U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program

7. Juni 2013

By Barton Gellman and Laura Poitras, The Washington Post

The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets, according to a top-secret document obtained by The Washington Post.

The program, code-named PRISM, has not been made public until now. It may be the first of its kind. The NSA prides itself on stealing secrets and breaking codes, and it is accustomed to corporate partnerships that help it divert data traffic or sidestep barriers. But there has never been a Google or Facebook before, and it is unlikely that there are richer troves of valuable intelligence than the ones in Silicon Valley.

Equally unusual is the way the NSA extracts what it wants, according to the document: “Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.”

London’s Guardian newspaper reported Friday that GCHQ, Britain’s equivalent of the NSA, also has been secretly gathering intelligence from the same internet companies through an operation set up by the NSA.

According to documents obtained by The Guardian, PRISM would appear to allow GCHQ to circumvent the formal legal process required in Britain to seek personal material such as emails, photos and videos from an internet company based outside of the country.

PRISM was launched from the ashes of President George W. Bush’s secret program of warrantless domestic surveillance in 2007, after news media disclosures, lawsuits and the Foreign Intelligence Surveillance Court forced the president to look for new authority.

Congress obliged with the Protect America Act in 2007 and the FISA Amendments Act of 2008, which immunized private companies that cooperated voluntarily with U.S. intelligence collection. PRISM recruited its first partner, Microsoft, and began six years of rapidly growing data collection beneath the surface of a roiling national debate on surveillance and privacy. Late last year, when critics in Congress sought changes in the FISA Amendments Act, the only lawmakers who knew about PRISM were bound by oaths of office to hold their tongues.

The court-approved program is focused on foreign communications traffic, which often flows through U.S. servers even when sent from one overseas location to another. Between 2004 and 2007, Bush administration lawyers persuaded federal FISA judges to issue surveillance orders in a fundamentally new form. Until then the government had to show probable cause that a particular “target” and “facility” were both connected to terrorism or espionage.

In four new orders, which remain classified, the court defined massive data sets as “facilities” and agreed to certify periodically that the government had reasonable procedures in place to minimize collection of “U.S. persons” data without a warrant.

In a statement issue late Thursday, Director of National Intelligence James R. Clapper said “information collected under this program is among the most important and valuable foreign intelligence information we collect, and is used to protect our nation from a wide variety of threats. The unauthorized disclosure of information about this important and entirely legal program is reprehensible and risks important protections for the security of Americans.”