Privacy Legislation And Regulation To Watch In 2017

By **Allison Grande**

Law360, New York (January 2, 2017, 1:03 PM EST) -- With Republicans in control of both the White House and Congress, privacy attorneys will be keeping a close eye on whether long-stalled efforts to modernize and unify government data access and breach notification laws will finally find traction in the coming year, as well as how active regulators such as the Federal Trade Commission and California attorney general will continue to be in policing privacy issues. The upcoming year promises to be anything but predictable when it comes to privacy policy issues, with widespread uncertainty expected to continue to swirl around long-simmering issues such as how far law enforcement should be allowed to go to force service providers such as Apple and Microsoft to turn over user data and whether the FTC's active privacy enforcement agenda and the Federal Communication Commission's newly instituted rules for broadband service providers will thrive. "I think we're all watching, waiting and trying to read the tea leaves as to what the Trump administration and new Republican Congress will mean for privacy and cybersecurity," Sheppard Mullin Richter & Hampton LLP privacy and security practice co-chair Laura Jehl told Law360. "Will they take a hands-off stance, allowing businesses to operate without the additional regulatory constraints that were proliferating under the Obama administration?" she said. "Or will the perceived popular demand for greater privacy and cybersecurity protections mean that a populist Trump administration will embrace such regulation?" Here are some of the top policy issues that privacy attorneys will be watching closely in 2017. **The Data Encryption Wars** The debate over whether service providers can be forced to provide special data access channels for law enforcement reached a fever pitch in 2016, primarily thanks to Apple's decision to press a bicoastal fight over the FBI's demand that the tech giant help it unlock phones belonging to a deceased suspect in the San Bernardino mass shooting and a confessed drug dealer in New York. "It will be interesting to watch whether Congress creates additional authority for law enforcement to spread its wings," said Jeffer Mangels Butler & Mitchell LLP partner Robert E. Braun. In the midst of the Apple battles, which the government ultimately dropped after finding ways to access both phones without the tech giant's help, federal lawmakers floated various proposals to help address the tension between privacy and national security. And attorneys expect that these ideas — ranging from one to **create an independent commission** of public- and private-sector stakeholders to tackle encryption and other issues related to digital security, to another than would require companies to give backdoor access to law enforcement officials who obtain court orders for inaccessible data — won't disappear with the change of the calendar year. "The ability of the government to force private companies to turn over data or help the government by turning over data, that's always a question," said Dechert LLP partner Tim Blank. "We'll see if Congress acts on that. However, given that I do think the next administration is going to be heavily focused on national security at the expense of

privacy, I think that equation is going to be less balanced than it has been in the past." President-elect Donald Trump has made it clear that national security is his top priority and during his campaign called for a boycott of Apple until it caved to law enforcement's data access demands, a stance that indicates that efforts to work with the tech community to study the issue and craft a mutually-acceptable way forward may face a tougher road than they would have during the Obama administration. "In 2017, we're likely to see this dialogue continue and expand and probably take on the flavor that President-elect Trump has identified, which is putting some additional emphasis on national security," said David Turetsky, co-leader of Akin Gump Strauss Hauer & Feld LLP's cybersecurity, privacy and data protection practice. However, Bradley S. Shear, managing partner of Shear Law LLC, was quick to note that the incoming administration could still have some surprises up its sleeves when it comes to dealing with such privacy issues. "The different experiences that the president-elect has had might spur him to come up with some out-of-the box solutions," Shear said. "So maybe we should give the president-elect and his team the benefit of the doubt until we actually see what policies that put in place." **Pushing for Broader Data Access** Law enforcement data access demands don't end with iPhones. For years, both companies and privacy advocates have been pushing for updates to modernize the Electronic Communications Privacy Act, which was enacted in 1986 and is becoming increasingly difficult to neatly apply to the ways in which electronic data is stored by service providers. "I don't expect to see too much federal legislation on privacy, but one area where it could happen because there's still bipartisan support is ECPA reform," Hogan Lovells senior associate Bret S. Cohen said. "It seems like the ECPA reform drum has been beating for awhile, so the question will be whether it's a priority for this upcoming Congress." Lawmakers in 2016 came extremely close to pushing through a long-sought after change that would remove a distinction that creates a lower access bar for emails that are more than 180 days old or opened and instead create a blanket warrant requirement for the contents of all digital data. The measure passed the U.S. House of Representatives in a 419-0 vote in April, but failed to make it out of the Senate Judiciary Committee due to concerns over its potential impact on civil regulatory agencies. "ECPA reform has been on the table every year for quite awhile, so I certainly think it will be an issue that is at least discussed on many levels," said Kendall Burman, a Mayer Brown LLP counsel and former deputy general counsel for the U.S. Department of Commerce under the Obama administration. Another aspect of the outdated privacy statute that could generate some noise in Congress is how it applies to electronic data that U.S. service providers have housed in storage centers located overseas. The issue formed the basis of a closely watched court challenge that found its way to the Second Circuit, which **ruled in July** that ECPA doesn't apply extraterritorially and thus can't be used to force Microsoft and other service providers to disclose email content data stored overseas. Shortly before the Second Circuit handed down its decision, which the federal government has asked the full appellate court to reconsider, a bipartisan group of lawmakers **floated legislation** designed to set a clear standard for when the government can reach overseas to obtain user data. Known as the International Communications Privacy Act, or ICPA, the proposed bill would allow law enforcement agencies to obtain from service

providers the electronic communications of U.S. citizens and permanent residents regardless of where the individuals or communications are located, as long as officials first obtain a warrant. The bill would also permit law enforcement to use warrants to obtain communications related to foreign nationals in situations either where the foreign government does not have a law enforcement cooperation agreement with the U.S. or where a cooperating foreign government does not object to the disclosure, and would reform the mutual legal assistance treaty, or MLAT, process countries use to facilitate such data-gathering. "It's troubling when law enforcement is overstepping its authority under the law, but it's also troubling when law enforcement is following the law, and can't get access to the data it needs," Shear said. "So lawmakers have to come up with the proper mechanism that strikes the right balance between privacy and giving law enforcement what it needs to do its job." **Unifying Breach Laws** The prediction that Congress will finally act to unify a patchwork of 47 state data breach notification laws has been a popular one in recent years, and the 2017 forecast is no different. "There's always hope for a uniform federal breach notification law," Blank said. "We've been waiting for a long time for that." Beginning with California in 2003, states have steadily been enacting laws that require companies that have detected data breaches to report the incidents to consumers and in some cases to state attorneys general in a timely manner. Some states, most notably Massachusetts, have also established baseline data security standards for businesses. Federal lawmakers have floated several proposals in recent years to set nationwide data security and breach notification standards for businesses that handle customer data, but the bills have failed to gain traction, most notably because of the resistance to the suggestion that the legislation preempt stronger state laws. "There's likely to be interest in 2017 in national breach notification proposals that would preempt much of the 47 state laws in this area," Turetsky said. "Whether it will pass or not, I don't know, but there's been Republican interest and some Democratic interest in that, so I would expect that would get attention in the upcoming year." Even if federal lawmakers again fail to act, attorneys say that there will almost certainly be movement on data security and breach notification laws at the state level. California recently amended its breach notification law to require reporting when encrypted data and its accompanying encryption key has been leaked, and similar tweaks are expected to proliferate in 2017. "States may be in a better position to focus their efforts on legislation, and we're likely to continue to see breach notification laws amended because as one state does something new, other states do it as well," Cohen said. "So until we have federal preemption, states are going to continue to experiment with and refine their notice obligations." Breach notification is also going to be a hot topic outside the U.S., including in Canada, where a recent amendment to the country's long-standing national privacy law — which is expected to take effect some time in the new year — will force companies for the first time to report breaches to the Canadian Privacy Commissioner, individuals and others. "People are going to be hearing more about breaches in Canada," VLP Law Group LLP partner Melissa Krasnow said. **What Will the Regulators Do?** Given that the president-elect has indicated that he favors a light touch when it comes to regulation, attorneys will be keeping a close eye on whether the increasingly aggressive stance that regulators such as the FTC and FCC have

been taking to privacy enforcement in recent years will continue. "One of the major platforms of the president-elect was to dismantle regulations that in his view harmed businesses, so we should fully expect that to trickle down to the regulatory processes and priorities that federal administrative agencies take," Cohen said. When it comes to the FTC, which has long considered itself the top cop on the privacy beat, the president-elect will be immediately faced with the task of appointing nominees to fill two vacant commissioner spots and choosing someone to replace the FTC's current chair, Edith Ramirez, who is a Democrat. "Obviously, who the president-elect puts in there will be fundamentally different from if the election had gone the other way, and it will be interesting to see from a policy perspective if this make the FTC take a lesser role in consumer protection generally and on cybersecurity in particular," said Morrison & Foerster LLP global privacy and data security group co-chair Andrew Serwin. At the FCC, current Chairman Tom Wheeler **recently announced his intention** to step down on Jan. 20, casting an even larger shadow of uncertainty over many of the defining developments of his three-year tenure, including his successful push to establish stringent privacy rules for broadband service providers. "Attorneys who represent communications-industry clients should be closely watching the fate of the FCC's new privacy rules for common carrier broadband internet service providers," Jehl said. "It remains to be seen whether the FCC under the incoming Trump administration will continue to back the rules as drafted, or whether they will be eliminated completely." Privacy regulation at the state level will also be worth keeping an eye on, particularly in California, where Congressman Xavier Becerra is poised to take over the attorney general post from Kamala Harris, who took the lead on policing many privacy issues and will now join the U.S. Senate. "The California attorney general's office has been at the forefront of privacy and often is deemed a de facto national regulator given California's privacy laws and significance to the US in terms of population and economy and as the home of many leading technology companies," Krasnow said, adding that it will also be interesting to monitor "whether the influence of California and other states in privacy will become stronger as a result of changes in privacy regulators at the federal level in the new administration." Another state to watch will be New York, whose Department of Financial Services in September unveiled a **first-in-the nation regulation** that requires banks, insurers and others to establish and maintain a comprehensive cybersecurity program and that takes effect on Jan. 1. "This regulation could become a model for other states to follow to fill the gap if federal protections recede," Hughes Hubbard & Reed LLP data privacy and cybersecurity group co-heads Dennis Klein and Seth Rothman said in a joint email. **Revving Up for Big Changes in the EU** One of the biggest cybersecurity developments from the past year happened in May, when European officials, after more than four years of negotiations, finally **approved a sweeping overhaul** of the bloc's data protection regime. Slated to take effect in May 2018, the new general data protection regulation will replace the bloc's current data protection directive with a uniform regulation that tightens restrictions on the use and flow of data while empowering national privacy regulators to levy fines of up to 4 percent of companies' annual global revenue. "With the EU General Data Protection Regulation coming into effect in 2018, many companies have already begun planning

because of the many onerous changes to their business operations that are required as well the potentially business-critical penalties for noncompliance," said Squire Patton Boggs LLP partner Gretchen Ramos. The collective of EU data protection regulators known as the Article 29 Working Party released guidance in December on several key provisions of the regulation, including the requirement for some companies to appoint a data protection officer, the establishment of a "right to data portability," and the notion of a "one-stop shop" enforcement mechanism, and attorneys say they will be watching for further feedback on the regulation in the upcoming year. "2017 will be an important year for the GDPR because as we run closer to implementation in 2018, companies will be looking to devote a lot more attention to it," Turetsky said. Attorneys will also be monitoring how regulators and others react to the new trans-Atlantic Privacy Shield data transfer agreement, which went into effect over the summer and is up for its first annual joint review by EU and U.S. officials in the middle of 2017. "When the Department of Commerce agreed to the Privacy Shield with the European Commission, one of the underlying promises was that the Commerce Department would be more active in making sure companies complied with their commitments under Privacy Shield," Cohen said. "The last few months have been focused on getting the program up and running, but once they're into the flow of things, it will be interesting to keep an eye out for how actively the Department of Commerce and the FTC are in going after U.S. companies for their Privacy Shield compliance."