Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

NSA Spying To Bolster Calls For Strict EU Privacy Regime

By **Allison Grande**

Law360, New York (June 12, 2013, 10:31 PM ET) -- The revelation that the Obama administration is collecting vast troves of phone and Internet records has prompted outcries from European Union officials that attorneys say could undermine aggressive efforts by Google Inc., Facebook Inc. and other U.S. companies to water down the bloc's proposal to tighten its data protection regime.

Since **reports emerged last week** about secret intelligence-gathering programs that allow the National Security Agency to routinely seize customer data from Google, Facebook and others, EU regulators and lawmakers have been quick to demand clarification from their U.S. counterparts on how these practices affect citizens in Europe, where privacy is a constitutional right.

The incident "does not help allay any fears that the EU has about the amount of information that U.S. technology companies have, but rather adds an additional fear about how that data is being used," Davis & Gilbert LLP partner Gary Kibel said. "[It] is going to raise questions about whether sufficient controls are in place or ... if all of their suspicions have been correct."

European Commission Vice President Viviane Reding on Tuesday sent a letter to U.S. Attorney General Eric Holder with seven questions about the reach, aim and methods of the government in obtaining information through electronic surveillance programs such as PRISM, which authorizes the NSA to collect emails and other personal data from nine top Internet companies in order to track foreign targets.

The pair are scheduled to meet at the upcoming trans-Atlantic ministerial meeting in Dublin that begins on Thursday, where U.S. officials will be expected to provide Reding and others with an explanation that will quiet long-running concerns that U.S. companies cannot be trusted to adequately safeguard EU consumers' data, according to attorneys.

Reding's questions will likely find their way into the ongoing debate over the European Commission's proposal to tighten the bloc's data protection regime by replacing the current directive implemented by each member state with a binding regulation that would impose several new and more stringent requirements regarding how companies protect personal information.

Since the draft proposal was **leaked in December 2011,** U.S. officials and companies have lobbied aggressively to curb its reach and ease restrictions on the way that data controllers collect, use and share consumer information, an effort attorneys say will likely suffer after the recent revelations.

“U.S. tech companies have been lobbying hard, with some success, to water down the proposed data protection regulation,” Cohen & Gresser LLP intellectual property practice chair Karen Bromberg said. “But it is possible that the revelations that the very same companies who have lobbied so vigorously to weaken these regulations are the ones that have given the NSA — either knowingly or otherwise — access to customer data may give a boost to those calling for tougher data protection standards."

While the EU has held firm on many provisions, the U.S. lobbying efforts have so far resulted in several concessions.

One of the earliest, which was first reported by the Financial Times on Wednesday, came around the time that the proposal was formally introduced in January 2012, when the European Union's executive body agreed to drop a clause from the measure that would have limited the ability of U.S intelligence agencies to gather data from non-U.S. citizens through programs like the ones exposed last week.

Companies have also found success at chipping away at the commission's proposal, with EU justice ministers late last week giving their preliminary backing to a draft of the regulation prepared by the Council of the European Union that would narrow the scope of the reform to exclude certain entities and ease restrictions such as the standard for consent for data collection.

But with fresh concerns over the way U.S. companies guard their data, the tide may soon turn back to a more restrictive approach to ensure that consumers' information doesn't end up in unintended hands, according to attorneys.

“The debate over the proposed EU regulation had recently reached a crucial stage with a proposal from the Council of the European Union to make the commission’s proposed regulation somewhat more business friendly,” Snell & Wilmer LLP partner Timothy Toohey said. “I would expect that those who are in favor of greater restrictions will point to the controversy to argue that the NSA is taking advantage of the relatively unfettered collection and retention of data by large U.S. companies.”

One provision that could be reassesed is the controversial “right to be forgotten,” which EU officials have eased in recent months amid U.S. companies' concerns over the impracticality of being able to delete users' data at their request, Kibel said.

“The right to be forgotten is all about users being able to to ask companies to delete the information that they hold about them, but with the government involved, it is not forgotten and actually retained for a greater period of time,” he said. “The right to be forgotten is likely to be pulled back a bit now and be back on the table because of these additional issues.”

The revelations could also impact other agreements between the two regions over the way that companies store and transfer data, including the existing U.S.-EU Safe Harbor and upcoming transatlantic trade talks, according to attorneys.

“The whole international data flows debate will be severely distorted as this type of story gives powerful ammunition to those who argue that international data transfers are inherently unsafe and should be prohibited by default, which of course disregards the the reality of Internet and mobile communication,” London-based Field Fisher Waterhouse LLP partner Eduardo Ustaran said.

But Christopher Wolf, the director of Hogan Lovells' privacy group, predicted that the impact will not be as adverse as some are forecasting because, as his firm pointed out in a recent white paper on national security access to data, other countries including France, Germany and the U.K. use information collected from phone and Internet companies in a

similar manner, often without the judicial due process and legislative oversight imposed on U.S. practices.

And while the disclosure of the U.S. government's surveillance polices has created "significant issues" in Europe for companies like Google and Facebook, the push to restrict their access to user data may ultimately fall short given the companies' dominance in the global market, according to Pryor Cashman LLP digital media practice group co-chair Robert J. deBrauwere.

"While European users and their governments will be more wary of putting their personal information in the hands of American companies, and perhaps in adopting cloud computing technology, in general, there may ultimately be more bark than bite as there are few substitutes for the online services offered by companies like Apple, Facebook and Google," he said.

--Editing by Elizabeth Bowen and Jeremy Barker.