NSA, DEA, IRS Lie About Fact That Americans Are Routinely Spied On By Our Government: Time For A Special Prosecutor

By Jennifer Stisa Granick and Christopher Jon Sprigman **Forbes**

It seems that every day brings a new revelation about the scope of the NSA's heretofore secret warrantless mass surveillance programs. And as we learn more, the picture becomes increasingly alarming. Last week we discovered that the NSA shares information with a division of the Drug Enforcement Administration called the Special Operations Division (SOD). The DEA uses the information in drug investigations. But it also gives NSA data out to other agencies – in particular, the Internal Revenue Service, which, as you might imagine, is always looking for information on tax cheats.

The Obama Administration repeatedly has assured us that the NSA does not collect the private information of ordinary Americans. Those statements simply are not true. We now know that the agency regularly intercepts and inspects Americans' phone calls, emails, and other communications, and it shares this information with other federal agencies that use it to investigate drug trafficking and tax evasion. Worse, DEA and IRS agents are told to lie to judges and defense attorneys about their use of NSA data, and about the very existence of the SOD, and to make up stories about how these investigations started so that no one will know information is coming from the NSA's top secret surveillance programs.

"Now, wait a minute," you might be saying. "How does a foreign intelligence agency which supposedly is looking for terrorists and only targets non-U.S. persons get ahold of information useful in IRS investigations of American tax cheats?" To answer that question, let's review this week's revelations.

Back in 2005, several media outlets reported that NSA has direct access to the stream of communications data, carried over fiber optic cables that connect central telephone switching facilities in the U.S. with one another and with networks in foreign countries. Reports suggested that the NSA had installed equipment referred to as "splitter cabinets" at main phone company offices, where they make a copy of all data traveling on the fiber optic cable and route it into a secret room where computers scan through the information – searching for names and terms that are themselves secret — as it goes by. For years, the federal government refused to comment on these reports. But on August 8, an unnamed senior administration official confirmed this practice to the New York Times.

We also learned that the NSA can grab information off these fiber optic cables in near real time using a tool called XKeyscore (XKS). Searching the firehose of Internet and telephone data as it flows takes an immense amount of computing power. The XKS system dumps a portion of the communications information NSA snatches into a truly immense local storage "cache." This cache can keep network information for a few days, depending on the amount of traffic. This gives the NSA's computers time to search through what otherwise would be an unmanageable torrent of emails, phone calls, chats, social network posts, and other communications. And importantly, XKS

searches do not involve just communications "metadata". The XKS system searches the contents of our Internet and telephone communications. Which is directly at odds with repeated Administration statements suggesting that NSA mass surveillance was limited to metadata.

To seize and search through all of this information without a warrant, the agency must comply with just a few legal limitations. Under the FISA Amendments Act, the NSA is not allowed to intentionally collect purely domestic information. That is, the NSA can search communications it believes begin or terminate in another country, either based on the facility where the information is collected (for example, an undersea cable) or other signifier, like an IP address that suggests origination abroad. Of course, these determinations are subject to error, particularly when the surveilled facility is in the U.S. and carries a substantial amount of purely domestic traffic.

To reduce the amount of purely domestic traffic that ends up on the desks of NSA analysts, the agency relies on post-seizure "minimization" procedures. For several reasons, however, these procedures are fundamentally inadequate to protect communications privacy. First, the minimization procedures are themselves secret. Moreover, by law, purely domestic communications that the NSA inadvertently collects need be deleted only if they "could not be" foreign intelligence information – a provision that requires the NSA to delete very little. Some minimization procedures have been leaked to the public, and these show that the government may "retain and make use of "inadvertently acquired" domestic communications if they contain usable intelligence, information on criminal activity, threat of harm to people or property, are encrypted, or are believed to contain any information relevant to cybersecurity." Even otherwise privileged communications between individuals and their lawyers are not deleted. The agency merely stores those in a separate database so they are not sent to a law enforcement agency for use in a criminal case.

Once the NSA identifies the subset of international or "one-end" foreign communications (i.e., those where a foreigner is either a sender or recipient), analysts are supposed to search only for "foreign intelligence" information. But since "foreign intelligence" includes anything relevant to the conduct of U.S. foreign affairs, this limitation alone imposes no real restraint on NSA's warrantless spying. Certainly, the NSA isn't limited to counterterrorism operations.

In undertaking their searches, NSA analysts use either "strong" or "soft" selectors. "Soft" selectors are a broad kind of search that pulls up messages based on content or even the language in which a message is written. When the NSA uses soft selectors, it can search the vast amounts of information it collects to retrieve all Internet users' discussions of particular topics or in particular languages. The potentially very broad scope of searches using soft selectors is quite frightening, as ordinary Americans' communications are likely to show up in search results.

"Strong" selectors pull up information associated with a particular known individual. The Obama Administration has repeatedly assured us that these strong selectors may only target non-U.S. persons. But screenshots of the user interface for submitting selector queries tell a different story. Published by the Guardian, they show that NSA analysts are presented with dropdown lists of preapproved factors the NSA accepts as sufficient proof that a person is a foreigner, including being "in direct contact with (a) target overseas" or the use of storage media (like a server located abroad) seized outside the U.S. So any U.S. person who talks to a foreigner that the NSA has identified as a target, or who stores data on a server outside the U.S. (as someone might well do if emailing from a foreign hotel room) may be presumed to be a foreigner. And that's not even the worst of it. Leaked

NSA documents also suggest that the agency will presume that a person is a foreigner whenever there is no information suggesting otherwise. That sort of willful blindness gives the NSA a lot of leeway to target Americans.

Worse, we now know that the NSA's assertion that it does not "target" U.S. persons is either a lie, or is about to become one. Leaked NSA documents show that in 2011, the NSA changed its "minimization" rules to allow its operatives to search for individual Americans' communications using their name or other identifying information. Such a change would turn "minimization" into a blanket authority to warrantlessly spy on Americans – in defiance of specific legal restrictions prohibiting this sort of domestic spying. Senator Ron Wyden has said that the law provides the NSA with a loophole potentially allowing "warrantless searches for the phone calls or emails of law-abiding Americans", and raised the issue when he met with President Obama on August 1. This is the first time we've had evidence that the NSA has — or will have — the authority to warrantlessly search its databases with the specific intent of digging up information on specific U.S. individuals.

We can sum up very simply – at this moment, the NSA enjoys virtually unrestricted power to spy on Americans, without a warrant or any particular suspicion that any person spied upon has done anything wrong. Our phone, email and potentially other records are fair game for bulk collection. The contents of our communications with people overseas are also fair game, so long as there is an approved foreign intelligence purpose for the collection. The NSA does not believe that any stored emails are protected by the Fourth Amendment, so it can collect them from providers with little restraint. As far as we know, the only category of information the NSA currently believes is off limits to mass surveillance are the contents of phone calls it knows in advance are solely between Americans.

This is an astonishing development in the U.S., a nation that, until recently, carefully restricted the power of its domestic spying agencies by forcing them to submit narrow requests for spying authority to a court, which would issue a warrant if the government showed probable cause to believe that the surveillance target was engaged in some sort of wrongdoing. At this point, it's clear those limits are gone. The United States is now a mass surveillance state.

In last week's press conference, President Obama reassured the nation that "America isn't interested in spying on ordinary people." In other words, do not worry, because the information will only be used for narrow counterterrorism or broader foreign intelligence purposes. But the latest revelations show that these assurances too are a lie. Under current U.S. surveillance law, the NSA may share with domestic law enforcement information obtained both through authorized surveillance, and information unlawfully but unintentionally collected, if it contains evidence of a crime. This rule was worrisome when the NSA was only conducting targeted surveillance of foreign powers. It is terrifying now that the NSA scans virtually all American cross-border communications. And this is especially true in light of the recent reports showing that any number of other three-letter agencies are howling for access to NSA data for use in investigations of Americans' drug use, tax evasion, and even copyright infringement. Usually, these agencies would need at least warrants based on probable cause that an individual was committing a crime before they could obtain the contents of our communications, and would need to certify to a public court that email or phone records are relevant to an ongoing criminal investigation before it could collect such traffic data. But if they get their hands on NSA data, all these bothersome civil liberties protections simply vanish.

Which brings us to the Drug Enforcement Administration (DEA). As we noted previously, the DEA has a secret division called the Special Operations Division or SOD. The SOD receives intelligence intercepts, wiretaps, informants and a massive database of telephone records from its partner agencies, of which the NSA is just one, to distribute to authorities across the nation to help them launch criminal investigations of Americans. The SOD gets information from the NSA and shares it with, among other agencies, the IRS.

And this is where things get truly ugly. When agents receive SOD information and rely on it to trigger investigations, they are directed to omit the SOD's involvement from investigative reports, affidavits, discussions with prosecutors and courtroom testimony. Agents are instructed to then use "normal investigative techniques to recreate the information provided by SOD." IRS agents receiving SOD data, which presumably can include information from the NSA, have been similarly instructed. They are instructed, in other words, to create a fake investigative file, and to lie. To lie, in particular, to defense lawyers and to judges, about the source of the evidence used in criminal prosecutions.

By hiding the fact that information comes from NSA surveillance, the government both masks the extent to which NSA's domestic spying is used to trigger investigations of Americans, and prevents legal challenges to highly questionable surveillance practices like bulk phone record collection, warrantless access to American communications with friends and family overseas, and retention and use of illegally obtained domestic calls and emails.

This is outrageous conduct. It is the sort of thing you expect from the Chinese government, or one of the now-vanished governments of the Warsaw Pact. And there is no stronger proof of the dangers of the NSA's domestic spying effort than the fact that the government has consistently lied about it and attempted to cover it up. Think for just a moment about the stories J. Edgar Hoover could have plausibly concocted about Dr. Martin Luther King, Jr. or any other civil rights activist with this kind of detailed information. The Obama Administration has gone after leakers, and the journalists at outlets like the Associated Press or the New York Times who use them as sources, with unprecedented force. Think about what the current Attorney General, Eric Holder, could do to bring down these reporters who cover – sometimes in ways the Obama Administration doesn't like — the conduct of American foreign policy. At this point, it's plain to see that the Obama Administration has no intention of honestly fixing this mess. So it's time now for Congress to act. A good first step would be to appoint a Special Prosecutor with wide power to subpoena Administration officials, and to bring criminal indictments where appropriate. Congress should then begin the process of reforming surveillance law to make absolutely clear that the NSA has no power to conduct warrantless mass surveillance of Americans.

First they came for the terrorists and the foreigners, and no one did anything. Then they came for the drug dealers. Then the tax cheats. Then the journalists. And that's just what we know about. How much worse does it have to get before we say enough is enough?