Subject: The Criminal N.S.A.
Posted by CyberkNight on Mon, 01 Jul 2013 14:06:32 GMT
View Forum Message <> Reply to Message

The twin revelations that telecom carriers have been secretly giving the National Security Agency information about Americans' phone calls, and that the N.S.A. has been capturing e-mail and other private communications from Internet companies as part of a secret program called Prism, have not enraged most Americans. Lulled, perhaps, by the Obama administration's claims that these "modest encroachments on privacy" were approved by Congress and by federal judges, public opinion quickly migrated from shock to "meh."

This view is wrong -- and not only, or even mainly, because of the privacy issues raised by the American Civil Liberties Union and other critics. The two programs violate both the letter and the spirit of federal law. No statute explicitly authorizes mass surveillance. Through a series of legal contortions, the Obama administration has argued that Congress, since 9/11, intended to implicitly authorize mass surveillance. But this strategy mostly consists of wordplay, fear-mongering and a highly selective reading of the law. Americans deserve better from the White House -- and from President Obama, who has seemingly forgotten the constitutional law he once taught.

The administration has defended each of the two secret programs. Let's examine them in turn.

Edward J. Snowden, the former N.S.A. contract employee and whistle-blower, has provided evidence that the government has phone record metadata on all Verizon customers, and probably on every American, going back seven years. This metadata is extremely revealing; investigators mining it might be able to infer whether we have an illness or an addiction, what our religious affiliations and political activities are, and so on.

The law under which the government collected this data, Section 215 of the Patriot Act, allows the F.B.I. to obtain court orders demanding that a person or company produce "tangible things," upon showing reasonable grounds that the things sought are "relevant" to an authorized foreign intelligence investigation. The F.B.I. does not need to demonstrate probable cause that a crime has been committed, or any connection to terrorism.

Even in the fearful time when the Patriot Act was enacted, in October 2001, lawmakers never contemplated that Section 215 would be used for phone metadata, or for mass surveillance of any sort. Representative F. James Sensenbrenner Jr., a Wisconsin Republican and one of the architects of the Patriot Act, and a man not known as a civil libertarian, has said that "Congress intended to allow the intelligence communities to access targeted information for specific investigations." The N.S.A.'s demand for information about every American's phone calls isn't "targeted" at all -- it's a dragnet. "How can every call that every American makes or receives be relevant to a specific investigation?" Mr. Sensenbrenner has asked. The answer is simple: It's not.

The government claims that under Section 215 it may seize all of our phone call information now because it might conceivably be relevant to an investigation at some later date, even if there is no particular reason to believe that any but a tiny fraction of the data collected might possibly be suspicious. That is a shockingly flimsy argument -- any data might be "relevant" to an investigation eventually, if by "eventually" you mean "sometime before the end of time." If all data is "relevant," it makes a mockery of the already shaky concept of relevance.

Let's turn to Prism: the streamlined, electronic seizure of communications from Internet companies. In combination with what we have already learned about the N.S.A.'s access to telecommunications and Internet infrastructure, Prism is further proof that the agency is collecting vast amounts of e-mails and other messages -- including communications to, from and between Americans.

The government justifies Prism under the FISA Amendments Act of 2008. Section 1881a of the act gave the president broad authority to conduct warrantless electronic surveillance. If the attorney general and the director of national intelligence certify that the purpose of the monitoring is to collect foreign intelligence information about any non-American individual or entity not known to be in the United States, the Foreign Intelligence Surveillance Court can require companies to provide access to Americans' international communications. The court does not approve the target or the facilities to be monitored, nor does it assess whether the government is doing enough to minimize the intrusion, correct for collection mistakes and protect privacy. Once the court issues a surveillance order, the government can issue top-secret directives to Internet companies like Google and Facebook to turn over calls, e-mails, video and voice chats, photos, voice-over IP calls (like Skype) and social networking information.

Like the Patriot Act, the FISA Amendments Act gives the government very broad surveillance authority. And yet the Prism program appears to outstrip that authority. In particular, the government "may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."

The government knows that it regularly obtains Americans' protected communications. The Washington Post reported that Prism is designed to produce at least 51 percent confidence in a target's "foreignness" -- as John Oliver of "The Daily Show" put it, "a coin flip plus 1 percent." By turning a blind eye to the fact that 49-plus percent of the communications might be purely among Americans, the N.S.A. has intentionally acquired information it is not allowed to have, even under the terrifyingly broad auspices of the FISA Amendments Act.

Full article: http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html?pagewanted=all&_r=0