What All The Privacy Reform Recommendations Really Mean

Law360, New York (January 31, 2014, 12:42 PM ET) -- Since unauthorized leaks first disclosed certain bulk collection of commercial data by the U.S. intelligence community nearly eight months ago, debate has raged about the breadth and appropriateness of government surveillance in the world of "big data." At the forefront of this debate has been the National Security Agency’s telephone metadata program, under which the agency collects in bulk the telephony metadata of virtually all Americans to aid in national security investigations.

Privacy and civil liberties advocates have argued that the bulk collection is illegal and unduly intrusive, while various government officials and other supporters of the NSA’s program have countered that the program is legally sound, does not collect private information such as content, and is necessary to prevent terrorist attacks.

Two federal district courts have considered the constitutionality of the program and reached opposite conclusions in December. These arguments for and against the NSA’s bulk collection of telephony metadata reflect broader questions currently being debated about how to balance national security interests with privacy and civil liberties concerns at a time when technology enables government agencies, as well as private companies, to collect and analyze massive amounts of data about individuals’ lives.

In the past month, three public reports containing recommendations on how to reform the NSA’s telephone metadata program have been unveiled. These reports may prove to be major steps towards reaching certain consensus points on the contours of the telephone metadata program generally and on government surveillance issues more generally. Moreover, the recommendations that prevail from those reports could have ramifications for U.S. companies — particularly technology and communications companies — that hold significant amounts of data about individuals’ activities. Those recommendations could change the requirements on how these companies will store and protect such data, and how companies will relate to both government investigators seeking disclosure and consumers expecting that their data be kept private.

U.S. companies, especially the major technology and communications companies, have borne the brunt of the criticisms associated with the newly revealed programs. The NSA and other government agencies have sought to access those companies’ records as part of national security and other investigations; the companies generally are reluctant to interfere with government investigations, particularly where national security may be at stake.

At the same time, those companies have come under scrutiny from privacy and civil liberties advocates following revelations that they have provided considerable amounts of personal information to the
government. The companies are also concerned that such revelations may undermine their customers’ trust that their personal data will be protected, and may ultimately drive customers away. Not surprisingly, several major technology and communications companies have been lobbying Congress to reform the government’s surveillance programs.

The problem for companies is particularly acute in the context of the NSA’s telephone metadata program because of the way the program works under federal law. The program operates under Section 215 of the Patriot Act, which provides that the government may obtain an order from the Foreign Intelligence Surveillance Court (commonly referred to as the “FISC” or the “FISA Court”) requiring production of records as part of terrorism investigations where the government has “reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation.”

Citing Section 215, the NSA periodically obtains orders from the FISA Court allowing it to collect from the major U.S. telecommunications companies bulk telephony metadata — information about a person’s phone calls, including duration of calls and the numbers dialed, but not including the contents of calls — of virtually all Americans. The NSA has been collecting the metadata on an ongoing basis for seven years.

The FISA Court is designed to allow for ex parte presentations by the government when petitioning for a collection order, meaning that the individuals whose records are being provided are not informed of the government’s petition and cannot challenge it in the FISA Court.

While that arrangement may make sense to protect the secrecy and integrity of a terrorism investigation, it puts the recipients of the FISA Court order — the telecommunications companies — in a difficult position. Although they are the only party that could presently challenge the orders in the FISA Court, they are understandably unwilling to interfere with a terrorism investigation. Yet their customers may feel that the companies are not doing enough to protect their data from unwarranted government intrusion, particularly given the vast breadth and duration of the NSA’s collection.

The three recently issued reports on how to reform the telephone metadata program could have a significant impact on these companies as they try to thread the needle between cooperating with government investigations and honoring consumers’ privacy. The first-released report was issued by the Review Group on Intelligence and Communications Technologies, an ad hoc group comprised of renowned law professors and former intelligence community officials. The group released 56 recommendations on how to wholesale reform many aspects of signals intelligence gathering and use, including the telephony metadata program.

Next, on Jan. 17, 2014, President Obama outlined five concrete initiatives to modify — but not overhaul — the program. Then on Jan. 23, the statutorily created Privacy and Civil Liberties Oversight Board issued 12 discrete recommendations focused on the telephony metadata program and the FISA Court. Although each of these sets of proposals deals specifically with the telephone metadata program, each clearly has an eye toward the broader issue of balancing national security and privacy interests in general.

While the three sets of proposals are at odds in some respects, they share three prevailing recommendations: (1) reconsideration of how the bulk collection of telephone metadata is currently being conducted; (2) creation of a public advocate before the FISC to present an alternative position to the U.S. Department of Justice when FISC orders are being sought (to modify the ex parte process); and (3) having the intelligence gathering operations, particularly when involving private sector or
commercial data, be as transparent as possible. Each of these themes will impact private companies and their relationship with the intelligence community.

Storage of Bulk Telephone Metadata

Although the three reports disagree on whether bulk telephony metadata collection is legal, appropriate, or necessary at all, all three contemplate the possibility that the bulk data might be retained by another entity other than the government, such as the telecommunications companies themselves or a third party. Whether doing so is feasible is unclear, but it is likely that the bulk collection and storage of metadata will continue in some form (despite the PCLOB’s recommendation that it be stopped in its entirety).

The president announced the end of the NSA telephone metadata program “as it currently exists,” but advocated retaining the program in some form, therefore its continuation is likely. There may be modifications on the level of controls needed to access the database, however, and on the standard of review.

A regime in which private companies, particularly the telecommunications companies that have been providing the information to NSA pursuant to FISC orders, are expected to retain massive amounts of information well beyond the time they would be retained for business purposes could pose significant challenges for those companies.

Such storage could impose significant infrastructure costs, and would cause additional security, communications and data quality problems. The bulk collection and storage of telephony metadata still poses significant privacy and data security risks, regardless of where the information is physically stored. Transferring the long-term burden onto private companies does not provide additional privacy protections while potentially generating additional data security risks.

Advocate in the Foreign Surveillance Intelligence Act Court

Despite public opposition from FISC judges, all three reports recommended the creation of a public advocate to engage on the merits of some, or all, of the FISC orders. The authorities and responsibilities of the proposed advocate varied, as did the scope of work, but the adversarial approach was evident in each proposal.

A public advocate of sorts could assist private companies in two ways. First, the public advocate would relieve the pressure on the companies to resist the government’s bulk data collection in the FISA Court. Although the proceedings would remain ex parte, the companies would no longer be the only potential voices of opposition in the FISA Court.

The public advocate’s official role would be to represent the interest of the public — including the telecommunications companies’ customers — to maintain privacy over personal information, and the companies could sensibly rely on the public advocate to represent that interest in whole or in part. Second, the adversarial process may increase public support and understanding of the FISA Court process. Even if the details of the proceedings cannot be made public, knowing that both sides of the argument are presented should increase public comfort and provide the system added legitimacy.

Increasing Transparency About Bulk Intelligence Gathering
The call for increased transparency about bulk intelligence gathering has echoed throughout this debate; not only did all three sets of recommendations advocate for increased transparency when possible, members of Congress, FISC and telecommunications companies have all clamored for more transparency (without undermining security). The major technology companies, which have faced considerable public pressure to be more open about their cooperation with government surveillance, have been strongly lobbying for increased transparency and the ability to provide greater specificity about the law enforcement and national security requests they receive.

The Obama administration took a major step toward addressing these calls on Jan. 27 when the Department of Justice reached a settlement in a suit brought by several major technology companies seeking permission to publish more information about their responses to government demands for data pursuant to national security investigations. Under the settlement, which must still be approved by the FISA Court before going into effect, the plaintiffs and other companies will be permitted to disclose general information about the number of demands they receive from the government, how many customers’ accounts are affected, and the legal authorities for those demands.

The settlement, and increased transparency in general, may benefit companies by increasing public confidence in both the process and the companies themselves. By making these disclosures, companies may be able to quell some fears that they readily are capitulating to the government without considering legal protections or their customers’ privacy.

Moreover, the creation of a standard set of information that companies may disclose will provide the companies with needed certainty. Rather than each company having to determine what level of transparency is appropriate, and whether to be more or less transparent than their competitors, the companies can simply refer to the settlement or other standards that emerge.

Despite the progress made by the settlement, questions about the appropriate level of transparency for both the government agencies that seek customers’ data and the private companies that receive those requests will remain prominent. The information that may be disclosed under the settlement is general, and many consumers and privacy advocates may still feel that it is insufficient to assure the public that the government’s surveillance programs are not unduly intrusive. After all, the information that can be disclosed under the settlement is unlikely to provide any revelations about the bulk telephony metadata collection that have not already been made public by the unauthorized leaks.

Conclusion

The era of "big data" for signals intelligence continues, however, the consistent themes of transparency, advocacy and analyzing alternatives to wholesale undifferentiated bulk collection are important recommendations to mature these practices. Some of the elements — such as adding a public advocate — will need congressional approval, but the consistency and widespread support of these overarching recommendations may encourage Congress to consider these modifications.

American businesses have been disproportionately disadvantaged by the unauthorized disclosures of the signal intelligence gathering, particularly in their inability to respond to general allegations with details and figures. This in turn has impacted sales of products and services, particularly internationally.

These types of recommendations for transparency, advocacy and additional alternatives should benefit U.S. companies, and the U.S. public, and should be strongly considered by Congress and by relevant intelligence officials. To the extent bulk collection of commercial information is necessary to the national
security mission, the three reports and companies agree — be transparent as possible, and integrate privacy and security in the process. The next steps will be to determine exactly how to implement these broad themes into an effective, and privacy-protective, solution for U.S. intelligence, and U.S. business.

—By Mary Ellen Callahan and Michael T. Borgia, Jenner & Block LLP

Mary Ellen Callahan is a partner in Jenner & Block’s Washington, D.C., office. She founded and chairs the firm’s privacy and information governance group. Michael Borgia is an associate in the firm’s privacy and information governance group in Washington.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2014, Portfolio Media, Inc.