The job of protecting security and privacy

By ALEXANDER W. JOEL, Civil Liberties Protection Officer for the Office of the Director of National Intelligence

McClatchy-Tribune News Service

August 13, 2013

Many Americans probably don't know that there is a senior official whose job by law is to help ensure that civil liberties and privacy protections are built into intelligence programs. I am that official - the "Civil Liberties Protection Officer." I engage with the director of national intelligence and other intelligence officials to oversee and guide intelligence activities.

I lead a team of experts who coordinate not only with intelligence operators and analysts, but also with government lawyers, inspectors general, compliance officials and oversight boards, to help shape intelligence activities and oversee their implementation. As the intelligence agencies seek to protect the nation's security, they must also protect civil liberties and privacy.

Explaining to the public how all of this comes together is important, but is hard to do because it involves sensitive information that adversaries could exploit to avoid detection. By definition, most intelligence work can't be done openly. A fully transparent intelligence service, after all, could not be an effective one.

It's human nature for such secrecy to fuel suspicion and mistrust. People assume that when someone hides something, it's because he's doing something wrong. This natural suspicion is evident in the concerns about two programs that were recently disclosed: the telephone metadata program conducted under the "business records" provision of the Foreign Intelligence Surveillance Act (which was amended by Section 215 of the PATRIOT Act), and the collection of communications from foreign intelligence targets who are non-U.S. persons located outside the United States, conducted under Section 702 of FISA. The Office of the Director of National Intelligence has published a significant amount of information about both of these programs on its public website, www.dni.gov.

Because these are complicated programs, I want to address a few publicly discussed concerns here in a non-legalistic way.

Under the phone metadata program, the government obtains and reviews phone records only to identify whether telephones associated with a foreign terrorist organization are in communication with a telephone inside the United States (directly or indirectly). This does not involve collecting actual phone conversations. While the government believes that it has been carrying out this program in a manner that protects both national security

and privacy, we are carefully exploring alternatives with the congressional oversight committees to address public concerns.

Under the Section 702 program, the government can only obtain foreign intelligence information as defined by law, using court-approved procedures to identify specific foreign intelligence targets outside the United States. This authority cannot be used to intentionally target United States persons or anyone inside the United States.

If the government is focusing on a foreign intelligence target abroad, and incidentally obtains a communication between that target and a United States person (or discussing a United States person), what happens? Section 702 requires that such communications be carefully handled only as specifically authorized by court-approved procedures; for example, information identifying a U.S. person may only be included in an intelligence report if it is necessary to understand the foreign intelligence being reported.

Compliance under these programs is verified by several layers of oversight. For example, my office jointly oversees the Section 702 program with the Department of Justice. We verify that potential compliance incidents are documented and reported, and that any improperly collected information is purged from government systems. We regularly visit the facilities involved, review audit records, talk directly to the analysts, and submit our findings to Congress and the FISA Court.

Mistakes happen, and when they do, they are taken seriously. To date, we have found errors caused by inadvertence or technical problems, but have not found an intentional violation (which could result in criminal penalties, with fines of up to $10,000 and imprisonment of up to five years).

Oversight boards are also involved. The President's Intelligence Oversight Board reviews reports of potential violations. The Privacy and Civil Liberties Oversight Board, an independent federal agency, is currently conducting an in-depth review of these two programs, and has full access to classified information about them and to the personnel involved. My office works with both boards to ensure that they are receiving the information they need to perform their oversight functions.

Congress also provides oversight, through the intelligence oversight committees, which were established specifically to provide a venue in which classified intelligence activities could be comprehensively discussed and reviewed. Both programs are regularly briefed to the congressional oversight committees.

And in the FISA Court, the government's activities are strictly supervised. The Court is composed of regular federal district court judges, who take their responsibilities seriously, and act with care and deliberation. These judges are by no means a "rubber stamp." During my office's regular engagements with government officials on matters before the Court, I have been impressed with how rigorously the Court oversees government activities.

Some people question whether people who work for the government can be trusted. In my experience, intelligence professionals ï¿½ and those overseeing them - are profoundly committed to the oath they take to support and defend the Constitution. People inside government have questions and concerns just like everyone else. It's my job to raise civil liberties and privacy issues about intelligence activities, and I do. If intelligence personnel have legal or civil liberties concerns, they can raise them in secure ways, including by contacting my office, offices of inspector general, or the congressional oversight committees. Under law, they are protected from reprisal if they do.

Can more public transparency be provided? We recognize how crucial this is to earning and retaining public trust, and are working to provide it in a way that does not compromise the nation's security. In addition to posting information about both these programs on its public website, the ODNI just declassified additional documents pertaining to the phone metadata program.

Protecting civil liberties and privacy in the conduct of our intelligence activities is not my job alone; it is the job of every intelligence professional. No one is perfect, of course, and it is important to examine carefully different alternatives that enable the intelligence community to fulfill its core mission of serving the American people, under the law, in a manner that protects both their security and their freedom. While there are undoubtedly ways to do this job differently, I hope no one doubts our commitment to get it right.

ABOUT THE WRITER

Alexander W. Joel is the Civil Liberties Protection Officer for the Office of the Director of National Intelligence; he reports directly to the Director of National Intelligence. He wrote this for McClatchy-Tribune News Service.