Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Cybersecurity Policy To Watch For The Rest Of 2017

By **Allison Grande**

*Law360, New York (July 12, 2017, 7:47 PM EDT)* -- As uncertainty persists about federal strategies for data protection enforcement and government rulemaking has nearly ground to a halt, state lawmakers and regulators, by contrast, have taken decisive recent steps in the sphere of cybersecurity and online privacy, experts say.

In several notable actions, a coalition of state attorneys general secured a record $18.5 million settlement with Target Corp. over the retailer's 2013 data breach; the New York Department of Financial Services instituted stringent cybersecurity rules; and several states moved to enact broadband privacy rules that would replace those struck down by the Federal Communications Commission. Experts say they see no signs the activity will slow down during the second half of 2017.

"These recent actions show that states are taking the reins on some of the issues related to cyber regulation rather than wait for action at the federal level," said Erik Rasmussen, North American practice leader of Kroll's cybersecurity and investigations group.

Here, cybersecurity policy watchers forecast what they expect to be the hottest topics in the U.S. and abroad for the rest of 2017.

**States' Moves on Cybersecurity Issues**

On legislation and enforcement fronts, privacy attorneys anticipate that state houses around the country will become new centers of action for cybersecurity law making and enforcement.

"I expect that state AGs — at least in some prominent states — will increase their activity," said Kirk Nahra, privacy chair for Wiley Rein LLP. "I also expect state legislatures to fill in some gaps created by an administration and Congress that aren't likely to do much on privacy and security generally."

New York is a state to watch carefully, experts say. The state moved earlier this year to enact first-of-their-kind cybersecurity rules that require banks, insurers and other institutions to develop detailed data security programs and report breaches within 72 hours. Businesses must fully comply with most requirements of the rule by Aug. 28.

"One of the biggest things I'm keeping my eye on is when is the first enforcement action going to come under the new Department of Financial Services' cybersecurity regulations," said Jim Pastore, partner

with Debevoise & Plimpton LLP.

Other states are likely to follow New York's approach in enacting industry-specific cybersecurity regulations, lawyers say, with Peter S. Vogel, co-chair of cybersecurity and privacy legal services at Gardere Wynne Sewell LLP, saying it wouldn't surprise him if "more states put the burden of responsibility on companies to avoid disasters if there's a cyber intrusion."

New York again is forecast to be in the lead as attorneys general around the country are expected to pursue new data security enforcement initiatives. After participating in the Target breach settlement, New York AG Eric Schneiderman last month pursued a health provider for failing to give timely notice of a data breach. He also led the charge in warning an e-commerce hosting company that allegedly advised online retailers against notifying certain customers of a massive data breach.

"State attorneys general have always been very active in protecting consumers' needs, and given that you can't go a day without reading about a data breach, states will likely be very committed to these issues in response to constituents who are looking for the government to do something about this problem," Rasmussen said.

On the legislative front, Foley Hoag LLP counsel Christopher Hart said he'll be interested to see if states continue amending the patchwork of breach notification laws that are in effect in every state except Alabama and South Dakota. State lawmakers have moved to update those statutes in recent years to broaden types of data considered to be personal information and clarify the triggers for notification, he said.

Reece Hirsch, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP, predicted that states may also be motivated to tweak their laws in light of recent global ransomware attacks that have hit businesses ranging from DLA Piper to FedEx in order to make the reporting requirements more explicit for when companies are blocked from accessing their data.

Other attorneys pointed to states' increased interest in the regulation of biometric data and the expanding world of internet-connected devices. Al Saikali, data security and privacy group chair with Shook Hardy & Bacon LLP, said privacy laws under consideration in Connecticut, Alaska and New Hampshire could create new challenges for companies that collect, use, share and store biometric information about users of their products.

A California senator earlier in the year introduced a bill to mandate that connected devices sold in the state be equipped with "reasonable" security features and clearly disclose what information is being collected and how it will be used. That bill was pulled from consideration in June when it appeared to lack the votes to pass, but it still could make a comeback.

"The internet of things just seems to be getting bigger all the time, and for things like who's going to own the data and what kind of privacy and security policies you have to have in place, it's still a little like the Wild West," Haynes and Boone LLP partner Gavin George said. "There's not good law or a regulatory regime built up around those issues yet, but it may be coming in the next six months or year."

Hirsch noted that a bill like the one passed in California could end up becoming a "de facto national standard" for all connected device manufacturers and that he would anticipate states like California to take the lead on regulating these issues, as well as similar tech innovations such as the rise of mobile health apps.

A number of states have introduced legislation this year that would require internet and app companies to be more upfront about their data collection and disclosure policies, according to Edelson PC partner Ari Scharg.

"What's fascinating about this, at least to me, is to see who is supporting and opposing these bills," he said, noting that both consumer groups and small to midsize internet and app companies have spoken out in favor of the proposals.

"The thinking is that when presented with two identical apps — one that collects and sells personal data and one that does not — users will choose the one that does not every time," Scharg added. "Though transparency measures have been proposed in the past, the outcome might be different now that a growing number of tech companies are pushing for them."

**Feds Could Be Wildcards**

With the Trump administration pushing deregulation, attorneys aren't expecting much action on privacy and cybersecurity at the federal level. But that doesn't mean they won't be paying attention.

"I'm watching whether the administration will change in significant ways the enforcement approach on various privacy laws," said Kirk Nahra, Wiley Rein privacy practice chair. While these changes may not be explicit, "there easily could be less enforcement as a result of budget and staff cuts," he said.

The Federal Trade Commission will be one of the most closely watched agencies. Acting Chairman Maureen Ohlhausen has repeatedly stressed that she favors "regulatory humility," and she has directed her staff to focus on actual privacy and data security harms, not speculative ones.

"There's a sense that the FTC is going to step back from its traditional role as the top cop on cybersecurity and data privacy issues with state regulators potentially becoming more active," Pastore said.

Less enforcement by the FTC could leave an opening for other regulators that steadily have been expanding their presence in privacy matters, including the FCC, U.S. Department of Health and Human Services' Office for Civil Rights and the U.S. Securities and Exchange Commission.

An SEC official said in April that a formal enforcement action against a public company for failing to report cyber incidents and risks could be on the horizon, and Mark Krotoski, a partner at Morgan Lewis, pointed out that the SEC's new co-directors of enforcement recently flagged cybercrime as the biggest market threat and a top priority for the commission, indicating that "we will likely be seeing more focus from the SEC in the coming months."

Though the focus in Congress on issues such as health care and tax reform could stymie any movement on privacy or data security initiatives, attorneys say there is one possible law that may see action: the Electronic Communications Privacy Act of 1986. New legislation may require warrants for all email content and to clarify whether law enforcement is allowed to reach overseas to obtain such information.

Lawmakers already have held hearings this term with witnesses such as Google Inc. and Microsoft Inc. to explore the issue of law enforcement access to data stored abroad, an indication that there may be momentum and broad support to act on this topic, attorneys say.

"Almost every judge who has looked at this issue says this requires congressional action," Krotoski said. "The question now is whether there will be a narrow fix to address the issue raised by the Second Circuit's ruling that the government couldn't access data stored overseas by Microsoft or if lawmakers will undertake a more comprehensive reform, which would have significant ramifications not only domestically but globally as well."

**Europe's Sweeping Data Protection Reform**

Outside the U.S., multinationals are looking ahead to a very important date: May 25. That's the effective date of the General Data Protection Regulation, which was approved by EU policymakers in 2016 as a more stringent and uniform regime.

Kristin Ann Shepard, a shareholder with Carlton Fields, said the GDPR “extends to U.S. companies processing the personal information of EU residents and imposes strict penalties for noncompliance.”

Attorneys say companies will want to use the rest of 2017 to get up into step with the sweeping requirements of the regulation, which include installing a data protection officer, providing consumers with greater access to and control over their data, and reporting breaches within 72 hours.

"We have been coping with cyberattacks and resulting breach notification in the U.S. for 14 years," said Lisa Sotto, head of Hunton & Williams LLP's privacy and data security practice. "The EU will soon fall in line — and the data protection authorities undoubtedly will find themselves drowning in a sea of breach notifications."

The consequences for noncompliance for multinationals are steep, with data protection regulators — who currently have limited fining power — being given the ability to impose penalties of up to either 4 percent of a company's annual global revenue or €20 million ($22.8 million), whichever is greater.

"The heavy fines are definitely the attention-getter," George said. "Up until now, U.S. companies in particular have not really been afraid of the data protection authorities because the penalties have been small, and they've tended to focus on the big technology companies like Google, Microsoft and Facebook. But GDPR gives companies a good reason to get their houses in order."

Regulators including the U.K. data protection authority and the collective of national privacy regulators known as the Article 29 Working Party have started issuing some guidance on their expectations for how companies should implement the new regulations, and attorneys expect more advice to trickle out before the end of the year.

Scott Vernick, Fox Rothschild LLP privacy and data security practice leader, advised colleagues to watch for national data protection regulators to step up their enforcement of privacy and data security issues in the coming months, even before the enhanced fining powers take effect, as a warm-up for the main event next May.

"So if you're a U.S. company gathering information from EU residents, you have to have hard consent from them to gather and process the data and be able to articulate to regulators what kind of data security and data governance plans you have in place to keep data secure," Vernick said.

**Privacy Shield Under the Microscope**

The first EU-U.S. review of a Privacy Shield mechanism enacted about a year ago is slated to begin in September, an event that is sure to be on the radar of privacy attorneys and their clients.

In 2015, the European Court of Justice invalidated the safe harbor mechanism that had permitted data to flow between the U.S. and EU, a decision that sent more than 7,000 companies scrambling for alternate ways to continue transferring information.

EU and U.S. officials in July 2016 provided some relief by launching the Privacy Shield. It obligates U.S. companies to protect EU citizens' personal data and requires more rigid monitoring and enforcement by U.S. regulators. The shield allows Europeans to complain about data misuse through several channels and compels the U.S. government to make commitments about the scope of its surveillance practices. Since it's inception, Google, Facebook, Microsoft and more than 2,200 other organizations have signed up to comply.

"With the review of the Privacy Shield in September, rhetoric will fly on both sides of the Atlantic," Sotto said. "Hopefully, cooler heads will prevail, and the Shield will remain intact and untarnished as a valid data transfer mechanism."

Foley & Lardner LLP partner Aaron Tantleff noted that some companies already have received questionnaires from the European Commission on their experience with Privacy Shield, a sign that "they are trying to understand what is actually going on and see what compliance looks like to date and what needs to be done and should be done."

Another development that is likely to factor heavily into the Privacy Shield review is whether U.S. lawmakers will reauthorize Section 702 of the Foreign Intelligence Surveillance Act. The statute, which gives U.S. intelligence authorities broad authority to conduct surveillance on specific foreign targets, expires at the end of the year.

"Section 702 gave European officials a lot of heartburn when it came to negotiating the Privacy Shield, and they will likely be watching to see what happens with reauthorization and how broad foreign surveillance will or won't be as part of their assessment of whether Privacy Shield is working or not," Vernick said.

--Editing by Christine Chun and Philip Shea.

---