

Obama-appointed civil liberties board upholds mass internet data collection by NSA

Thomas Gaist
3 July 2014

The five-member Privacy and Civil Liberties Oversight Board (PCLOB), appointed by President Obama, released a report this week upholding core components of the US government's surveillance apparatus. Specifically, the panel affirmed the constitutionality of operations conducted under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, which authorizes PRISM and other bulk electronic data collection operations run by the National Security Agency (NSA).

The report gives a bogus stamp of legitimacy to some of the most aggressive and criminal surveillance operations carried out by the US government. The surveillance operations covered by the report are responsible for mass spying on an astonishing scale.

The PCLOB document, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," found that surveillance conducted under Section 702 does not violate the Fourth Amendment and that "minimization" procedures undertaken by the intelligence agencies are generally sufficient to protect the constitutional rights of US citizens. The programs can continue, the PCLOB held, so long as the government deems them useful for "foreign intelligence" purposes.

"Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence," PCLOB wrote.

The PCLOB claimed that data acquisition by the NSA under PRISM and Section 702 operations complies with the "totality of circumstances standard for reasonableness under the Fourth Amendment." According to this concept, a police officer may conduct a search without receiving a warrant from a judge if doing so is reasonable under existing circumstances.

An officer may stop and search an automobile seen driving recklessly, for instance, if there are reasons to suspect the driver is drunk or engaging in criminal activity.

This legal pretext is now being used to rationalize dragnet surveillance programs that collect the personal information and communications of tens and hundreds millions of people.

The operations covered by the report have grown rapidly since the promulgation of the "global war on terrorism" in 2001. Section 702, passed by Congress as part of the 2008 FISA Amendments Act, institutionalized surveillance procedures that had already been developed by the executive branch under the George W Bush administration after 9/11, in the form of the Terrorist Surveillance Program (TSP), initially called the President's Surveillance Program.

When a series of media reports exposed the use of warrantless wiretapping by the Bush administration under the TSP, Congress moved to legalize the spying after the fact, passing the 2008 FISA legislation. According to the PCLOB report, the passage of Section 702 allowed for "a dramatic increase in the number of people who can realistically be targeted," above and beyond the "traditional" FISA process.

Under Section 702, the US Attorney General and Director of National Intelligence are empowered to order surveillance of targets they "reasonably believe" to be non-US persons, and to do so by compelling service providers to hand over any data that is presumed relevant. The US government issues written orders to the telecommunications companies containing "selectors" and "tasks," which specify email addresses, user names, etc. The providers are then required by law to furnish all data associated with the selectors submitted by the government.

Elizabeth Goitein, director at the Liberty and National Security Program of the Brennan Center for Justice, rejected the findings of the PCLOB, writing, “The collection of Americans’ phone calls and e-mails without a warrant is unconstitutional, regardless of whether they are communicating with their next-door neighbor or a suspected terrorist overseas...The board’s recommendation would leave in place the government’s ability to spy on its citizens—along with their friends, family members, and partners overseas—without any suspicion of wrongdoing.”

While the PCLOB repeats the standard line of the government that the purpose of the surveillance is “monitoring terrorist networks,” in reality the surveillance programs covered in the report are collecting data produced by ordinary people. With Section 702 as its legal basis, the NSA’s PRISM program taps directly into fiber optic cables and extracts data from servers run by all the main American telecommunications and Internet companies, including Google, Facebook, Microsoft, Apple and others, sucking up nearly every type of communications data produced by internet and telephone users.

The PCLOB issued a previous report in January of this year finding that collection of US telephone metadata under Section 215 of the Patriot Act violates the Fourth Amendment. The Obama administration disagreed with the finding and has continued these operations, with the entirely formal change that the NSA will now submit data demands to the companies rather than storing US telephone metadata on its own servers.

The PCLOB report offered a series of recommendations on the basis of its investigation of Section 702, which it said were “designed to put the program more comfortably into the sphere of reasonableness.” These include minor revisions to the intelligence agencies’ “minimization” procedures, periodic reassessment of technologies using communications filters, and the issuance of written statements by the NSA specifying why particular selectors have “foreign intelligence value.”

These new “safeguards” proposed by the PCLOB amount to insignificant modifications of the surveillance machinery, and are intended to whitewash programs based on massive and systematic violation of the US Constitution and Bill of Rights.

Obama’s “reform panel” has served its purpose: after making initial criticisms of one aspect of the NSA surveillance, it has given virtually unqualified approval to programs that are among the most massive and indiscriminate being run by the government, and which collect huge reams of personal data from US and non-US persons on a daily basis without warrants.



To contact the WSWWS and the Socialist Equality Party visit:

wsws.org/contact