

US Court of Appeals finds NSA phone data collection is illegal

Ed Hightower
8 May 2015

On Thursday, the US Court of Appeals for the Second Circuit ruled that a key provision of the USA Patriot Act does not provide a legal justification of the National Security Agency's bulk telephone metadata collection program, making that program unlawful. The court overturned a 2013 ruling in the government's favor.

The Court of Appeals has remanded the case, *American Civil Liberties Union v. Clapper*, for further proceedings at the district court level. Thursday's ruling denied the plaintiffs' request for a preliminary injunction that would have halted the spying program until the case was decided on the merits. Thus, the practical significance of the ruling is essentially nil.

At the same time there are profound political implications for Thursday's court opinion. It is not every day that the second highest court in the United States issues a 97-page legal memorandum calling the NSA's flagship domestic spying program what it is: blatant illegality on a monumental scale.

Officially, the court declined to review the constitutional claims that the warrantless data collection violated the plaintiffs' rights of free association and rights against unwarranted searches and seizures. Instead, the court only considered whether the NSA program had a legitimate statutory basis in the Patriot Act and its legal predecessors.

The court's findings about the telephone metadata program speak volumes about the criminality that prevails at the highest levels of state.

The opinion notes that the public first learned about the NSA's telephone metadata program on June 5, 2013, when the *Guardian* published a Foreign Intelligence Surveillance Court (FISC) order leaked by former government contractor Edward Snowden, which directed telecom giant Verizon Business Network

Services, Inc. to give the NSA "on an ongoing daily basis. .. all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."

The NSA has been collecting telephone metadata information in bulk under § 215 of the USA PATRIOT Act, since at least May 2006, when the FISC issued its "Primary Order" requiring production of "all call detail records or 'telephony metadata' created by [redacted]. .. , includ[ing] comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number[s], communications device identifier[s], etc.), trunk identifier, and time and duration of call."

The program, and the FISC order authorizing it, have been renewed 41 times since May 2006 (FISC orders must be reissued every 90 days). The current authorization was issued on February 26, 2015 and expires on June 1, 2015. Section 215 of the Patriot Act will also expire on June 1.

American Civil Liberties Union v. Clapper concerns a FISC order that requires Verizon "to produce call detail records, every day, on *all* telephone calls made through its systems or using its services where one or both ends of the call are located in the United States."

The government's arguments were riddled with internal inconsistencies. To cite one, government attorneys disputed any characterization of the telephone metadata program as collecting "virtually all telephony metadata" associated with calls made or received in the United States, but the same attorneys never argued that Verizon is the only telephone service provider subject to such a FISC order.

The key issue in Thursday's opinion was the specific

language in § 215 which limits the issuance of FISC orders to instances where there exist “reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation ... to obtain intelligence information not concerning a United States person or to protect against international terrorism ...”

Government lawyers supporting the NSA telephone metadata program made the absurd and chilling argument that all of the seized information from essentially all persons in the US, all of the time, are *relevant* if they merely lead to improvements in databases or collection techniques that *eventually* aid in later, as yet unanticipated terror investigations. By the same logic, governmental placement of video cameras inside of every US household would be *relevant* to any number of criminal investigations.

The Court of Appeals took the government to task on this point, if only verbally:

“Thus, the government takes the position that the metadata collected—a vast amount of which does not contain directly ‘relevant’ information, as the government concedes—are nevertheless ‘relevant’ because they may allow the NSA, at some unknown time in the future, utilizing its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information that *is* relevant.”

And later:

“The overwhelming bulk of the metadata collected by the telephone metadata program, as the government itself concedes, concerns ... individuals who are not targets of an investigation or suspected of engaging in any crime whatsoever, and who are not even suspected of having any contacts with any such targets or suspects. Their records are sought solely to build a repository for the future application of the investigative techniques upon which the program relies.”

For all its sneering at the government’s farcical, if Orwellian, lines of argument in favor of omnipresent surveillance, the Court of Appeals took as a given the legitimacy of the “war on terror” and the overarching concern for “national security.” It suggested that balancing the inalienable rights enshrined in the US Constitution with the requirements of a police state is a task best undertaken by Congress and the president, who are at least nominally accountable to the population by way of the ballot box.

As the court put it:

“Congress is better positioned than the courts to understand and balance the intricacies and competing concerns involved in protecting our national security, and to pass judgment on the value of the telephone metadata program as a counterterrorism tool.”

This is nothing more than a call for a more robust pseudo-legal foundation for dictatorial forms of rule.

For its part, three weeks before the expiration of Section 215, Congress has yet to arrive at a bill that would extend or modify the warrantless telephone metadata collection program. Whatever form such legislation may take, it will pose no threat to the military-intelligence apparatus.



To contact the WSWWS and the Socialist Equality Party visit:

wsws.org/contact