US drug enforcement agency acknowledges longstanding warrantless wiretapping program

Thomas Gaist
19 January 2015

The US Drug Enforcement Administration (DEA) carried out mass surveillance of telephone calls over a period of more than a decade, compiling huge quantities of data through warrantless and dragnet-style spying operations, according to information included in an official declaration submitted by the agency to a federal court.

The DEA declaration was submitted last week in the case of *United States v. Hassanshahi*. Shantia Hassanshahi was seized and his personal electronic devices forcibly taken by US government agents in California in January 2012. The government subsequently claimed that evidence taken from Hassanshahi's laptop proves that he was engaged in illegal business dealings involving the sale of civilian energy technology to Iran.

The DEA yielded up information about its warrantless wiretapping operations to the court only after the judge insisted that the agency reveal at least "the contours" of the "mysterious law enforcement database" in which US government agents found Hassanshahi's number.

The DEA database contains "telecommunications metadata obtained from United States telecommunications service providers," requisitioned from the companies through "administrative subpoenas," according to a declaration was signed by DEA Assistant Special Agent in Charge Robert Patterson and submitted to judge Rudolph Contreras of the US District Court for the District of Columbia. The targeted communications included outbound overseas calls originating in the US.

Patterson's statement asserts that the powers granted to the DEA by the 1988 Controlled Substances Act authorize the DEA to issue unilateral administrative decrees demanding data from the telecommunications corporations. Administrative decrees differ from ordinary subpoenas and warrants in that they are not subject to any direct judicial oversight, and are issued by the agency instead of by a court.

The DEA initiated large-scale telephone data collection from targets on US territory sometime during the 1990s, according to unnamed sources cited by the *Wall Street Journal*.

The DEA has apparently been free for years to conduct this dragnet spying without any accountability or oversight. While the DEA's spying operations included having unhindered access to AT&T's global communications network until at least 2013, the DEA did not have to submit its activities for approval to any judicial body. It did not even seek authorization from the Foreign Intelligence Surveillance Court.

Instead, the DEA essentially re-interpreted the Controlled Substances Act, unilaterally imposing its own interpretation that authorized warrantless domestic spying. The US government "has used strained legal theories to justify the surveillance of millions of innocent Americans," ACLU attorney Patrick Toomey said.

The DEA's bulk surveillance blatantly violates the Fourth Amendment to the US Bill of Rights, which protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and prohibits the government from carrying out searches and seizures without a judicial warrant.

The DEA engaged in "bulk collection of records from service providers," doing so "without judicial review or

independent oversight," US Senator Patrick Leahy acknowledged in a March 2014 letter that was unknown to the public until Friday.

The DEA database is "likely unconstitutional" and "functions entirely like the NSA [National Security Agency] database," said the defense attorney for Hassanshahi, Saied Kashani. The DEA "used it to gather routinely and monthly records of every phone call placed by every American [to someone] overseas, and then they're making this information available secretly to every other government agency," he added.

The Justice Department has claimed that the program was ended and all of its data was deleted as of September 2013. However, when asked by reporters whether the DEA maintains any other bulk data collection programs, a DOJ spokesperson refused to answer.

DEA spying was first brought to light when documents leaked in 2013 exposed the agency's so-called "Hemisphere Project." Under this program, run jointly by the DEA and the White House Office of National Drug Control Policy, US government agents enjoyed direct and unlimited access to AT&T's network since at least 2007.

The DEA's archives of personal electronic data contained some 4 billion call detail records (CDRs) stretching back to 1987, including location data, the leaked documents showed.

The DEA Internet Connective Endeavor (DICE) catalogues more than 1 billion phone records obtained by DEA wiretapping operations. Through DICE, the DEA distributes wiretap data to a network of more than 10,000 police officials throughout all levels of government. DEA agents are able to search the massive database, which is updated in near real time to include all calls placed up to an hour before the inquiry is made.

The US government paid AT&T to embed its own employees with DEA units and special police teams at the local level, the *New York Times* reported in 2013.

The DEA also launched criminal prosecutions based on surveillance data disseminated throughout the federal agencies by the Special Operations Division (SOD). In order to conceal the extent of domestic spying, US law enforcement agencies trained their personnel to invent pretexts for targeting individuals, using a technique called "parallel construction" to deceive judges and juries.

The DEA spying revelations are only the latest proof that multiple agencies of the federal government are deeply mired in illegal domestic spying operations. A top secret document released last week showed that the FBI, while it is heavily involved in the NSA spy programs and effectively co-manages the NSA's targeting lists, is exploiting its own sources of communications data independently of the NSA.