New documents detail NSA surveillance of Yahoo

Thomas Gaist
13 September 2014

A trove of some 1,500 documents released Thursday by Yahoo Inc. shed new light on the US government's warrantless electronic data mining programs, which have targeted Yahoo users for years.

The documents cover 2008 rulings by the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court Review (FISCR), a secret appeals court established to review FISC decisions. Large sections of the documents will remain "sealed and classified," according to a top Yahoo official.

Rejecting Yahoo's challenges to the warrantless surveillance, the FISC ruled in 2008 that "there is a foreign intelligence exception" to Fourth Amendment protections against warrantless spying, the documents show. The court held that provisions in the Protect America Act (PAA) of 2007 authorized the National Security Agency (NSA) to conduct warrantless surveillance of the communications of American citizens.

Reviewing the ruling in August of 2008, the FISC-R affirmed that warrantless electronic surveillance does not violate the Fourth Amendment as long as it is carried out for "foreign intelligence" purposes. The FISC-R cited previous US Supreme Court decisions, saying they had authorized the US government to ignore Fourth Amendment protections under exceptional conditions of "special needs," such as those arising from the "global war on terrorism."

In a statement published Thursday in response to the Yahoo releases, Director of National Intelligence (DNI) James Clapper defended the FISC rulings, arguing that provisions in the PAA empowered the NSA to spy on targets "reasonably believed" to possess "foreign intelligence information."

DNI Clapper bluntly asserted that "incidental collection" of data from US persons associated with such operations does not violate the Fourth Amendment, even if the targets are located in the US.

"Any incidental acquisition of the communications of non-targeted persons located in the United States and of non-targeted US persons, wherever they may be located, is also reasonable under the Fourth Amendment," Clapper wrote.

Behind the convoluted pseudo-legal rationales promulgated by the intelligence bureaucracy and secret surveillance courts—including "incidental collection," "special needs," and "foreign intelligence exceptions," etc.—the underlying reality is that the US government spies on whomever it wants, collects as much data from as many sources as possible, and does so in direct violation of core democratic rights protected by the US Constitution. As the NSA's own documents make clear, the agency is guided by a maximalist "collection posture" defined by six main principles: "Collect it All; Process it All; Exploit it All; Partner it All; Sniff it All; Know it All."

The US government began developing its mass warrantless surveillance techniques years before the passage of the surveillance legislation—the PAA of 2007 and the FISA Amendments Act of 2008—cited by the FISC in defense of the spying. Starting in 2005, the US launched the so-called Real Time Regional Gateway (RTRG) program, which sought to collect and analyze all electronic communications produced inside Iraq.

RTRG became the model for PRISM, the NSA's primary data mining program. Yahoo, Google, Facebook, AOL, Apple, Microsoft, Skype, YouTube, and other major tech and communications companies were revealed as active collaborators in the PRISM program by the 2013 leaks from former NSA contractor

Edward Snowden.

According to one of the NSA slides leaked by Snowden, “98 percent of PRISM production is based on Yahoo, Google and Microsoft.” Another slide described PRISM as “the number one source of raw intelligence used for NSA analytic reports,” saying that it collects 91 percent of Internet data acquired in the course of NSA operations.

Under PRISM, NSA analysts can access every type of data hosted by these companies, including email, chat, webcams, web-based telephones, social media data, and numerous other forms. NSA agents can spy on these communications in real time and troll through user archives at will.

In its official statement released Thursday, Yahoo sought to portray itself as a principled opponent of the warrantless surveillance.

“We refused to comply with what we viewed as unconstitutional and overbroad surveillance and challenged the US Government’s authority … we had to fight every step of the way to challenge the US government’s surveillance efforts,” Yahoo general counsel Ron Bell wrote.

Such claims, made in one form or another by all the major tech firms involved, are part of a public relations campaign mounted by the corporations to conceal their close relations with the US government and its surveillance apparatus. Despite their posturing, Yahoo and the other tech giants have transferred huge amounts of data to the government for a period spanning years and actively facilitated government efforts to penetrate their information systems.

Relations between the NSA and Microsoft highlight this contradiction between the companies’ rhetorical and legal maneuvers, on the one hand, and their actual actions when it comes to customers’ data.

Like Yahoo, Microsoft has challenged US government surveillance powers in court, yet it has simultaneously worked together with the NSA to enable the agency to defeat the company’s own encryption systems, and to grant the FBI and NSA direct access to the SkyDrive file-hosting service used by more than 250 million people worldwide. Microsoft’s acquisition of Skype massively accelerated NSA efforts to spy on the communications platform’s hundreds of millions of users, Snowden-leaked documents show.