Office of the Inspector General
U.S. Department of Justice

A Review of the FBI's Use of Pen Register and Trap and Trace Devices Under the Foreign Intelligence Surveillance Act in 2007 through 2009

Executive Summary

Oversight and Review Division 15-06 June 2015

EXECUTIVE SUMMARY

This Executive Summary provides a brief overview of the results of the Department of Justice (Department or DOJ) Office of the Inspector General's (OIG) review of the Federal Bureau of Investigation's (FBI) use of pen registers and trap and trace devices under the Foreign Intelligence Surveillance Act (FISA) during calendar years 2007 through 2009. We completed a draft of this report in February 2014. At that time, we provided the draft report to the Department, the FBI, and the Intelligence Community to conduct factual accuracy and classification reviews. In May 2014, we circulated an updated draft report that reflected minor revisions made in response to the factual accuracy comments we received. We did not receive the final results of the classification reviews until April 2015. We provided the full classified version of this report to DOJ leadership offices, the FBI, the Office of the Director of National Intelligence, and appropriately cleared members of the relevant congressional oversight and intelligence committees.

Pen registers and trap and trace devices have long been used for federal law enforcement purposes.[1] The federal criminal pen register statute was enacted in 1986 and, in 1998, Congress amended FISA to authorize the government to use pen registers to collect foreign intelligence information in national security investigations after obtaining an order from the Foreign Intelligence Surveillance Court (FISA Court). Pen registers record telephone numbers, e-mail addresses, and other dialing, routing, addressing, or signaling information that is transmitted by instruments or facilities – such as telephones or computers – that carry wire or electronic communications. Trap and trace devices record similar information that is received by such instruments or facilities. The information that is recorded is commonly referred to as "metadata" and does not include the contents of communications, which pen registers and trap and trace devices are statutorily prohibited from recording.

In our classified report, we describe the process that the FBI and the Department follow to file applications with the FISA Court for pen register orders and extensions of orders, and examine the FBI's use of pen register authority from 2007 through 2009. We describe the different types of pen registers that were used and the variety of information that was collected, as well as some of the technological and legal issues the Department and FBI faced with particular uses of pen register authority. We also describe the investigative circumstances under which the authority is generally used and trends in its use. The FBI and the Intelligence Community determined that much of this information is classified or "for official use only," and therefore we cannot include it in this Executive Summary.

[1] We use the term "pen register" in this Executive Summary to refer to pen registers and trap and trace devices. Any distinction between the two will be expressly noted where relevant.

Our classified report also describes the FBI's practices for storing and handling pen register information, most of which have remained substantially unchanged since our 2007-2009 review period, and it provides an overview of the compliance process and a summary of the compliance incidents involving the use of pen register authority that occurred from 2007 through 2009. Our classified report also includes several findings, only one of which we can describe in this unclassified Executive Summary.

Methodology of the OIG Investigation

We initiated this review to examine the process to obtain a FISA Court order authorizing the use of a pen register, the different types of pen registers and the information that they collect, how the information that is collected is stored and accessed, and any illegal or improper uses of the pen register authority. We reviewed the records associated with a sampling of pen register applications submitted to the FISA Court during our review period. The records included applications, orders, certifications of senior Department and FBI officials, and memoranda of law that accompanied certain pen register applications. The cases we examined included each of the emergency pen registers requested under 50 U.S.C. § 1843 during the review period and each of the applications the government filed in connection with the now-discontinued National Security Agency (NSA) program to collect bulk electronic communications metadata under the pen register provisions of FISA. We also selected applications for review based on certain noteworthy aspects of the cases, and reviewed additional applications that we selected randomly.

During the course of this review, we interviewed approximately 35 FBI and Department employees, including line attorneys in the FBI's Office of General Counsel and the Department's National Security Division (NSD) who prepared pen register applications, and supervisory personnel in both offices responsible for approving the submissions to the FISA Court. We also interviewed FBI technical personnel involved in the collection of pen register information and its storage in FBI databases.

We relied on the Department's reporting to the FISA Court to describe any compliance incidents that occurred during the 2007-2009 time period, and did not conduct an independent compliance review of individual cases to determine whether there was any improper use of the pen register authority, or whether the information that the government sought with a pen register matched what the government actually obtained. However, with respect to several of the types of pen registers we reviewed, we highlighted the challenges the Department faced, and still faces, in ensuring that the government collects or uses only that information it is lawfully permitted to obtain.

Legal Background

Title IV of FISA was enacted on October 20, 1998, and governs the use of pen registers to obtain foreign intelligence information in national security

investigations. *See* 50 U.S.C. §§ 1841-1846. Title IV adopts the definitions of "pen register" and "trap and trace device" from the statute that governs the use of these investigative tools in criminal investigations. *See* 50 U.S.C. § 1841(2). The government is not authorized under FISA to obtain the contents of wire or electronic communications with a pen register order.

The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (Patriot Act) amended the definitions of "pen register" and "trap and trace device" in 2001 to clarify that the pen register provisions apply to an array of modern communications technologies, such as cellular phones and the Internet, and are not limited to traditional telephone lines.[2] The Patriot Act also amended the definitions to expressly state that information collected by a pen register "shall not include the contents of any communications."Pub. L. No. 107-56, § 216(c), 115 Stat. 272, 290 (2001). In addition, the Patriot Act added language ensuring that any "investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Pub. L. No. 107-56, § 214(a)(1), 115 Stat. 272, 286-87 (2001).

An application to the FISA Court for an order authorizing the use of a pen register must be in writing, under oath or affirmation, and approved by the Attorney General or a designated attorney for the Government. *Id.* at § 1842(b)-(c). The application must also identify the federal officer seeking to use the pen register and contain:

> a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

Id. at § 1842(c).

The FBI's Domestic Investigations and Operations Guide (DIOG) contains specific guidance for the use of pen registers in FBI investigations. This guidance sets forth the standards for the use of pen register information, the approval requirements for requesting a pen register, and the specific procedures for obtaining a pen register order. The FBI's use of pen registers also is governed by the Attorney General's Guidelines for Domestic FBI Operations, which apply to all FBI investigations.

---

[2] Pub. L. No. 107-56, § 216(c), 115 Stat. 272, 290 (2001); *see* H.R. Rep. No. 107-236(I) at 52-53 (Oct. 11, 2001); *see also* 147 Cong. Rec. S10999-S11000, S11006 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy).

There are important differences in the FISA statute between pen register authority and the authorities to conduct electronic surveillance and physical searches. The most important difference between the authorities is the standard that must be met for an order to be issued. As described above, a pen register order requires a certification that the information likely to be obtained is foreign intelligence information not concerning a U.S. person or is relevant to an authorized national security investigation. However, to obtain an order from the FISA Court authorizing electronic surveillance under § 1805 or a physical search under § 1824 of the FISA statute, the government must, among other requirements, demonstrate probable cause to believe that the target of the collection is a foreign power or an agent of a foreign power.

The FISA statute includes certain restrictions on the use and disclosure of information acquired in response to a pen register order. *See* 50 U.S.C. § 1845. For example, as with information acquired under FISA-authorized electronic surveillance or physical search, no information acquired with a pen register may be disclosed for law enforcement purposes unless it is accompanied by a statement that such information, or information derived from it, may only be used in a criminal proceeding with the advance authorization of the Attorney General. 50 U.S.C. § 1845(b).

However, unlike FISA's electronic surveillance and physical search provisions, the pen register provisions do not require that the information collected be subject to "minimization procedures." Minimization procedures are specific rules that govern the acquisition, retention, and dissemination of non-publicly available information concerning U.S. persons that has been obtained without their consent. Nonetheless, we found that the FISA Court occasionally included in its orders restrictions on the use, dissemination, and retention of pen register acquired information even though such restrictions are not required by statute. In addition, as with all foreign intelligence information, the FBI's use and dissemination of pen register acquired information must be handled in accordance with applicable Attorney General Guidelines, Executive Orders, and internal FBI policies.

The OIG's Findings Regarding the FBI's Storage and Handling of Pen Register Information[3]

Most of the FBI's practices for storing and handling pen register information have remained substantially unchanged since our 2007-2009 review period. The FBI receives the vast majority of pen register information electronically. Typically, the provider is served with an order and, shortly thereafter, pen register information for the targeted account is electronically

[3] As noted above, the OIG's descriptions of the process that the FBI and the Department follow to file applications with the FISA Court for pen register orders and extensions of orders, and the OIG's examination of the FBI's use of pen register authority from 2007 and 2009, are not included in this Executive Summary because the FBI and the Intelligence Community determined that much of this information is classified or "for official use only."

delivered to an FBI collection system. Once received, the collection system converts the information into a standard format used by the FBI and then exports the information into the FBI database that stores that type of information. The telephone and electronic communications information is stored as a matter of course in three databases: telephone pen register information is sent to a database called Telephone Applications, which is the FBI repository for all telephone metadata collected pursuant to FISA and non-FISA authorities; and electronic communications information is sent to one of two classified databases. Numerous other FBI databases also may eventually receive some or all of the pen register information collected in a particular case, and as a result the information obtained pursuant to pen register authority is broadly available to FBI personnel with access to the databases in which pen register data is stored.

The OIG's Findings Regarding the Compliance Process

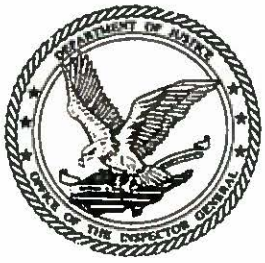
Under Executive Order 13,470 and FISA Court Rules of Procedure, the illegal or improper use of pen register authority must be reported to the FISA Court, the Intelligence Oversight Board (IOB), and the Director of National Intelligence (DNI).[4] The FISA Court's Rules of Procedure require the government to immediately notify the FISA Court if it discovers that "any authority or approval granted by the Court has been implemented in a manner that did not comply with the Court's authorization or approval or with applicable law." Similarly, executive orders require the U.S. intelligence community to report to the IOB and the DNI "any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive." E.O. 13,470 § 1.6(c), *amending* E.O. 12,333 on United States Intelligence Activities.

We found that the Department's National Security Division and FBI do not conduct systematic compliance reviews of pen registers, and instead rely on personnel assigned to cases involving pen registers to report any potential compliance violations. Internal FBI policy describes the process that employees are expected to follow for identifying and reporting potential violations, and FISA Court rules require that all compliance incidents be immediately reported to the FISA Court. The National Security Division is responsible for notifying the FISA Court of compliance incidents, and a summary of all such incidents is included in the Attorney General's semiannual reports to Congress that are required by the FISA statute. Our classified report describes the compliance incidents that were reported during our review period; while we did not conduct an independent compliance review of individual cases, we did not find any compliance incidents that had not been previously identified.

---

[4] The IOB was created by Executive Order in 1976 and charged with reviewing activities of the U.S. intelligence community and informing the President of any activities that the IOB believes "may be unlawful or contrary to executive order or Presidential Directives." *See* E.O. 12,863.

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline . 369-4499.



Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig