10 Areas Of Privacy Law That Look Ripe For Change In 2021

Law360, New York (January 3, 2021, 12:02 PM EST) –

Kirk Nahra

While still in its relative infancy, privacy law has quickly become a turbulent teenager, with constant change around the world.

At a minimum, 2021 will require meaningful efforts to implement the changes of 2020, with a reasonable likelihood of even more substantial change.

What are the major issues to be watching in 2021?

1. California

Jan. 1, 2020, brought the beginning of the formal era of the California Consumer Privacy Act, or CCPA.

Because enforcement could not begin until July 1, companies faced a reasonable implementation period, to develop policies that addressed the certainly complicated and most likely confusing and awkward provisions of the hastily drafted law.

Draft regulations were issued — and issued again — and then finalized, only to be revised again. The California Legislature, meanwhile, further amended the law.

Then came the California Privacy Rights Act, or CPRA, referendum passing in November.

Chaos is probably too strong a word — more on that later. Implementation and compliance challenges are real and continue, even for companies trying hard to do the right thing.

Consumer attitudes have been mixed. The law is poorly written in many places, regardless of your view on the substance. Some of the CCPA makes little sense as it applies to certain kinds of business practices.

And now we will await not only the new substantive provisions of the CPRA but also the creation of a new enforcement entity to replace the California attorney general.

Will there be meaningful enforcement?

Will the plaintiffs bar be able to use its creative energy to expand the reach of the private cause of action?

Will the California Legislature reach a lasting solution on the employee and B2B exemptions in both the CCPA and CPRA that will expire on Jan. 1, 2023?

How long will we have to wait for CPRA regulations now that we finally have some clarity on the CCPA?

2. Other States

Since the CCPA's passage, those of us in the privacy bar have expected other states to follow suit. So far, they haven't.

Apparently, its hard to pass a broad privacy law without the gun to the head of an aggressive referendum. Not too many states have really even tried at this point.

We expect Washington state to revive its efforts in 2021. New York looks poised to try again as well, this time with the It's Your Data Act, which was proposed in October.

I would expect several more states also get moving in 2021, although we don't really know which states. It's going to be hard — and, even more important, any laws that result are not likely to look much like California.

Will the first state after California set the model?

That's a key issue to watch. If not, we may see states going off in different directions. What seems to be easier, and where I would expect activity in 2021, is on narrower laws targeted at specific practices or data — like additional laws targeting facial recognition or biometrics.

3. A National Privacy Law

And then there's the chance of a national privacy law. This effort began in earnest in 2018, and continued for about two years with the full Washington experience — white papers, briefing statements, stakeholder press conferences, congressional hearings, and draft legislation. Some progress, but not much.

Then COVID-19 hit — and all legislative efforts on a privacy law stopped, other than the possibility (not yet fulfilled) of a pandemic privacy law focused on contact tracing.

It is safe to say that this effort will begin again in 2021. Both parties in the U.S. Senate are trying to develop full scale bills.

The U.S. House of Representatives has been a little quieter, but some meaningful efforts are underway. There are large scale overall bills, and narrower bills focused on things like giving the Federal Trade Commission more authority.

It is clear that the two big issues where there is yet no consensus involve (1) preemption of state law and (2) creation of a private cause of action.

The real meat of a privacy law is very much up in the air — what the relevant use and disclosure principles will be, what individual rights will be created, who the enforcement agency will be, what will happen with the other federal laws, and whether the law will take on discrimination issues related to artificial intelligence and big data.

2021 is likely to be a year of modest but important progress.

The Biden administration presumably will be supportive, but will have a lot of other things to be doing.

A wild card involves Vice President Kamala Harris — who made her reputation at least in part through actions on privacy when she was the California attorney general.

My bet is that there's a good chance of a law, before the end of the first term of a Biden administration. The timing wild card involves the states — if three to five meaningful states pass their own laws, corporate America will need to get behind a reasonable consensus bill as it will be extremely challenging to meet the standards of multiple states.

4. Schrems II and the Data Transfer Mess

Chaos is a reasonable word to describe the current situation involving data transfer out of Europe. The decision in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, or Schrems II, from the European Court of Justice threw out the EU-U.S. Privacy Shield program.

There's no clear movement toward a replacement program — although we can at least expect reasonable negotiations with Europe under a Biden administration.

The alternative option — the standard contractual clauses — is now clearly on its last legs, as various signals from EU authorities are creating impossible to meet standards for appropriate implementation of the standard contractual clauses.

There is a real possibility of a vast data island in Europe — and meaningful attention needs to be addressed to the question of whether this is in fact good for either European citizens or businesses, I think it's a lose-lose at this point.

There's clearly some disconnect between the European courts and the data regulators but no clear path toward a resolution of these differences.

It does not seem likely that the U.S. will give up its surveillance options. But we may see increasing attention toward the potential hypocrisy of European authorities that both rely on this same kind of surveillance authority and engage in very similar efforts themselves.

For now, companies need to figure out a way to tread water provide reasonable protections, stay out of the limelight and be reasonable in dealings with vendors and data partners.

5. The Rest of the World

While Europe creates its own problems, the rest of the world is continuing to make privacy law a global phenomenon.

We saw a new Brazilian law in 2020.

Brexit's fallout will continue — and perhaps be resolved in 2021, although the U.K. may face American problems on data transfer issues if the U.K. standards are not found to be adequate.

India, China and Canada are pursuing expansive new laws.

There is some slight movement toward a global standard similar to General Data Protection Regulation, but there are enough differences in different places that a true global approach is not near.

6. FTC/Data Security and the FTC in General

Part of Europe's concern with U.S. privacy protections involves the role of the FTC. Typically viewed as the primary privacy regulator at the national level, the FTC is relying primarily on a more than 100-year-old statute that obviously intended nothing specific about privacy or security.

The FTC — through the magic of unimpeded enforcement – has created an extensive body of law related to appropriate data security protections. That unimpeded effort will not be feasible in the privacy area.

Privacy lawyers have read both the U.S. Court of Appeals for the Third Circuit's 2015 decision in FTC v. Wyndham and the U.S. Court of Appeals for the Eleventh Circuit's 2019 decision in LabMD v. FTC, and know the courts skepticism about the FTC's actions.

Those uncontested settlements likely won't be easy to come by on privacy issues. So, many of the national proposals are directed in large part to giving the FTC more specific authority in the privacy and security areas, including both the ability to draft regulations and the ability to impose fines in the first instance (remember that the record shattering Facebook fine was due to a prior settlement).

Recent statements by two of the FTC commissioners have encouraged a more aggressive path, including more substantial settlement terms, additional attention to privacy protections and even litigation where necessary. Under a Biden administration, these dissenters likely will become the majority.

At the same time, the FTC is pursuing a rulemaking proceeding under the Gramm-Leach-Bliley Act that may blow up existing data security law.

The original GLB Safeguards rule created the overall approach to a "reasonable and appropriate" data security program, and became the model for the FTC's approach outside of financial institutions regulated by GLB.

It is now pursuing a more explicit set of security requirements for GLB. If that approach is enacted and followed in other areas, that could create a monumental change to how companies must develop and implement their data security programs.

7. Attorney General Enforcement

The FTC also has a strong competitor to the title of primary privacy regulator. The state attorneys general are taking significantly more aggressive action involving privacy and data security claims.

These cases can be individual, in small or large groups of states, or in a handful of 50-state cases.

They are taking follow-on enforcement action after other agencies have acted, focusing on particular practices of concern that typically have some kind of consumer harm, and are at times creating new bodies of law to fill in current gaps.

Both the New York attorney general's efforts at filling the gaps of the Health Insurance Portability and Accountability Act and the California attorney general's effort to impose new standards for apps from the September Glow Inc. settlement are examples of both aggressive enforcement and use of enforcement to impose new standards.

The attorneys general are using their authority on consumer protection to build new bodies of law — in potentially retroactive ways.

Keep watching them in 2021, in a wide variety of settings. Companies need to be thinking about reactions in developing privacy practices, even if there is no obvious law that is being violated.

Privacy lawyers are going to need to pay closer attention to the creepiness factor that arises in data collection activities, as an additional element of legal advice beyond just reading the rules.

8. New Administration Priorities

In addition to these state level issues, we can expect somewhat more aggressive enforcement overall at the federal level due to the incoming administration. Privacy issues have not occupied a lot of campaign attention. In addition, the relevant enforcement agencies often are somewhat limited in their ability to take aggressive enforcement action.

Similarly, even under an Obama administration, privacy and security enforcement was reasonable and limited, as regulators took appropriate action to address both reasonable compliance activities (particularly on data security, where perfection is not expected) as well as more problematic actions.

Some agencies will bring in significantly different personnel. At the same time, it is important to recognize that different priorities do not necessarily mean more enforcement. The U.S. Department of Health and Human Services' Office for Civil Rights, for example, has undertaken careful, thoughtful enforcement throughout its tenure under different administrations.

Where companies have been trying to do the right thing, OCR does not tend to take action even if something goes wrong. My colleagues in the privacy bar may criticize me for saying this, but we have seen the same kinds of actions from the FTC — they work hard at their cases and take action on enforcement when a company is really out of line with appropriate behavior.

We will be watching the new administration in its enforcement, in its consideration and encouragement of a national law and for its thoughtful activity on issues like big data discrimination — where careful attention to developing the right approach likely is more important that just passing something.

9. Private Cause of Action/Ongoing Litigation

The role of the plaintiffs bar in the privacy and security debate remains a critical element of any discussion of future law. Today, we are seeing increased litigation, motivated by three things:

1. Security breaches — of virtually any kind, with little consideration of fault or reasonable security practices.

2. Cases filed under state or federal laws with specific statutory damage provisions — mainly the Telephone Consumer Protection Act, the Biometric Privacy Act and now the CCPA.

3. Various policy-oriented cases driven by potentially problematic privacy or data practices.

This isn't only a U.S. issue. In the U.K. under GDPR and the Data Protection Act, there has been a recent rise in the U.K.'s form of class action litigation, where the courts have been more supportive of individual consumer claims.

Many of these cases have faced an uphill battle, particularly the data breach cases. Courts have been careful and thoughtful. The plaintiffs bar has been creative and aggressive.

As more laws are passed, and as more cases are brought, we will need to pay careful attention to whether there is a true breakthrough case that opens the floodgates for litigation. If that case happens soon, it may impact the debate in a national

law about both preemption and a private cause of action (remember the fallout from the Fair and Accurate Credit Transactions Act cases involving truncated credit card numbers).

10. Ransomware/Security Attacks

While legislative attention has been focused on privacy issues, data security continues to be a growing and actual problem on a regular basis, across industries.

Certain industries have been targeted — in some settings there was significant attention for the government to credible threats of ransomware attacks directed at the hospital industry.

Hackers have been getting more aggressive and more organized. Companies need to be paying substantial attention to these risks — through better monitoring, improved training, appropriate and aggressive incident — response and meaningful prebreach planning. For example, the recent volume of ransomware attacks has placed renewed attention on the need for data recovery and appropriate back-up systems.

Data security risks are real and can have a major impact on companies in real time – independent of subsequent litigation and/or litigation activity. Careful thoughtful planning is necessary now, to protect data and company systems.

Conclusion

Privacy law is becoming more complicated every year. There are real questions about whether the current state of U.S. law in particular is good for either consumers or businesses — with the increasing likelihood of a lose-lose situation.

Consumers cannot possibly understand the law, and companies are facing increasing complexity and burdensome detail just simply to understand and apply the law.

It's a great time to be a privacy lawyer, but we may be the only people benefiting from the current state of the law.

—By Kirk Nahra, WilmerHale

Kirk J. Nahra is a partner in WilmerHale's Washington DC office who specializes in Cybersecurity and Privacy