governance and obligations that companies must follow even if individuals never exercise their rights. Instead, the CCPA's focus was on transparency, coupled with a right to opt out of the sale of one's data.

At first it appeared that a number of states were poised to mimic California. State legislators around the country proposed laws that directly cut-and-pasted language from the CCPA. Like California's initial law, those proposals emphasized individual

transparency and rights, with less if any emphasis on corporate obligations. Then, however, a counter-model emerged out of Washington state.

Never passed in its home state, and by many accounts heavily influenced by Microsoft lobbyists, the Washington version of data protection more clearly resembled a mini-GDPR. It might be counterintuitive that a large company would support any data privacy regulation; in fact, large companies that are already forced to absorb the compliance costs of the GDPR can be eager to impose the same costs on smaller competitors, especially when they come out looking like good actors in the process. The Washington bill included duties for data controllers (entities that process personal data), going beyond transparency and restrictions on sale to include, among other things, a duty under some circumstances to conduct impact assessments and mitigate data privacy risks.

On the one hand, this version of American data protection law more closely tracked European law and other data protection laws around the world. On the other, consumer protection and civil liberties advocates feared that boiling down Europe's 90-page regulation to a 20-page version with somewhat cagey standards would retain the trappings of data protection law without its teeth. At the same time, academics rightfully skeptical of the American emphasis on individual autonomy instantiated in "notice and choice" feared that the individual rights in both the Washington and California laws wouldn't get used in practice.

Where does this leave us now? Hopefully, in a place of cautious optimism. The Washington bill did not come to pass—in Washington state. It did, however, become the scaffolding on which a number of other states began enacting their own data protection laws. Some states, like Utah, arguably watered the bill down further. Others, like Colorado, added some interesting elements to it, including a prohibition on using manipulation to obtain consent. One of the most important things Colorado did was enable the state attorney general to promulgate rules to further explicate, and perhaps strengthen, the vaguer terms of the act. That rule-making is ongoing as of early 2023.

Meanwhile, California went to the ballot and enacted, by initiative, another layer of law on top of the CCPA: the California Privacy Rights Act, or CPRA. Substantively, the CPRA afforded more rights to California residents, including the right to opt out not just of

sale but of sharing sensitive information. It, too, established risk assessments. It also established a rule that California legislators cannot pass less privacy-protective law going forward. And it created a new specialist enforcement agency, gave that agency rule-making authority, and kicked off another round of rules.

Some real good is thus arising from this reemerging American experiment with data protection law. Affording individuals consistent data protection rights, including clear rights to opt out of the more harmful types of data processing and sale, is a good thing. The fact that these laws now also include some obligations for companies is good, too, although the devil will be in the details: how real the obligations are, and how attentive enforcers will be. It is encouraging to see a shift from aggregating without permission toward minimizing data collection—an acknowledgment that companies must be more thoughtful, and that all-of-the-data-all-of-the-time is not an acceptable approach going forward. The experimentation with enforcement and regulation is promising, too, with Colorado's attorney general's office deepening its expertise in privacy, while California develops a new specialized agency.

Moreover, the much-feared fifty-laws-for-fifty-states problem has not developed in any significant way, as states have paid attention to the cost of significant legal divergences for companies, both as they enact their laws and as they promulgate their regulations. There are certainly states that appear not to be interested in enacting data protection law at all, leaving gaps in protection for their residents. There are also states that appear to be interested in enacting laws only as a bare symbolic minimum.

Yet I remain optimistic. If not a race to the top, it's a careful relay right now—largely between California and Colorado regulators—toward a higher degree of data protection in the United States than we could have imagined even ten years ago. Couple that with the fact that many companies will de facto be following California's law, which can only ever be amended upward, and the new era of American data protection can be said to have truly begun.

There is a lot to love about the American Data Privacy and Protection Act, the federal bill that nearly made it last year. But for the act to have passed, Congress would have had to agree to preempt state data privacy laws, which Nancy Pelosi, listening to constituents in California, refused to do. A part of me similarly wants not to preempt the

ensuing muddle, to wait and see what happens next at the state level, as regulations are passed and enforcement begins in earnest. It hasn't disappointed thus far.

FROM THE SYMPOSIUM

Democracy and Technology: Allies or Enemies?

SEE ALL

READ MORE ABOUT DEMOCRACY INTERNET TECHNOLOGY

MARGOT KAMINSKI is Associate Professor of Law at Colorado Law School, where she teaches, researches, and writes on law and new technology, with a focus on data privacy law. She is a graduate of Harvard University and Yale Law School, and the recipient of a 2018 Fulbright-Schuman Innovation Award that enabled her to research data protection law in Europe.

ALSO ON **DEMOCRACY**

The Death of "Deliverism"
a month ago · 1 comment
Economic policy success isn't enough. We need a more holistic approach to ...

The New Libertarian Elitists
4 months ago · 5 comments
What's behind the dangerous new notion that democracy should be left ...

Lessons for the Next Resistance
7 months ago · 3 comments
Veterans of the EPA knew it would face unprecedented attacks under Donald ...

Elevatin Democr
10 months
I was bor of age be in the mo