pages from

BEHIND THE BLACK BOXES

trying to make sense out of a heavily-redacted report on the FBI's involvement in the PRISM surveillance program

featuring interviews with Kade Crockford and Heather Kapplow, and a psychic reading by the Center for Cognitive Chaos & Astral Physics Research

a project by Tim Devin

For copies, go to
timdevin.com/btbb.html
or email
tdevin@yahoo.com

Table of Contents

Table of Contents (Cont'd)

The 2012 Office of the Inspector General (OIG) report on the FBI and the PRISM surveillance program

I first came across the OIG report when the *New York Times* published a redacted version of it in January 2015. The document is an overview of the FBI's role in the now-notorious PRISM surveillance program, and shows how that role has changed over time. It also talks about errors the FBI has made, and the FBI's reluctance to send reports to its overseers—reports that it is required by law to write.

That much is clear from the document as it was released. The trouble is that the specifics (how is the program supposed to work? what errors did the FBI make?) were mostly blacked out.

Endless black boxes

Introduction

The public version of the document is fascinating: filled as it is with cryptic phrases, strange acronyms, and references to departments and units that I personally had never heard of before. And then there were the endless black boxes, covering information that the government felt could not be made public. I thought if I could only figure out what those black boxes were hiding, I'd understand the document—and have a better sense of whether PRISM really was as bad as I thought it was.

So I read a lot. The more I learned, the more I realized that just filling in the boxes wasn't going to be enough. I also needed to understand all the jargon, all the past decisions, all the players—in other words, I needed to understand the government culture that produced PRISM, too.

So I went back and read even more: endless government reports, countless news sources and blogs (left wing, right wing, and conspiracy-spouting tinfoil hat). I also interviewed Kade Crockford, the Massachusetts ACLU's expert in digital privacy.

That was all well and good, but I was still hitting some walls. I thought if only I could ask someone some direct questions, I'd get somewhere. The FBI not being responsive, I hired Heather Kapplow

o portray an FBI agent, and interviewed her instead. Just to be thorough, I also hired the Center for Cognitive Chaos & Astral Physics Research to do a psychic reading of the document.

Behind the black boxes

What you have in your hands pulls all of this together.

Section 1 shows you my attempt at filling in the boxes. It's only the "executive summary," but it gives a nice overview of what's covered in the full document. (The full document is over 200 pages, and is freely available online if you want to have a look.)

Section 2 gives an overview of the context of the document—the culture that produced it, the laws that it draws on, and a hundred other things. Basically, all of the things that I found helpful in trying to understand the document.

Section 3 has transcripts of the three interviews I did as part of this project, since they give a wealth of information that I couldn't fit into the other sections.

And in a brown envelope in the back, you'll find some photos and slips of paper. In case you want to learn any more yourself.

...

minimized data to other U.S. agencies and foreign governments. The FBI retains a portion of the raw data for analysis and dissemination as finished intelligence products. (S) b1, b3, b7E

~~(S//NF)~~ These two basic activities, which are discussed below and in detail in Chapters Three and Four of the OIG's report, are carried out by personnel in the Counterterrorism Division's Operational Technology Division (OTD). These personnel are drawn primarily from the Electronic Communications Surveillance Unit (ECSU), and the Data Intercept Technology Unit (DITU), two of five units within OTD. We refer to these personnel as the 702 Team. The 702 Team is supported by the FBI's Communications Exploitation Section (CXS) and the Weapons of Mass Destruction and Domestic Terrorism Section (S). The 702 Team also works closely with attorneys from the FBI Office of General Counsel (OGC), including attorneys we refer to in this report as the Operations Attorney and the Policy Attorney. b1, b3, b7E

III. (U) The FBI's Targeting Activities Under Section 702

~~(S//NF)~~ The FBI's primary role in the 702 Program is to acquire the electronic communications from the partner service providers. This process begins with the NSA's determination, based on intelligence from other agencies and its own analysis of signals intelligence already collected, that electronic communications of a selector (typically an e-mail address) may yield foreign intelligence information. The NSA applies its FISA Court-approved targeting procedures to determine that the account is used by a non-U.S. person reasonably believed to be located outside the United States. (S) (S) b1, b3, b7E

~~(TS//SI//NF)~~ The NSA may apply its targeting procedures to target a selector if it is a one-time target. This can be done through Upstream, which acquires data directly from internet backbones. When the NSA targets a selector in this way, then the FBI, through DITU, provides technical assistance only. When the NSA nominates a selector for ongoing surveillance, the 702 Team must first apply the FBI's own targeting procedures before conducting the necessary steps to notify the partner internet service providers in order to collect the requested communications. Since each partner system (e.g., Google) functions in a different way, the steps that the FBI takes vary according to which partner has the communications in question. (TS) (TS) (TS) (TS) b1, b3, b7E

~~(S//NF)~~ The NSA notifies the FBI, and then its nominations are forwarded to the 702 Team in two ways: (1) by "selector sheets" that are e-mailed to the 702 Team each day, and (2) through an FBI system called PRISM, which collects and manages the requests, and routes the acquired communications to the appropriate agents and analysts. Since the PRISM program (S) (S) b1, b3, b7E

is so central to this method of collection, it has come to be the default name for this collection method itself. This use, common in the agencies involved in this type of 702 collection, will be used throughout the current report. And it is this type of 702 collection that this report investigates. (S)

A. (U//FOUO) The FBI's Targeting Procedures

~~(S//NF)~~ The 702 Team's analysts are responsible for applying the FBI's FISA Court-approved targeting procedures to the nominated selectors. The work of these analysts is reviewed by supervisory special agents or the OTD Unit Chief, and in some instances, by attorneys in the Office of General Counsel and officials in the NSD, for a final determination as to whether a (S) target can proceed. To implement the general requirements of its targeting procedures, the FBI developed its own targeting procedures (SOPs) for internal (S) (S) circulation, which provide the 702 Team step-by-step procedures for processing NSA targeting requests. (S) b1, b3, b7E

~~(S//NF)~~ As set forth in the Office of Legal Counsel's interpretations of Section 702, the FBI has two primary obligations under its targeting procedures. First, the FBI must review and evaluate the sufficiency of the NSA's explanation for its reasonable belief that the user of the nominated account is located outside of the United States, and the information that the NSA provides concerning the user's non-United States person status. The targeting procedures state that this sufficiency review will be done "in consultation with" the NSA. (S) b1, b3, b7E

~~(S//NF)~~ The second of the FBI's two primary obligations under its targeting procedures is to collect the requested communications from the internet service providers, and to then route them to the NSA. If directed by the NSA, the FBI will also send unminimized data to the CIA or to the FBI's Counterterrorism Division. The targeting procedures require the FBI to conduct minimization procedures (see related sections in this report), and then, if directed by the NSA, to route that data to other U.S. agencies, or to foreign governments. (S) b1, b3, b7E

~~(S//NF)~~ The targeting procedures do not obligate the FBI to conduct an independent, *de novo* analysis of a target's U.S. person status and location. Rather, unless the FBI has evidence in its databases that the target is a U.S. person, the FBI's targeting procedures state that "the FBI will acquire the requested communications from the partner companies." In addition, the targeting procedures state that the "NSA will . . . be responsible for determining that a significant purpose of the acquisition is to obtain foreign intelligence (S) b1, b3, b7E

...

Timeline: PRISM Precursors and Development

Oct. 25, 1978
The Foreign Intelligence Surveillance Act of 1978 passed into law. Among other things, it provides certain circumstances under which the intelligence community can monitor the communications of foreign agents inside the United States. The FISA Court is also established to oversee these actions; it begins work in 1979.

December 4, 1981
Pres. Reagan signs Executive Order 12333, which expands the intelligence community's ability to collect electronic communications.

Sept 11, 2001
A series of large-scale terrorist attacks on the US.

Oct 2001
Pres. Bush authorizes the President's Surveillance Program. This involves monitoring and collecting certain communications into and out of the US, without seeking court approval first.

2004 (exact date unknown)
President's Surveillance Program is transitioned in part to FISA Court oversight.

August 27, 2004
Pres Bush signs Executive Order 13355, which amends Executive Order 12333. Among other things, this means that the intelligence community now reports to the President through the newly created Director of National Intelligence.

Dec 16, 2005
Terrorist Surveillance Program (which is part of the President's Surveillance Program) is exposed by *The New York Times*.

January 2007
At Pres. Bush's request, the FISA court issues an order that communications companies must hand over records of non-US users, without having to seek a warrant.

April 2007
FISA court judge Roger Vinson says this January 2007 order is illegal.

...

The FBI is one of the two government units that are most heavily involved in PRISM operations. The OIG report is about the FBI's role in PRISM.

**

The Federal Bureau of Investigation
J Edgar Hoover Building, 935 Pennsylvania Ave NW,
Washington DC, 20535-0001
Founded: 1908
Number of employees: 35,104
Budget: $8.3 billion
Current Director: James B. Comey, Director, Sept. 2013 to present; he was appointed by Pres. Obama (Democrat)
Most recent past Director: Robert Mueller, Sept. 2001-Sept. 2013; he was appointed by Pres. G.W. Bush (Republican)
Parent agency: Department of Justice

The Federal Bureau of Investigation (FBI)

The Director of the FBI reports to reports to both the Deputy Attorney General and the Director of National Intelligence. After 9/11, it was made the lead organization in all domestic terrorism investigations.

**

[The FBI's priorities are to:]
1. Protect the United States from terrorist attack
2. Protect the United States against foreign intelligence operations and espionage
3. Protect the United States against cyber-based attacks and high-technology crimes
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational/national criminal organizations and enterprises
7. Combat major white-collar crime
8. Combat significant violent crime
9. Support federal, state, local and international partners
10. Upgrade technology to successfully perform the FBI's mission
- FBI's Quick Facts webpage, www.fbi.gov/about-us/quick-facts

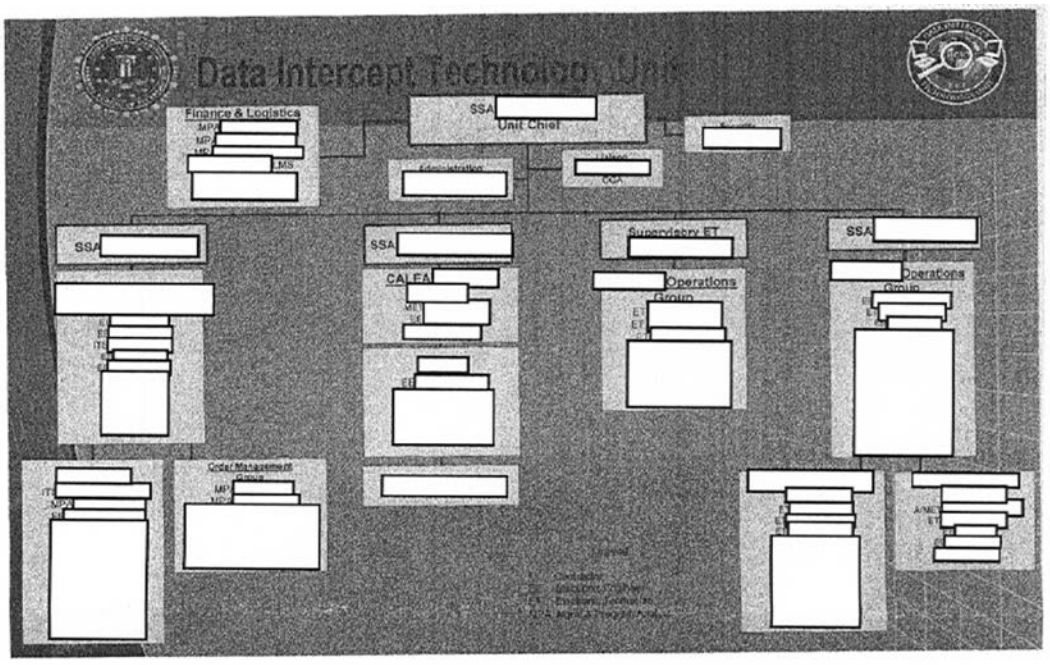
...

From the context, it seems like "the 702 team" may be a term invented by the writers of the OIG report to refer to the FBI units involved in PRISM as a group. There don't appear to be mentions of a "702 team" in other reports, but given the secret nature of these programs, that doesn't prove anything.

**

Data Intercept Technology Unit (DITU)
FBI's Training Academy in the Marine Corps Base
3250 Catlin Ave., Quantico, Virginia
Date established: unknown (first reference to it is 1997)
Number of employees: unknown
Budget: unknown
Unit chief: unknown
Parent unit: FBI's Operational Technology Division (OTD)

**



(DITU organizational chart, sent to Muckrock after they requested it through FOIA. Note that almost everything is redacted.)

**

...

Who Can See PRISM Information?

The FBI and NSA gather communications—but who are their end users? Who can view and use the communications that PRISM collects? That all depends on what type of information and evidence is found in those communications.

**

The FBI's minimization procedures govern who can see the information that is collected through PRISM. The version that was released in early 2014 was partially redacted, but here is what the unredacted sections say.

(Note: in the middle of the procedures explaining all of this, there is a large redaction. So this list is not complete.)

**

If the communications are from a non-U.S. person

If it is "foreign intelligence" (related to terrorism, espionage, or the sale of weapons of mass destruction), the FBI and NSA can give the communications to federal, state, local or tribal agencies who regularly handle foreign intelligence.

**

If the communications are from a U.S. person

If it is "foreign intelligence" (related to terrorism, espionage, or the sale of weapons of mass destruction), the FBI and NSA can give the communications to federal, state, local or tribal agencies who regularly handle foreign intelligence, or to foreign governments.

If it is evidence of a crime, they can give the communications to federal, state, local or tribal law enforcement agencies, or to foreign governments.

**

The FBI and NSA can also search and use these communications for national security purposes; the FBI can also use communications for domestic law enforcement. Only trained FBI and NSA agents can