

Obama administration had secret court lift restrictions on domestic spying

Andre Damon
9 September 2013

In 2011, the Obama administration had a secret surveillance court authorize the NSA to deliberately target the emails and phone calls of Americans to be read and listened to, the *Washington Post* reported Sunday, citing recently declassified documents.

In 2008, the Foreign Intelligence Surveillance Court imposed a nominal ban on searches for the communications of US citizens and residents by the NSA. However, the Obama Administration succeeded in having the court overturn the ruling in 2011. This move was made without any public or congressional debate or discussion.

The ruling also extended the amount of time that the NSA is allowed to retain data it collected to six years, up from five years.

While the government claims that it does not specifically target US citizens, the wording of the ruling effectively allows the NSA to collect all communications that originated in or were routed through the US.

The recently declassified 2011 opinion allows the “NSA to query the vast majority of its Section 702 collection using United States-Person identifiers,” meaning that the NSA is allowed to search directly for the email addresses and phone numbers of US citizens and residents.

Gregory T. Nojeim, senior counsel at the Center for Democracy and Technology, told the *Washington Post*, “The government says, ‘We’re not targeting U.S. persons.’ But then they never say, ‘We turn around and deliberately search for Americans’ records in what we took from the wire.’ That, to me, is not so different from targeting Americans at the outset.”

Alex Joel, civil liberties protection officer at the Office of the Director of National Intelligence (ODNI), told the *Washington Post* that the court banned such

searches wholesale in 2008 in order “to remain consistent with NSA policies and procedures that NSA applied to other authorized collection activities.” Publicly, the NSA has claimed that it does not monitor the communications of US citizens.

In remarks to the *Washington Post*, however, Robert S. Litt, general counsel at the ODNI, admitted, “We did ask the court” to lift the ban on US domestic spying. “We wanted to be able to do it,” he said, referring to the searches through US communications.

The *Washington Post*’s story came the day after German magazine *Der Spiegel* reported, based on secret NSA documents, that the NSA has whole divisions dedicated to hacking into smartphones and is able to get into Apple’s iOS, Google’s Android, and Blackberry devices.

The documents also revealed that in 2010 the NSA succeeded in breaking through the encryption of Blackberry SMS messages, a development to which a top-secret memo responded with, “Champagne!” The NSA is also able to access the Blackberry mail system, despite the company’s insistence on the system’s security.

Hacking smartphones is just one of the tools in the NSA’s arsenal, ranging from the bulk collection of unencrypted data from fiber optic cables to the exploitation of secret electronic backdoors, to more conventional surveillance techniques.

These latest revelations come in the aftermath of the report Thursday by the *Guardian* newspaper in Britain that the NSA employs an enormous \$250 million-per-year program to systematically break encryption, exploit software manufacturers’ backdoors, and hack individual computers.

The program, which is ten times larger than the PRISM program exposed earlier this year, includes the

deliberate, “brute force” breaking of encryption by supercomputers, and includes working to “covertly influence” technology companies to make their product designs easier to exploit.

“For the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet encryption technologies,” noted a 2010 British intelligence document quoted by the *Guardian*. “Vast amounts of encrypted internet data which have up till now been discarded are now exploitable.”



To contact the WSWWS and the
Socialist Equality Party visit:

wsws.org/contact