US judge slams surveillance requests as “repugnant to the Fourth Amendment”

Thomas Gaist
21 March 2014

Federal Magistrate Judge John M. Facciola denied a US government request earlier this month for a search and seizure warrant, targeting electronic data stored on Apple Inc. property.

Facciola’s order, issued on March 7, 2014, rejected what it described as only the latest in a series of “overbroad search and seizure requests,” and “unconstitutional warrant applications” submitted by the US government to the US District Court for the District of Columbia. Facciola referred to the virtually unlimited warrant request submitted by the Justice Department as “repugnant to the Fourth Amendment.”

The surveillance request sought information in relation to a “kickback investigation” of a defense contractor, details about which remain secret.

It is significant, however, that the surveillance request denied by Facciola relates to a criminal investigation, unrelated to terrorism. This demonstrates that the use by the Obama administration of blanket warrants enabling them to seize all information on a person's Internet accounts is not limited to terrorism, as is frequently claimed, but is part of a program of general mass illegal spying on the American people.

Facciola’s ruling states in no uncertain terms that the Obama administration has aggressively and repeatedly sought expansive, unconstitutional warrants, ignoring the court’s insistence for specific, narrowly targeted surveillance requests.

“The government continues to submit overly broad warrants and makes no effort to balance the law enforcement interest against the obvious expectation of privacy email account holders have in their communications…The government continues to ask for all electronically stored information in email accounts, irrespective of the relevance to the investigation,” wrote Judge Facciola.

As stated in the ruling, the surveillance requests submitted to the court by the US government sought the following comprehensive, virtually limitless list of information about the target: “All records or other information stored by an individual using each account, including address books, contact and buddy lists, pictures, and files… All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifies, records of session times and durations, the date on which each account was created, the length of service, the types of service utilized, the Internet Protocol (IP) address used to register each account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means of payment (including any credit or bank account number).”

Responding to these all-encompassing warrant requests, Judge Facciola ruled that evidence of probable cause was necessary for each specific item sought by the government.

“This Court is increasingly concerned about the government’s applications for search warrants for electronic data. In essence, its applications ask for the entire universe of information tied to a particular account, even if it has established probable cause only for certain information,” Facciola wrote.

“It is the Court’s duty to reject any applications for search warrants where the standard of probable cause has not been met… To follow the dictates of the Fourth Amendment and to avoid issuing a general warrant, a court must be careful to ensure that probable cause exists to seize each item specified in the warrant application… Any search of an electronic source has the potential to unearth tens or hundreds of thousands of

individual documents, pictures, movies, or other constitutionally protected content."

Facciola also noted in the ruling that the government never reported the length of time it would keep the data, or whether it planned to destroy the data at any point.

Facciola's ruling represents a reversal from a previous ruling, in which a Kansas judge allowed the government to conduct such unlimited searches of Yahoo accounts.

Facciola's frustration at receiving repeated requests for opened-ended warrants against surveillance targets only underscores the aggressiveness of the Obama administration in expanding the blatantly unconstitutional surveillance operations. Under the Obama surveillance regime, mere suspicion by the government is grounds for sweeping up every scrap of information about an individual.

The Privacy and Civil Liberties Oversight Board (PCLOB), a body appointed by the executive branch to propose "reforms" for the surveillance state, held a hearing Wednesday on Section 702 of the Foreign Intelligence Surveillance Act of 2008 (FISA), which has been used to authorize mass spying on populations around the world.

The hearing exposed the complicity of the major tech companies in the illegal surveillance. Asked during the hearing whether the techs knew about and collaborated with the NSA's PRISM surveillance program, NSA general counsel Rajesh De replied, "Yes."

A PCLOB member asked for confirmation, saying, "So [tech companies] know that their data is being obtained?" De reaffirmed, "They would have received legal process in order to assist the government."

De's testimony exposed the lies of Microsoft, Yahoo, Google, Facebook, AOL and Apple, which all issued denials of any knowledge about PRISM in response to the leaks about NSA spying by Edward Snowden. Facebook, for instance, released a statement claiming that it does not "provide any government organization with direct access to Facebook servers." In fact, Facebook and the other tech giants maintain close working relations with the intelligence and security agencies.

In testimony, De and his deputy Brad Wiegmann rejected the privacy board's advice that the agency limit its data mining to specific targets approved by specific warrants.

"If you have to go back to court every time you look at the information in your custody, you can imagine that would be quite burdensome," said Wiegmann.

De further said on the topic, "That information is at the government's disposal to review in the first instance."

As these statements indicate, the intelligence establishment rejects any restrictions on their prerogative to spy on every aspect of citizens lives at will, even the entirely cosmetic regulations proposed by the Obama administration-appointed PCLOB.