NSA Surveillance
Just doing its job?

Scott Bradner

12/04/2023

Talk Scope

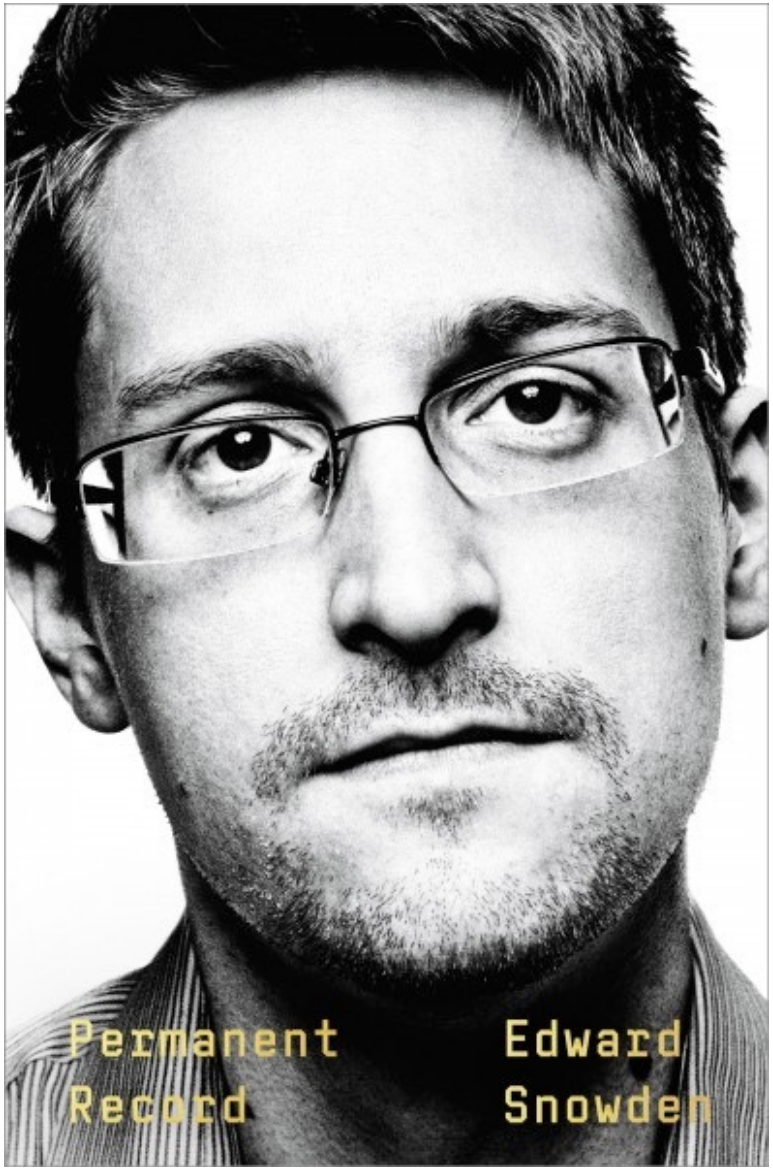
- NSA signals intelligence (SIGINT)
  - rules
  - programs
  - procedures
  - legal question

Not Covered

- NSA non-SIGINT special activities
- Providing cryptologic support to Armed Forces
- Hacking (Office of Tailored Access Operations)
- Providing public security guidance

  e.g., secure computer configuration guidelines
- K-12 outreach

Shine a light?



Section 702

- talk more about this later
- basic authorization & rules for NSA surveillance of non-US persons
- does not authorize NSA targeting US Persons

Basic Concept

- NSA SIGINT collects communications to or from targets or information created by a target
- Use “selectors” to identify the target information
- NSA collects the target information

  NSA can compel 3rd parties to provide information (“Downstream Collection”) (was “PRISM”)

  NSA can wiretap international communication links (“Upstream Collection”)
- Obtained communications are put into one or more NSA databases
- NSA analysists search databases using “queries”

Sec 702 Targets

- "US Person":

  a citizen of the United States;

  an alien lawfully admitted for permanent residence;

  an unincorporated association with a substantial number of members who are citizens of the U.S. or are aliens lawfully admitted for permanent residence; or

  a corporation that is incorporated in the U.S.

- "Non US Person"

  others

NSA Website

Sec. 702 Targets, contd.

- *A target inside the U.S. is assumed to be a US Person unless specific information to the contrary is obtained*
- *A target outside the U.S. is assumed to be a non-US Person unless specific information to the contrary is obtained*

NSA Website

- Sec 702 expanded targets beyond foreign powers or agents of foreign powers
- “lone wolf” targets added in 2004
- 129K targets in 2017, 203K in 2020, 246K in 2022

Sec. 702 issues

- FBI has warrantless access to the sec 702 database
  - 3.4 million warrantless searches in 2021
  - down to 204K in 2022 after outcry
- Sec 702 currently expires the end of 2023
  - FBI access is a major stumbling block to extending
- Congress working on an extension
  - some want warrant requirement to access US person info
  - some think that better internal supervision will do it
- FBI head says the FBI can not do its job if they have to obey the U.S. Constitution

NSA Collection Legality

- NSA data collection has been authorized
  - In that there were laws or presidential executive orders authorizing the underlying NSA activities
    - But some EO authorizations (e.g. Bush wiretapping) violated law
    - Actual collection & search has too often exceeded authority
- The specifics of the authorized activities have changed over time
- Specifics of the NSA activity have been challenged in court from time to time (when they became known)
  - Some courts have ruled against specific activities

NSA surveillance Milestones

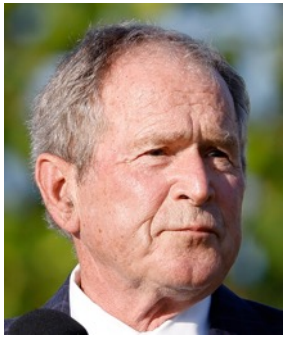
- 1952: NSA created by U.S. Secretary of Defense as directed by President Truman
  focused on government / military communications – protecting ours & intercepting theirs
- 1960s & 70s: NSA targeted U.S. anti-war and civil rights activists
- 1975: NSA monitoring of US persons uncovered by U.S. Senate committee run by Senator Church
- 1978: Carter EO 12036
  limited NSA monitoring of US Persons anywhere
- 1978: Foreign Intelligence Surveillance Act (FISA)
  set up FISA court to authorize surveillance activities

Milestones, contd.

- 1981: Reagan EO 12333: Basic authority and rules for NSA information collection
- 2001: USA PATRIOT Act: gave NSA more authority
- 2002: Bush secret EO:

  OKed "warrantless wiretapping" of US persons

  if communication was with non-US Person suspected of terrorist activities



- 2005: NYT publishes story on "warrantless wiretapping"
- 2007: "warrantless wiretapping" program terminated by administrative action

Milestones, contd.

- 2008: FISA update

  Section 702 set rules for electronic surveillance
- 2010s: Safe Harbor challenged
- 2014: Obama Policy Directive

  set rules for surveillance of non-US Persons
- 2015: Safe Harbor ruled invalid
- 2015: USA Freedom Act

  reauthorized Patriot Act with some limits
- 2022: Biden EO :

  set rules for surveillance of non-US Persons

Reagan EO 12333

- *NSA is authorized to collect, process, analyze, produce, and disseminate Signals Intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions, and to provide signals intelligence support for the conduct of military operations.*
- *prohibits the collection, retention, or dissemination of information about U.S. persons except pursuant to procedures established by the head of the agency and approved by the Attorney General.*

NSA Website

FISA

- The Foreign Intelligence Surveillance Act of 1978
- Established that non-criminal electronic surveillances within the United States were only permissible for the purpose of collecting foreign intelligence and/or foreign counterintelligence.
- Established procedures for the conduct of foreign intelligence surveillance

FISA, contd.

- Created the Foreign Intelligence Surveillance Court (FISC)

  Eleven federal district court judges designated by the Chief Justice of the United States

- Also multiple *amicus curiae* appointed to inform the court about specific legal or technical issues
- The names of the FISA judges and *amicus curiae* are public

Current Sec 702 Targeting Rules

- There must be a valid, documented foreign intelligence purpose, such as counterterrorism
- NSA is not permitted to target U.S. persons, or to target non-U.S. persons outside the U.S. if the purpose is to target a particular, known person inside the United States
- NSA is not permitted to intercept any "wholly domestic" U.S. communications
  can request the FBI to do that interception
- NSA is not permitted to target a non-US Person to collect information about a US Person without explicit OK

Targeting Rules, cont.

- NSA may collect communications of non-US Persons outside of U.S. if other conditions met
- Improperly collected communications must be promptly destroyed unless the NSA director exempts the specific communication(s) - limited permitted reasons

Explicit OK

- Consent of the target
- FISA Court order
- Attorney General determines US Person is an agent of a foreign power or an officer or employee of a foreign power & collection will acquire significant foreign intelligence or counterintelligence

  good for up to 90 days
- Exigent Circumstances
- NSA report: 67 US Persons & 309 non-US Persons in the U.S. targeted under FISA warrants in 2021

NSA Internal Watchdog

- Function strengthened by law in 2014
- Now "*an independent, Senate-confirmed watchdog*"
- Issues semi-annual report (with a public unclassified version)
- E.g., compliance issues listed in Sept 2021 report

  data accessed without proper authority
- NSA internal watchdog seems to be quite serious about the NSA obeying the law

  or at least obeying NSA's interpretation of what the law is

Selectors

- *a unique identifier associated with the target - for example, a telephone number or an email address. This unique identifier is referred to as a selector. The selector is not a "keyword" or particular term (e.g., "nuclear" or "bomb"), but must be a specific communications identifier (e.g., e-mail address)*
- Selectors are *electronic communication accounts/addresses/identifiers*

2014 NSA report on sec 702 program

Selector Process (sec 702)

- NSA analyst identifies target
- NSA analyst verifies & documents that the target is

  a non-US person

  is located outside U.S. at this time

  is likely to communicate foreign intelligence information
- NSA analyst identifies communication modes
- NSA analyst identifies unique ID (selector) for mode
- Request must be approved by two senior NSA analysts

NSA SIGINT Programs

- Collection Programs
  - Downstream Collection (was called PRISM)
  - Upstream Collection
- Other SIGINT related activities
  - Communication standards
    - NSA may have purposefully weakened a U.S. national cryptography standard

Downstream Collection

To facilitate the acquisition of downstream collection, if requested by NSA, FBI may serve a 702 directive on an ECSP, for example an email provider, compelling the provider to collect and produce the communications of an identified selector, for example an email address

2023 NSA report on sec 702 program

- Snowden leaked NSA presentation lists Microsoft*, Yahoo*, Google*, Facebook, PalTalk, AOL, Skype, YouTube and Apple

  note: companies required by law to comply
- Data collection & check for US Persons done by FBI
- Data include: stored communications, chat, real time notice of email or chat event, e-mail, VoIP, Web traffic, messaging photos etc, subscriber info, videos

*made up 98% of captured info in 2013

Downstream Collection, contd.

- Targets are non-US Persons not in the US when the request is made
- more than 200 million communications collected annually (2011)

Upstream Collection

upstream collection occurs with the compelled assistance of U.S. communications providers that control, operate, or maintain the telecommunications "backbone" over which communications transit. Upstream collection occurs inside the United States and only at locations that are likely to carry traffic associated with tasked Section 702 selectors.

2023 NSA report on sec 702 program

Upstream Collection, contd.

- *To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases.*

2023 NSA report on sec 702 program

- 2021*:* 85.3 million transactions captured

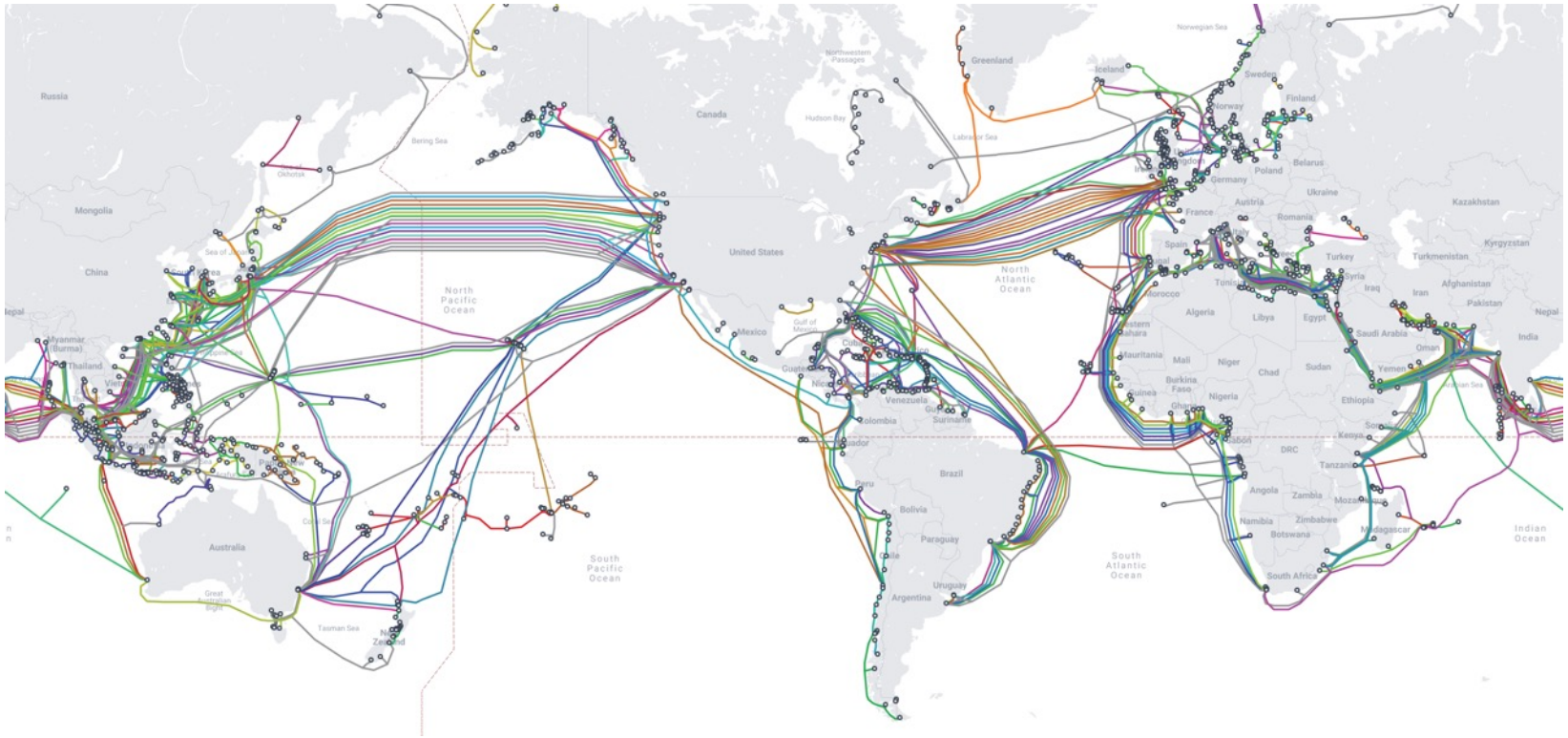
2023 NSA report on sec 702 program

Upstream Collection Mechanism

- The NSA has not disclosed many of the details

  But there are not many options

- NSA intercepts communications from at least some international communications links



Undersea Cables

- over 50 undersea fiber optic cables that connect the U.S. to other countries
  - 4 to 12 pairs of fibers in each cable
  - Up to 160 lambdas (links) per fiber
  - Up to 40 gigabits per second per lambda
- Some links are for Internet traffic and some are for internal corporate traffic
  - Assume the NSA focuses on the Internet links
- note that much of the traffic between some non-U.S. sites (e.g., South America and Europe) go through the U.S.

Which links to monitor?

- The NSA has acknowledged that it had 232,000 Section 702 targets in 2021, mostly outside the U.S.
- Communications between these targets and the U.S. will be directed by the Internet routing system via the "shortest paths"

  i.e., picking the international link that is on the shortest path
- With such a large number of targets distributed around the world target communications will use most if not all the international links that carry public Internet traffic

  In order for the NSA to have a chance of capturing communications from all of its targets

Processing

- NSA intercepts all packets on an Internet link
- Checks to see that at least one of the source or destination addresses are outside the US

  does not make this check in some cases
- Reassembles packets into communications
- Checks to see if communication includes a selector
- If yes, imports communication into a distributed database (XKeyscore)
- if no, the assembled communication is discarded

Not “wholly domestic”

- Must not be “wholly domestic”

  I.e, at least one end outside the U.S.

  NSA is required to use other technical means, such as Internet protocol (“IP”) filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States. 2014 NSA report on sec 702 program

- Large filter – e.g., one list of U.S. IPv4 address prefixes contains 66 K entries

  Also, list can be quite dynamic with current market-based IP address assignment process

Not always check

- The NSA says it does not always use a filter

~~(TS//SI)~~ In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [redacted] In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.

- It may be the case that the NSA assumes that traffic on some international links cannot be "wholly domestic" so does use an IP address filter on those links
- But Internet routing can cause that not to be the case
- So can "multiple communications transactions" (MCT)"

MCT

- MCT is where multiple individual communications are bundled into a long communication

  e.g., when a mail client connects to a mail server after being disconnected for a while - sends a burst of backed up email

  such a burst could include communications involving US Persons or “wholly domestic” communications

- FISA court limited the collection of MCTs in 2017

XKeyscore

- "a front end search engine" (Snowden)
- World wide collection of servers (> 700)
- Fed by NSA section 702 collection programs and other programs
- Database can be queried using selectors

  email addresses, IP addresses, phone numbers, etc. As well as names etc.
- Also more meta concepts (“users of Tor”)
- Includes other tools such as IP address to location mapper

NSA Query Rules

- NSA query procedures must be reviewed by the FISA court
  - To make sure that sec 702 restrictions are met
  - Protect US Persons
  - Protect attorney-client privilege communications
  - Queries are logged and may be audited
- NSA *procedures* are very protective of US Persons
  - Driven by law (e.g., USA FREEDOM Act) and FISA court
  - Procedures have not always been followed

XKeyscore

- Snowden claimed that Xkeyscore can be used to create real-time wiretaps anywhere in the world
  - NSA claims that is not true
- Intercept claims that Xkeyscore can aid in hacking
  - Just tell it what the target is – gives you sets of credentials
- Also used by non-US intelligence agencies
- Relies on audit logs and oversight to limit user activities rather than technical protections
  - may have changed over time
- Huge amount of data, stored for limited periods of time due to scale

NSA Utah Data Center

Collection History

- Snowden revealed many NSA questionable practices

  some have been tightened up post-Snowden

- E.g., until 2017 NSA collected communications that were “about” a target

  i.e. target selector appeared anywhere in the communication

  program terminated likely as a result of pushback by FISA court because too many US Person communications were being captured

Phone Numbers

- Snowden revealed the NSA bulk phone number collection effort in 2013
- Aim was to collect the origin and destination numbers for all phone calls in the U.S.
- Approved by FISA court
- Court ruled in 2015 program was unlawful
- Stopped by USA FREEDOM Act in 2015

  Also ruled “most likely unconstitutional” by court in 2020
- now the NSA has to go to a phone company to get specific records, cannot get bulk data

Factoid

- Edward Snowden took a lot of NSA internal documents
  - only about 1% have been published
  - a few more were published in 2023
- But, in a court of law, most of these documents are still classified and thus cannot be used to show what the NSA actually does

4th Amendment Issue?

- NSA upstream collection program makes copies of ALL communications on a link
  - Then checks to see if at least one end is outside the US
    - skips this check in some cases
  - Then checks to see if the message is from or to a target
  - Discards copies if checks fail
- Thus, the NSA makes (temporary) copies of large numbers of communications it has no legal justification to retain
- Does this violate the 4th Amendment to the U.S. Constitution?

Wikimedia v. NSA

Wikimedia v NSA update

- Court ruled that the NSA had captured Wikimedia communications
- NSA claimed they could not defend themselves without endangering national security
- The court accepted the NSA's statement & threw out the case

QUESTIONS?