PRIVACY & CYBERSECURITY

TARGETED DATA PRIVACY LAWS INCREASE RISK

Data privacy has been a growing source of class action litigation for some time—and now, an emerging breed of state laws is opening the door to new areas of risk.

"A number of states have enacted data privacy legislation designed to protect not just personal data in general, but very specific types of personal data, such as biometric and genetic information," says Gabriel Ramsey, a partner in Crowell & Moring's Litigation, Intellectual Property, and Privacy & Cybersecurity groups. This trend really began with the passage of the Illinois Biometric Information Protection Act in 2008, which covers information about biometric identifiers such as fingerprints, retina or iris scans, voiceprints, and hand or facial scans. Other states, such as Washington and Texas, have passed comparable biometric data laws.

In a similar vein, Alaska, Oregon, Illinois, and other states now have laws protecting genetic information—which could have ramifications not only for firms that offer DNA analyses to consumers, but also for hospitals and research centers that keep that type of information. And it appears likely that more states will adopt such legislation, if for no other reason than political expediency, because data privacy continues to be a major concern for the public.

"This growing patchwork of laws obviously affects traditional and start-up tech companies that are involved with biometric technology," says Ramsey. But the use of biometric data is becoming more widespread, and the technology is found in a growing range of products and services across industries.

"Many types of companies are at risk from niche state laws because many use these types of data in their businesses," says Ramsey. For example, a wide variety of brick-and-mortar companies have been sued over their use of fingerprint-enabled time-and-attendance systems, including an ambulance company, a convenience store chain, a janitorial services firm, and an auto repair company. But beyond these traditional contexts, biometric data is increasingly used in a wide array of disruptive digital technologies used in entertainment, health and fitness applications, financial services, and targeted user-specific applications. "Sometimes the technology is being used in middleware that is baked into other products—things like smartphone apps—where their use is fairly invisible to consumers," says Ramsey. "As the technology develops and expands, more and more companies will have to think about this."

GROWING BIPA LITIGATION

The Illinois biometric legislation remains the most prominent and strongest of these targeted privacy laws. BIPA says that companies collecting and storing biometric data need to inform individuals that they are doing so and get written consent for keeping their data. It also prohibits companies from selling or disclosing that data in most situations, unless the individual agrees. Notably, it provides a right of action to individuals, along with significant penalties of $1,000 per negligent violation and $5,000 for intentional or reckless violations. It also allows plaintiffs to recover attorneys' fees and costs.

For several years after the act was passed, courts saw little litigation around BIPA. But over the past two years, plaintiffs have filed dozens of BIPA lawsuits, a trend presumably driven by both the growing use of biometric technology in business and the potential for significant damages. As these cases move through the courts, the issue of standing has emerged as a key point of contention. "The question is basically whether violating the statute constitutes enough harm to create an injured class and confer standing, or whether standing requires that there be actual injury or damage," says Ramsey.

The courts have been divided on this issue. In *McCollough v. Smarte Carte, Inc.*, for example, a company used scanned fingerprints to enable people to open storage lockers. Plaintiffs

"Many types of companies are at risk from niche state laws because many use [biometric] data in their businesses."

—*Gabriel Ramsey*

sued, saying their biometric information had been collected without their consent. However, in 2016, the Northern District of Illinois found that there was no concrete injury and therefore no standing. In 2017, in *Vigil v. Take-Two Interactive Software, Inc.*, plaintiffs alleged that they had not received notice that their facial scans, used to create online video game avatars, would be stored. In this case, the Southern District of New York also found that there was not sufficient actual injury to confer standing.

DIFFERING OPINIONS

Other courts have differed. In *Monroy v. Shutterfly, Inc.*, plaintiffs said that Shutterfly, which allows users to upload photos to a website, was automatically extracting biometric information from these photos—including information about photo subjects who were not even users of Shutterfly. In 2017, the Northern District of Illinois said that this was enough to confer standing, even for non-Shutterfly users. Later, in *Patel v. Facebook, Inc.*—a suit involving Facebook's "tagging" feature for marking photographs—plaintiffs argued that the company was collecting and storing their biometric information without giving users notice or getting their consent. In 2018, the Northern District of California ruled that the mere allegation of a failure to comply with BIPA's requirements in those areas constituted a sufficiently pled invasion of privacy and a sufficiently pled injury for standing.

"These types of cases are important to watch as they make their way to the higher appeals courts and some sort of consensus starts to emerge," says Ramsey. "The litigation is still testing the waters, and if a few of these cases get traction, the damages could theoretically amount to billions of dollars. That could start to create a feedback cycle that would only encourage more lawsuits." Such developments could have a similar effect on state legislators, prompting the passage of new biometric and genetic data privacy laws in more states, or laws that focus on new types of specialized data—"perhaps something like a law specifically governing location-based data or other data that consumers or legislators perceive as particularly sensitive," Ramsey says. This in turn could further bolster the enforcement authority of state attorneys general. Such developments would compound the complexity of the existing patchwork of state privacy laws.

In this environment, companies need to make sure that they clearly understand how they are using biometric information and other types of specialized data—and have processes in place to ensure compliance with rules about gaining consent and using and safeguarding that data. More broadly, they should work to close any gaps that may exist between legal departments and product-development groups. "That's a long-standing issue; risk management in this kind of technology-related area is really about getting your legal team culturally integrated with your engineering team," says Ramsey. "Risk often flows from a disconnect between the fast-moving groups implementing products and the more deliberate legal function. When the lawyers are not part of the team, a technology product can easily end up bringing legal complications. So you have to figure out how to build trust between the legal and technical teams and integrate compliance into the design-build process from the very beginning."

FROM THE EU TO THE U.S.

On May 25, 2018, the EU's General Data Protection Regulation took effect, providing a rigorous set of rules designed to give individuals more control over how their personal data is used. In less than an hour, an EU form of a class action suit was filed under the regulation, to be followed by many others. "There has been aggressive litigation leveraging GDPR's requirements," says Crowell & Moring's Gabriel Ramsey. "European collective and group actions against major technology companies have accelerated dramatically."

Historically, class action suits have not been allowed in many EU countries. But the GDPR gives individuals the right of private action and allows them to assign their claims to nonprofit organizations to litigate on their behalf. A number of GDPR class action cases have been filed by privacy activist groups on behalf of plaintiffs. "These new litigation paths pose considerable uncertainty, given that they are untested and the law is just developing. And the GDPR poses substantial penalties and gives plaintiffs the right to seek monetary compensation," says Ramsey. "These features create a new risk of frivolous profit-motivated lawsuits in Europe that we will see play out in the coming years."

Last June, not long after the EU regulation was in place, the California Consumer Privacy Act took effect. It differs from the GDPR in some ways, but like the GDPR, it represents a stricter approach to protecting data privacy and gives people the right to access their data and the right "to be forgotten" and have their data deleted. Many observers expect other states to follow. As that happens, the GDPR could provide a model for understanding the future of the U.S. litigation landscape. Says Ramsey, "Watching the broad trends as GDPR-related litigation unfolds in Europe might provide insight into how litigation under the California statute and other similar statutes will evolve."