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

Trump's Security Focus To Hamper Corporate Privacy Efforts

By **Allison Grande**

Law360, New York (November 9, 2016, 2:38 AM EST) -- President-elect Donald Trump's preoccupation with national security is likely to stymie multinationals' increasing efforts to shield their customers' data from government eyes and could interfere with the trans-Atlantic data-transfer deal known as the Privacy Shield, but his hard-line stance against hackers and opposition to strict regulation could be a silver lining for businesses.

With his victory Tuesday night over Democratic nominee Hillary Clinton, Trump is poised to take over the presidency at a time when headlines have been dominated by cyberattacks on targets ranging from the Democratic National Committee to Yahoo Inc., as well as a raging debate over how far law enforcement can go to force companies like Apple to hand over user data.

"Cybersecurity has been a huge high-profile issue that's receiving a lot of attention as of late ... and will require some kind of response and immediate leadership in the first 100 days of the new administration," said Kendall Burman, a Mayer Brown LLP counsel and former deputy general counsel for the U.S. Department of Commerce under the Obama administration.

Law360 spoke with Burman and several other attorneys before the election to gather insight into how Trump would tackle such issues.

Trump spoke only briefly about cybersecurity during his campaign. During the first presidential debate, he said the government needed to get "very, very tough on cyber and cyberwarfare" and the following week he pledged to enhance the nation’s defensive and offensive cybersecurity capabilities. To do so, the Republican said he would take such steps as creating a team of public- and private-sector experts to review the government’s information systems and establish the capability to mount “crippling” counterattacks.

"This is one area where Donald Trump might well support increased government activity," said Drinker Biddle & Reath LLP partner Peter Blenkinsop and counsel Katherine Armstrong in a joint email. "That’s because he generally holds the view that the United States is being taken advantage of by other foreign powers, particularly China."

The Drinker Biddle attorneys noted that in his position paper on U.S.-China trade relations, Trump accused the country of "rampant cybercrime" and vowed that a Trump administration would respond to this issue.

"It would not be surprising, therefore, to find that Mr. Trump believes that stronger cybersecurity protections are needed to safeguard trade secrets of U.S. businesses from foreign hackers," they said, although they added that "what this might entail is anyone's guess, as many of Mr. Trump's positions are rather short on substance."

Dechert LLP partner Timothy Blank noted that Trump would also likely be more willing to use offensive weaponry, such as the "crippling" counterattacks he promised in his policy speech last month, than the Obama administration, and would also be "more willing to gloat about our capabilities."

"Hopefully, he would have somebody guiding him through that thought process when it comes to cybersecurity," Blank said.

Tilting the Scales Toward Law Enforcement

Attorneys said Trump's position on combating cyberattacks, especially those that are believed to be the work of nation-states such as China, Russia and North Korea, would likely help the business community by focusing more attention and resources on creating roadblocks to such attacks and ensuring that the private sector's concerns are heard.

But they also said the president-elect's stance in other related areas could be more troubling.

For example, there's the ongoing debate over how far companies such as Apple and Microsoft should be required to go to help the government in criminal and national security probes. Trump's laser focus on national security could result in mandates that run counter to businesses' desire to protect their customers' data from government prying.

"President Trump would be much more of a 'we need it so give it to us and we'll deal with the consequences later' type of leader," Blank said. "With Trump as president, it's likely that the collaborative atmosphere between the government and private businesses that has been fostered in recent years would probably disappear."

The most notable illustration of the collision between privacy concerns and law enforcement needs came earlier this year, when Apple pressed 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. After months of heated debate and magistrate judge rulings that both favored and went against Apple, the government ultimately dropped both fights after finding ways to break into the devices without Apple's help.

Trump responded to the dust-up by calling for a boycott of Apple until it provided access.

Legislative proposals have been floated to resolve this issue, 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.

While Trump has yet to say whether he will support any of these proposals, his reaction to the Apple row indicates that at the least, tensions between the public and private sectors will continue to grow.

"The way that privacy and security will evolve over the next four years is going to have to be with respect for and recognition of the importance of balancing the government's role as the protector of national security and the private sector's role as a really rich source of development in this area. But Trump's response to the Apple case completely ignored all the factors that must be balanced in this situation," Blank said. "It was purely a 'national defense trumps everything' stance, and that sort of view demonstrates a much lower regard for personal privacy and business concerns than what we've seen in the past."

An Expansion of the Surveillance State

Trump is likely to have a similar outlook when it comes to intelligence gathering, a topic that has grown in notoriety due to the actions of former NSA contractor Edward Snowden, who in 2013 began leaking classified materials that revealed the broad scope of the government's bulk data-collection programs.

As president, Trump — who has previously called for Snowden's execution — is likely to staunchly defend the sweeping bulk collection of citizens' and foreigners' data that has drawn so much criticism in both the U.S. and abroad, according to attorneys.

In the wake of these disclosures, Congress moved to reign in the mass, indiscriminate collection of individuals' data through the passage of the USA Freedom Act in 2015 and other such actions. But Trump has made clear that he believes that some civil liberties may need to be circumscribed in exchange for increased national security, and could seek to reinstate NSA programs that were brought to a close under the Obama administration, the Drinker Biddle attorneys noted.

"President Trump might seek to rescind or amend Presidential Policy Directive 28, which governs how the United States conducts signals intelligence activity, and we can expect to see him put pressure on Congress to reinstate provisions of the Patriot Act that were amended by the USA Freedom Act of 2015," they said.

Problems for the Privacy Shield

Taking actions to re-establish such broad data-gathering authority could reverberate not just in the U.S., but also have ripple effects overseas, attorneys say.

The most obvious impact of such an expansion would be on the stability of the Privacy Shield data-transfer pact, which U.S. and EU officials finalized earlier this year, and for which more than 700 multinationals**,** including Google and Microsoft, have already signed up in order to send personal data outside the EU.

The Privacy Shield deal was pushed through in large part to help multinationals that had long relied on the safe harbor data-transfer mechanism, which the European Court of Justice struck down last October on the grounds that it hurt EU citizens' privacy rights because U.S. intelligence officials were being given unfettered access to their personal data.

As a result of that ruling, the new Privacy Shield includes commitments from the U.S. about the robust safeguards and limitations that will be in place to keep U.S. law enforcement and intelligence officials from freely accessing transferred data, a delicate balance that may be disrupted by Trump's actions. Especially troublesome could be another provision in the deal that allows officials on both side of the Atlantic to conduct an annual review to monitor the functioning of the deal and make changes.

"Any walking back of promises made by the U.S. during Privacy Shield negotiations or changes to representations concerning how U.S. law balances privacy and national security are likely to be met with anger by EU data protection authorities and members of the European Parliament," Blenkinsop and Armstrong said.

These moves could create trouble during both the annual joint review and factor into closely watched challenges before the Court of Justice to both the Privacy Shield and the sufficiency of standard contractual clauses that many multinationals also rely on to transfer data across the Atlantic, the Drinker Biddle attorneys said.

"If these transfer mechanisms were invalidated, the impact on multinational companies in a variety of sectors would be tremendous, and many companies could be forced to re-engineer their data-processing systems and activities," they said.

A Relaxed Regulatory Environment

However, while the law enforcement and intelligence issues that companies frequently face could become more perilous under President Trump, the new administration may also create a slightly more welcoming regulatory environment than the one that businesses have faced under Obama.

The last few years have been marked by a rush of best-practices guidance and increased attention to privacy and data-security issues by agencies including the Federal Trade Commission, Federal Communications Commissionand U.S. Securities and Exchange Commission.

"Donald Trump has indicated that he eyes government regulations with skepticism and that he would seek to eliminate as many as possible," Blenkinsop and Armstrong said. "We might well see [the] Trump administration modify privacy regulations applicable to the health and financial sectors to provide businesses with increased flexibility to market their products and reuse personal data for secondary purposes."

The Trump administration may also seek to reign in attempts by the Consumer Financial Protection Bureau to regulate privacy, particularly in light of a recent D.C. Circuit ruling that found the agency's single-director structure to be unconstitutional, and to modify the direction of agencies such as the FCC and FTC over time through the appointment of new commissioners and chairs, the Drinker Biddle attorneys say.

Trump will have an immediate opportunity to leave his stamp on the FTC, which is widely viewed as the nation's top privacy regulator and currently has two vacant commissioner positions.

"I don't think anybody knows how Trump will handle the FTC," said Reed Freeman, WilmerHale's cybersecurity, privacy and communications practice co-chair and a former FTC staff attorney.

Freeman noted that when former President Ronald Reagan was elected, he appointed a chairman who "tried to effectively dismantle the FTC," while under a newly elected President Barack Obama the agency took a "sharp turn" and began to focus much more heavily on privacy issues with the appointment Jon Leibowitz as chairman in 2009.

With Trump being given the power to choose a new chair aligned with his political party as well as two new commissioners who will give Republicans a three-member majority on the commission, his pick is likely to have at least a marginal impact on the agenda and enforcement priorities of the FTC over the next four years.

"Given his campaign rhetoric, it doesn't seem to me like the consumer protection mission of the FTC would be the highest thing on his agenda as president," Freeman said. "And I would suspect that he would look to appoint moderate commissioners and a chair that would be a little less aggressive toward businesses on the margins, and that all of their enforcement and workshop activities designed to articulate new guidance or suggestions for compliance would slow down from its current pace."

--Editing by Mark Lebetkin and Rebecca Flanagan.
