NSA collects nearly 200 million phone text messages a day

Patrick O'Connor
17 January 2014

Britain's *Guardian* and Channel Four television news programme yesterday released documents from former National Security Agency (NSA) contractor turned whistleblower Edward Snowden detailing yet another mass US surveillance operation. Under the codename Dishfire, the NSA has been intercepting and permanently storing the metadata and content of billions of mobile phone text messages sent by ordinary people around the world.

The latest material from Snowden has been published at the same time as President Barack Obama is attempting to legitimise ongoing domestic surveillance of US citizens, under the guise of intelligence "reform" (see: "Obama's NSA 'reform' defends illegal spying").

The details of the ongoing Dishfire operation further expose the Obama administration's empty rhetoric about respecting the rule of law and the rights of the people. The internal NSA PowerPoint slide outlining Dishfire's capacities makes clear from the very beginning that it is aimed not at intercepting the communications of specific individuals deemed terrorists or security threats, but rather at collecting the text messages of everyone in every country around the world.

The slides, dated June 2011, begin with a series of statistics, including: 77 percent of the world's population has a mobile phone subscription, text messages were "still king of mobile messaging", and the "typical mobile subscriber sends and receives more SMS text messages than telephone calls."

The document's banner slide features the following: "SMS Text Messages: A Goldmine to Exploit."

In April 2011, the slideshow detailed, the NSA collected and stored 194.2 million text messages a day. This rate of interception has likely increased significantly in the past two and a half years, given the value of the program to the US intelligence agencies and their international counterparts in the "Five Eyes" alliance (Britain, Australia, Canada and New Zealand).

One of the leaked NSA documents reportedly included a warning from a Dishfire operative that the program was being "overwhelmed" by demand, and asked analysts to limit their searches to no more than 1,800 phone numbers at a time.

The slideshow published by the *Guardian* includes a Venn diagram for the intercepted text messages, showing "metadata" in one circle, "message content" in another, and a smiley face in the overlapping area. Metadata and content together, the document declared, "leads to analytic gems", with the "rich data set awaiting exploitation."

The NSA's sweeping violation of basic rights is made clear in the final slide of the document, which explained that the nearly 200 million messages intercepted every day included missed calls, SIM card changes, roaming information (from mobile phone companies texting customers when they cross into another country), and travel ("itinerary including multiple flights" and "changes: cancellations, reschedules, delays").

Moreover, the NSA was able to pick up electronic business cards (including images that could be extracted) and geocoordinates, including "requests by people for route info", "setting up meetings at a location", and "tracking information." Finally, the document continued, Dishfire can "track financial information", monitor money transfers, and "correlate credit cards to individuals."

According to the *Guardian*, the leaked documents "suggest" that "communications from US phone numbers were removed (or 'minimized') from the database." This likely counts for little—previously

leaked documents from Edward Snowden made clear the contempt with which senior political and intelligence figures held the American people and their constitutional rights.

There are no restrictions whatsoever placed on the interception of phone messages of non-American nationals, and the sharing of that intelligence with Washington's allies. This has been used as another way of circumventing domestic laws barring or limiting surveillance by the "Five Eyes" members of their own citizens. Both the *Guardian* and Channel Four detailed the way in which the British counterpart to the NSA, Government Communications Headquarters (GCHQ), used Dishfire to collect and examine British citizens' text messages.

A leaked GCHQ document from May 2008 informed analysts: "Dishfire collects pretty much everything it can… Using Dishfire is really quite simple. Enter your [telephone] numbers, fill in the rest of the query form and off you go."

The GCHQ memo added: "DISHFIRE contains a large volume of *unselected* SMS traffic… it is possible to examine the content of messages sent months or even years *before* the target was known to be of interest" (original emphasis).

It explained that the NSA program was "especially useful for untargeted and unwarranted UK numbers"—in other words it could be used to avoid the need for warrants and allowed for sweeping dragnets of the population, rather than targeting specific or selected individuals. The GCHQ's exploitation of Dishfire was undoubtedly replicated by the intelligence agencies of Australia, New Zealand, and Canada, as well as the US, against their own citizens.