The Snowden Files: What We Know About US Cyber-Surveillance & Espionage

By Riley Willis
Contents

● A History of NSA Whistleblowers
● Edward Snowden & The Snowden Files
● What Is Metadata?
● NSA Programs
● Partners In Crime
● Current Status & The Changing Status Quo
A History of NSA Whistleblowers

● Thomas Drake:
  ○ Believed new NSA tools were both a waste of money and violated privacy of US citizens
  ○ Expressed his concerns through proper channels, reporting to the NSA IG, DOD IG, and House and Senate Intelligence Committees
  ○ After no changes were made, he shared his complaints and some documentation with a journalist at the Baltimore Sun
  ○ In 2011, Drake was charged with several offenses, with up to 35 years in prison, but charges were dropped just before the trial was to take place

● William Binney, J. Kirk Wiebe & Edward Loomis:
  ○ Felt new NSA programs they had worked on developing were being used unconstitutionally
  ○ Reported their concerns to DOD Inspector General in 2002, including some that had been previously voiced by Drake
  ○ Had their homes raided by armed FBI agents in an apparent intimidation attempt in 2007 after a New York Times article revealed large-scale government surveillance of US citizens
A History of NSA Whistleblowers (Continued)

● Russell Tice:
  ○ Raised concerns to the NSA IG and DOD IG
  ○ Was a source for the 2005 *New York Times* article that exposed government surveillance of US citizens

● Mark Klein:
  ○ An AT&T communications technician who revealed that the company had worked with the NSA to install hardware to intercept US communications in 2006
Edward Snowden

- NSA contractor who became concerned about spying activities on US citizens after being stationed in an NSA facility in Hawaii
- In 2013, he flew to Hong Kong, where he met with journalists and revealed thousands of NSA documents
- Has been charged with violating the Espionage Act of 1917
- When flying from Hong Kong on his way to Ecuador, his passport was revoked, leaving him stuck in Moscow
- After a month of being stuck in the airport, he was granted asylum by Russia, where he is today
The Snowden Files

- Extensive collection of documents that revealed NSA programs for global communications surveillance
- Revealed that the NSA was collecting information from both within and outside the United States without warrants
- NSA had access to metadata provided by telecom companies, including phone providers, ISPs, and more
- NSA had direct access to even more information from various sources
1ST DEGREE: FRIENDS

498
or more than all members in the United States House of Representatives

ACTUAL: 435

2ND DEGREE: FRIENDS OF FRIENDS

81,373
or more than the capacity of Beijing National Stadium

ACTUAL: 80,000

3RD DEGREE: FRIENDS OF FRIENDS OF FRIENDS

13,296,348
or more than the population of Illinois

ACTUAL: 12,830,632

Graphic from The Guardian
1st Degree: Friends

998
or more than the capacity of the London Eye

Actual: 500

2nd Degree: Friends of Friends

163,073
or more than the population of Sioux Falls

Actual: 158,008

3rd Degree: Friends of Friends of Friends

26,646,128
or more than the population of Texas

Actual: 25,145,561
HERE'S MY PHONE NUMBER

ALREADY HAVE IT
What is Metadata?
Some Examples

Phonecall:
- What number was called?
- When was the call?
- How long was the conversation?

Email:
- What is the IP address of the sender?
- What is the IP address of the receiver?
- Size of files that were sent?

Picture
- When was the picture taken?
- Where was the picture taken?
- What camera and settings were used?
Collection Was Not Limited To Metadata...
The Programs
PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- Special Requests

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN
What is XKEYSCORE?

1. DNI Exploitation System/Analytic Framework

2. Performs strong (e.g. email) and soft (content) selection

3. Provides real-time target activity (tipping)

4. “Rolling Buffer” of ~3 days of ALL unfiltered data seen by XKEYSCORE:
   - Stores full-take data at the collection site – indexed by meta-data
   - Provides a series of viewers for common data types

1. Federated Query system – one query scans all sites
   - Performing full-take allows analysts to find targets that were previously unknown by mining the meta-data
How the NSA collects your data

SOURCES

Telecommunications Cables

AT&T  VERIZON  SPRINT  FACEBOOK  APPLE  GOOGLE  MICROSOFT  YAHOO  ADL

PATRIOT ACT
Section 215

FISA AMENDMENTS ACT
Section 702

NSA

FAIRVIEW, STORMBREW, BLARNEY, AND DAKSTAR
(Upstream, Data)

MAINWAY
(Phone Metadata)

NUCLEON
(Phone Content)

PRISM
(Internet Content)

MARINA
(Internet Metadata)

MOONLIGHTPATH
(Internet Metadata, planned Sept. 2019)

SPINNA RET
(Internet Metadata, planned Sept. 2019)

SHELLTRUMPET & EVILOLIVE
(Internet Metadata)
Partners in Crime
FVEY
(Five Eyes)

- United States
- United Kingdom
- Canada
- Australia
- New Zealand
Nine Eyes

- FVEY Countries +
- Denmark
- France
- Netherlands
- Norway
Fourteen Eyes (SIGINT Seniors Europe/SSEUR)

- Nine Eyes Countries +
- Germany
- Belgium
- Italy
- Sweden
- Spain
Where are we now?
USA Freedom Act

- Bans bulk collection of American telephone records and internet metadata
- Limits collection of data, reducing the breadth of collection
- Limits collection of data to “two hops” from a suspect
- Gives private companies more freedom to report the number of FISA orders they receive
- Provides new reporting requirements to FISA authorities
Advancements in Technology

- Widespread adoption of HTTPS (Hypertext Transfer Protocol Secure)
- Widespread adoption of encrypted communications
- Increased use of VPNs
- Increased use of TOR and other decentralized internet platforms
What Now For The NSA?

- Not much has changed other than USA Freedom Act, but data collected on US citizens is decreasing
- NSA now has increased reporting requirements and puts out annual Statistical Transparency Reports
**Figure 4: Section 702 Targets***

<table>
<thead>
<tr>
<th>Section 702 of FISA</th>
<th>CY2013</th>
<th>CY2014</th>
<th>CY2015</th>
<th>CY2016</th>
<th>CY2017</th>
<th>CY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of targets of such orders**</td>
<td>89,138</td>
<td>92,707</td>
<td>94,368</td>
<td>106,469</td>
<td>129,080</td>
<td>164,770</td>
</tr>
</tbody>
</table>


*Recall that only non-USPs are targeted.

**Previously the IC was not statutorily required to publicly provide this statistic but provided it consistent with transparency principles. The FISA Amendments Reauthorization Act of 2017 codified this requirement at 50 U.S.C. § 1873(b)(2)(A).

---

**Figure 19: CDRs Received Arising from Such Targets**

<table>
<thead>
<tr>
<th>Call Detail Records (CDRs)—Section 501(b)(2)(C)</th>
<th>CY2016</th>
<th>CY2017</th>
<th>CY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of call detail records arising from such targets that NSA received from providers pursuant to Section 501(b)(2)(C) and stored in its repositories*</td>
<td>151,230,968</td>
<td>534,396,285</td>
<td>434,238,543</td>
</tr>
</tbody>
</table>

*While the statute directs the government to count the unique identifiers, until May of 2018, the government was not technically able to isolate the number of unique identifiers; thus, the number reported above counts total CDRs received for the year and includes duplicate records. Additionally, the number of records contains both domestic and foreign numbers, including numbers used by business entities for marketing purposes.

---

**FISA Title VII—Section 702**

- Commonly referred to as “Section 702.”
- Requires individual targeting determinations that the target (1) is a non-U.S. person (2) who is reasonably believed to be located outside the United States and (3) who has or is expected to communicate or receive foreign intelligence information.
### Figure 11: Section 702 Reports Containing USP Information Unmasked by NSA

<table>
<thead>
<tr>
<th>Section 702 Reports Containing U.S. Person (USP) Information Disseminated by NSA</th>
<th>CY2016</th>
<th>CY2017</th>
<th>CY2018</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REPORTS</strong>—Total number of NSA disseminated § 702 reports containing USP identities <em>regardless of whether or not the identity was openly included or masked.</em></td>
<td>3,914</td>
<td>4,065</td>
<td>4,495</td>
</tr>
<tr>
<td><strong>REPORTS</strong>—Total number of NSA disseminated § 702 reports containing USP identities <em>where the USP identity was masked.</em></td>
<td>2,964</td>
<td>3,034</td>
<td>3,442</td>
</tr>
<tr>
<td><strong>REPORTS</strong>—Total number of NSA disseminated § 702 reports containing USP identities <em>where the USP identity was openly included.</em></td>
<td>1,200</td>
<td>1,341</td>
<td>1,379</td>
</tr>
</tbody>
</table>

Rows 2 and 3 will not total row 1 because one report may contain both masked and openly named identities.
Other Issues

- Alliances such as FVEY allow storage of data in other countries, bypassing laws that stop NSA from storing data on US citizens
- Increased use of trackers used by websites, particularly internet giants such as Google, Facebook, and Amazon
- As advancements in technology for consumer privacy continues, so does the advancement of technology used for surveillance
- Widespread adoption of the “If you have nothing to hide, you have nothing to fear” mentality
Big Brother is watching you.

George Orwell
Thank You!
For more info on internet privacy, you know where to find me.