WIRED

5 Fun Facts From the Latest NSA Leak

By: Kim Zetter – June 20, 2013

After a brief respite, the *Guardian* newspaper has resumed its publication of leaked NSA documents. The latest round provides a look at the secret rules the government follows for collecting data on U.S. persons.
We found a number of interesting disclosures in two documents released by the newspaper. Among them:

1) The NSA generally destroys communication of U.S. persons that are collected incidental to collecting data on foreign individuals — unless the communication is encrypted, which means that encrypted email and text communications involving U.S. persons that are collected by the NSA in the course of conducting bulk collections would be retained by the agency. It does this as a matter of course, the document appears to say, to further its research and assessment into cracking encryption. The NSA may retain the encrypted communications for "any period of time" during which it might prove to be useful.

Per the document: "In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis."

Furthermore, using the "wrong" encryption program might make you an NSA target. That's because the National Security Agency takes a number of variables into account in determining whether it can target you for surveillance. One indicator that you might be fair game: using "specific types of cryptology or steganography" that are "extensively used by individuals associated with a foreign power or foreign territory."

2) The NSA maintains a massive database of U.S. email addresses and phone numbers. The agency says it does this only to help determine who is a U.S. citizen and therefore make sure that it's not accidentally spying on those people.

Per one of the documents, the NSA "maintains records of telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons. Prior to targeting, a particular telephone number or electronic communications account/address/identifier will be compared against those records in order to ascertain whether NSA has reason to believe that telephone number or electronic communications account/address/identifier is being used by a United States person."

3) The NSA also maintains a database of information incidentally collected from GSM and Home Location Registers to determine when a foreign person being targeted has entered the U.S. According to the document, “These registers receive updates whenever a GSM phone moves into a new service area. Analysis of this HLR information provides a primary indicator of a foreign user of a mobile telephone entering the United States.”

4) When the NSA does pick up purely domestic communications, it can still use or pass the intercepted call or email to the FBI or other federal agencies if there is evidence of a crime or a national security leak. Although the NSA has long been allowed by statute to refer to the FBI information collected in national security investigation if it shows evidence of a crime, this has always been presumed to refer to targeted investigations. But it takes on new meaning in light of what we now know about the kinds of bulk collections the NSA is doing of internet communications, including of U.S. data, and raises the possibility for the government to do pattern analysis to uncover criminal activity on large sets of data.

“When you combine the ability to share evidence of a crime unrelated to foreign intelligence with the … bulk acquisition of every American’s records, you have obvious potential for the use of this to circumvent even ordinary safeguards applying to criminal investigations,” says Julian Sanchez, research fellow at the Cato Institute. “It becomes a completely different story if you’re saying that everyone’s records are in the pool now, and you still have the ability to share information….”

5) If the NSA intercepts data between an attorney and client, it will still be retained, but will be marked for special handling, such that the portion of the communication related to national security is segregated from the rest of the communication. The procedures apply, however, only when the client is known to be under criminal indictment. The rules do not mention what the NSA does if the clients are communicating with their attorneys on civil cases and other legal matters.

A final fun fact: The NSA still uses magnetic tapes.