New documents expose more NSA programs

Robert Stevens
14 December 2013

New documents published by the *Washington Post* from Edward Snowden, the former National Security Agency (NSA) whistle-blower, reveal that the United States and British governments and their partners made use of cookies placed on computers by Google for state surveillance.

The cookies are known as "GooglePrefIDs". They are files containing a numeric code placed on computers to help the search firm remember users. Many firms use Google's technologies to place adverts, meaning internet users may have PrefIDs on their computer even if they have never visited the search firm's own services such as Gmail or Google+.

Cookies typically do not reveal information such as a user's name and e-mail address, but are able to identify a particular browser. On this basis, explains the *Post*, "the NSA is able to single out an individual's communications among the sea of Internet data in order to send out software that can hack that person's computer."

The newspaper said it was not clear how the NSA obtained internet users' cookies or if Google "cooperates in these programs, but other documents reviewed by the *Post* indicate that cookie information is among the data NSA can obtain with a Foreign Intelligence Surveillance Act order. If the NSA gets the data that way, the companies know and are legally compelled to assist."

The documents refer to the NSA's Special Source Operations (SSO), previously described by Snowden as the "crown jewel" of the NSA. It manages surveillance programs that involve collaboration with corporate communication providers.

The *Post* notes that one of the slides "indicates that SSO was sharing information containing 'logins, cookies, and GooglePREFID' with another NSA division called Tailored Access Operations, which engages in offensive hacking operations. SSO also shares the information with the British intelligence agency GCHQ."

New documents also reveal that the NSA is using commercially gathered information to help it locate mobile devices globally. Many apps running on iPhones and Android devices, as well as the Apple and Google operating systems, track the location of each device. A program named HAPPYFOOT allows "the NSA to map Internet addresses to physical locations more precisely than is possible with traditional Internet geolocation services," one of the slides reveals.

Other documents disclosed by Snowden and published by the *Guardian* earlier this week reveal that the NSA and GCHQ have the ability to infiltrate tens of millions of people, via the massive online communities, who play online games such as *World of Warcraft* and *Second Life*. The *Guardian* notes, "In May 2007, the then-chief operating officer of Second Life gave a 'brown-bag lunch' address at the NSA explaining how his game gave the government 'the opportunity to understand the motivation, context and consequent behaviours of non-Americans through observation, without leaving US soil'."

Britain's GCHQ had made a "vigorous effort" to exploit games, including "exploitation modules" against Xbox Live and *World of Warcraft*, said one document. Another memo noted that among *World of Warcraft* 's active subscribers were "telecom engineers, embassy drivers, scientists, the military and other intelligence agencies."

The new documents were released even as the European Union agreed to allow Snowden to give evidence by video link to its committee on civil liberties, justice and home affairs (LIBE). Snowden had indicated in July that he would be prepared to give evidence to the EU.

The move by the EU to question Snowden reveals the extent of concern in European ruling circles as to the massive extent of the unrestrained spying organised by the NSA, GCHQ and their other "Five Eyes" partners, Canada, Australia and New Zealand. Their concern is not that their own populations are under constant and growing surveillance, but that Snowden has also confirmed that the NSA and GCHQ systematically spy on the governments of their main imperialist rivals in Europe and internationally.

According to *Spiegel Online*, "Representatives from different groups in the European Parliament have already compiled more than 20 questions for Snowden. These range from 'How are you?' and 'Can we help you?' to a detailed exploration of whether and how European intelligence agencies also collect private data."

The questioning is to go ahead despite moves to block it by conservatives in the European People's Party (EPP), the association of Europe's Christian-Democratic and conservative parties.

Timothy Kirkhope, a Member of the European Parliament for the UK's Conservative Party, which is not part of the EPP, also attempted to prevent Snowden from appearing by sending a letter to all members of the LIBE committee. He said the proposed evidence session was "a provocative act that would enable [Snowden] to further endanger security around Europe and beyond."

A further indication of the disquiet in ruling circles is the open letter to the Obama government and the US Congress from some of the world's main technology firms—Apple, Google, Microsoft, Facebook, Yahoo, LinkedIn, Twitter and AOL. The letter states, "The balance in many countries has tipped too far in favour of the state and away from the rights of the individual—rights that are enshrined in our constitution." It adds, "This undermines the freedoms we all cherish. It's time for change."

A major factor in the concerns of Google, Microsoft, et al. is the impact of the revelations on their profitability and even their continued existence. Brad Smith, Microsoft's general counsel, said, "People won't use technology they don't trust. Governments have put this trust at risk, and governments need to help restore it."

Even as the EU is putting on a show of opposition to the mass spying of the NSA and GCHQ, its component governments continue to build up their own vast surveillance operations against their populations. On Wednesday the French parliament passed legislation, Article 13 of a new military programming law, allowing its intelligence and anti-terrorist agencies, as well as a number of government ministries, full powers to directly monitor internet users who use computer, tablets or smartphones, in real time without any prior authorisation. The defence, interior, economy, tax and finance ministries will all be able to snoop on all "electronic and digital communications."

For their part the US and the British Conservative/Liberal Democrat governments have both refused to back down.

The head of the NSA, General Keith Alexander, testifying at a Senate Judiciary Committee hearing Wednesday, defended its activities to the hilt. Claiming that global threats against the US are growing, in Iraq and Syria in particular, he declared, "There is no other way that we know of to connect the dots... Taking these programs off the table is absolutely not the thing to do."

In Britain, the government continues to demand Snowden's persecution, while also seeking the prosecution of the *Guardian*.

Those responsible for the UK's spying network are being protected from being held to any account. On Wednesday it was reported that the request by Parliament's Home Affairs committee to question Andrew Parker, the head of the MI5 domestic spying organisation, next week was rejected by Home Secretary Teresa May. The committee had requested he appear to justify his false claim that the *Guardian* has put national security at risk by publishing in redacted form a small percentage of the Snowden documents.

Prime Minister David Cameron also rejected a request that Kim Darroch, the national security adviser, give evidence to the committee's inquiry into counterterrorism. Cameron wrote that "it was not a good idea" for Darroch to appear, as Darroch's role was to provide him and the National Security Council with private advice, and an appearance would "set a difficult precedent."