A history of NSA hijinks

The Bush Years

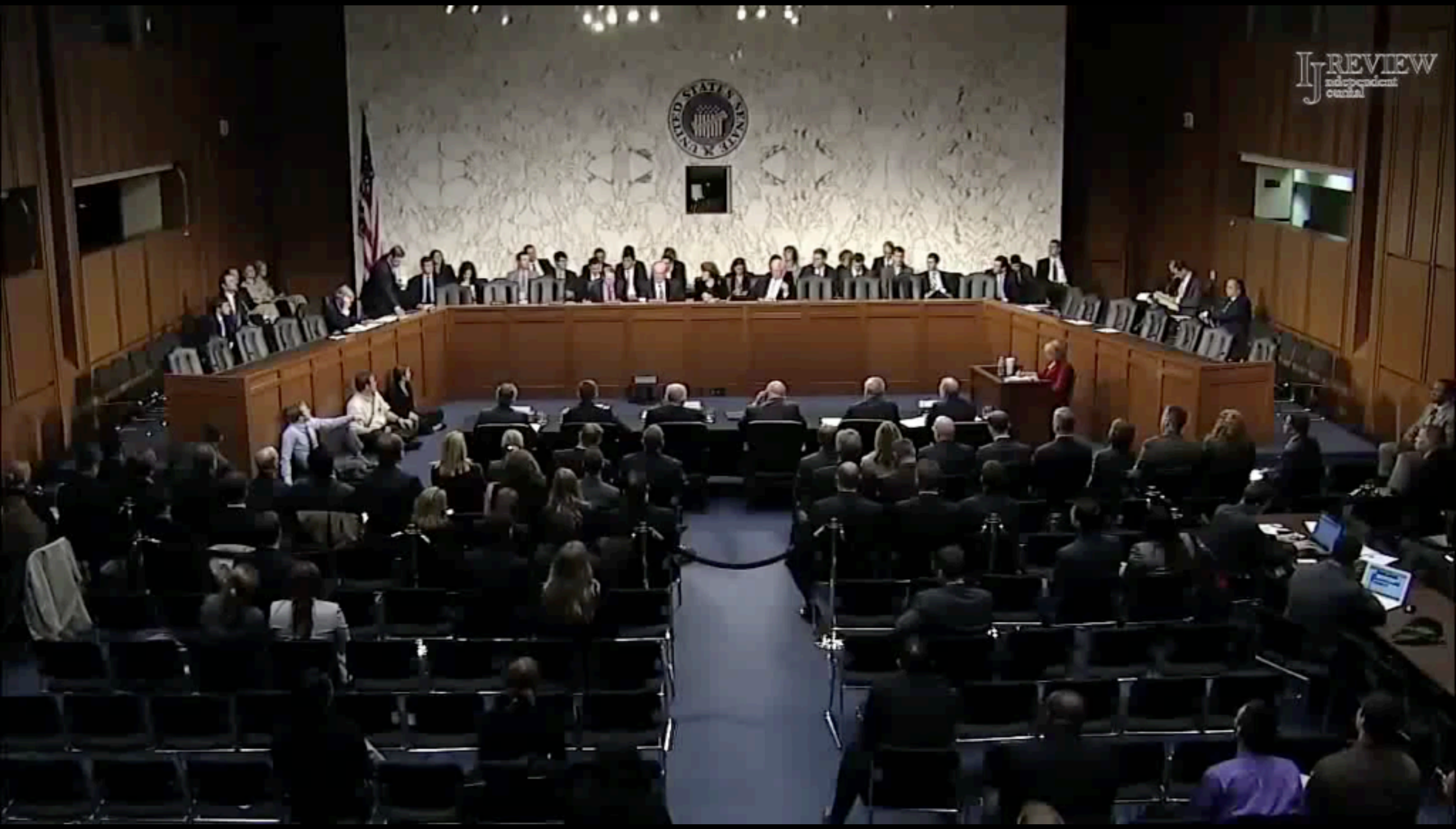
- Patriot Act allowed targeted surveillance approved by FISC, including phone taps and business records search.

- Bush issued an executive order allowing wiretaps on foreign targets without approval of the FISC

- In 2005 Bush publicly admitted to allowing the NSA to domestically wiretap hundreds of Americans linked to Al Qaeda without warrant.

- In 2006 USA Today reported mass call metadata collection

- In 2008, the FISA Amendments Act codified warrantless wiretapping, required cooperation of telecoms, and granted them retroactive immunity from prosecution for their cooperation.


IJ REVIEW
independent
courtist


MR. SANCHEZ
MR. ANDREWS
MR. JOHNSON

First Snowden Leaks

- Worked for Booze Allen Hamilton, a contractor for the NSA. “From my desk I could wiretap anyone: you, a federal judge or the president of the United States”

- The Guardian reveals FISA order allowing indiscriminate collection of metadata from Verizon phone calls for 3 months.

- The Washington Post reveals PRISM, a program where the NSA obtains internet data from major internet companies through the FBI, authorized by FISA orders

- Data about individuals three degrees away from a target can be examined. “Incidentally obtained” information can also be used.

- Data once queried from these data sources is stored in the “Corporate store”, which can be queried indiscriminately.

(TS//SI//NF) 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**

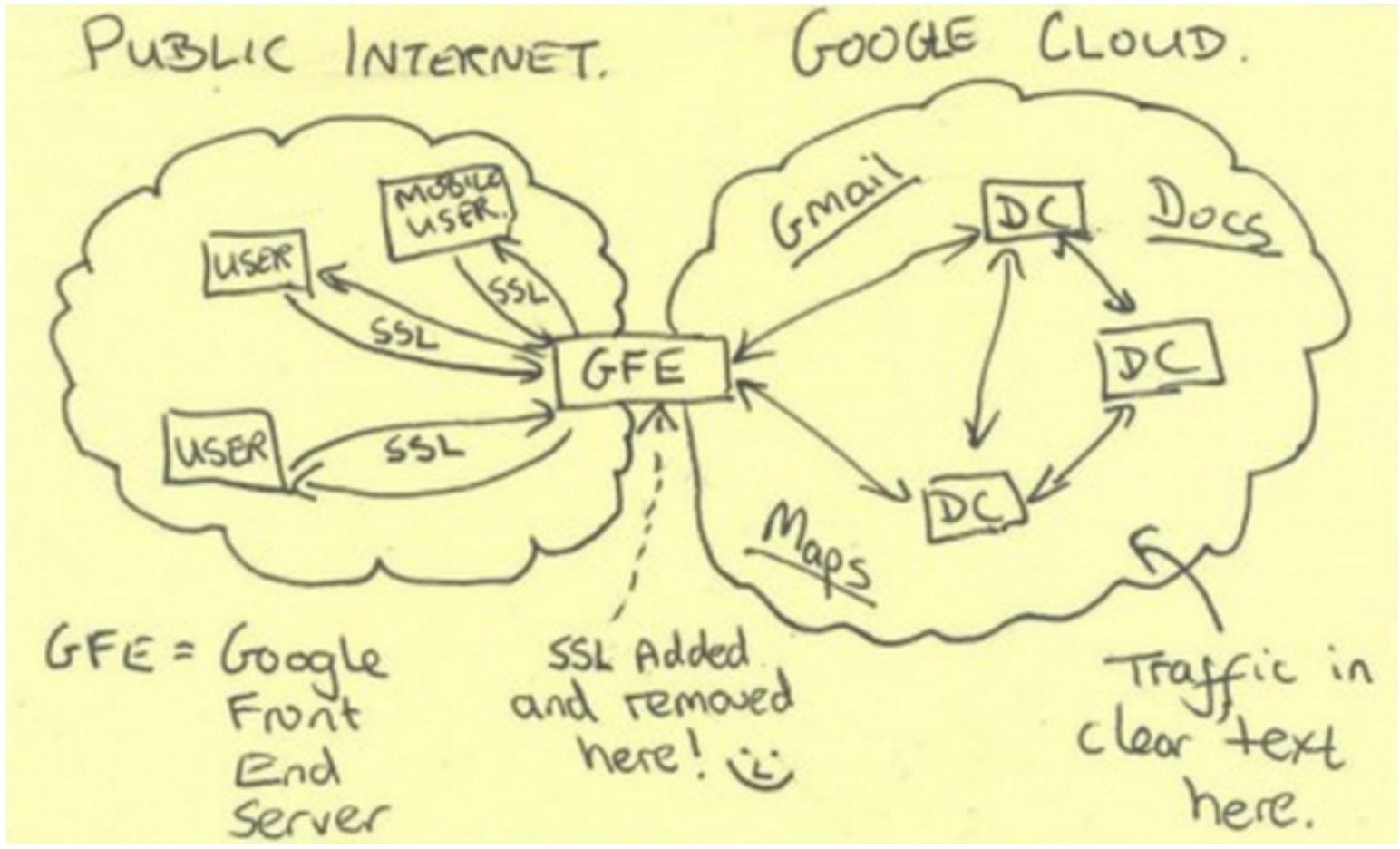
Complete list and details on PRISM web page:
Go PRISMFAA

Tapping Undersea Cables

- NSA can't collect domestic communications without FISA warrant… however, internet companies replicate data internationally between data centers.

- GCHQ captures "millions of records every day from internal Yahoo and Google networks" by tapping private leased fiber containing unencrypted data.

- Government coerces network operators to agree by withholding FCC licensing.


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
SSL
SSL
GFE
USER
SSL
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here!
Traffic in clear text here.

Weakening Encryption

- After failure of Clipper chip in the ‘90s, NSA has been working to weaken crypto and obtain keys.

- NSA coerces companies to add backdoors or reveal encryption keys.

- Leaked budget document includes goal to “influence policies, standards and specifications for commercial public key technologies”.

- Attacks against SSL, VPNs, and cell networks.

Dual_EC_DRBG

- Random number generator in NIST standard with NSA as sole author.
- Contains a constant (Q) of unknown origin that may embed a backdoor:

  Q = d*P

  If the NSA knows d, they can predict the RNG
- NSA paid RSA, a security company, $10 million to use as default RNG! RSA couldn’t quite deny it.

QUANTUM

- General framework for exploitation via MITM attacks
- QUANTUM INSERT Servers located on the internet backbone watch for a request, get a response back sooner than the real host
- Redirects to Foxacid server with QUANTUM THEORY zero day exploits
- If an existing server isn't close enough, they hack your router. NSA has implanted software in over 100,000 computers!
- Dodge SSL via fake certificates. See DigiNotar.

QUANTUM, cont'd

- Browser profiling used to ID target
- Used to unmask Tor users
- Hacked Belgocom admins via fake Slashdot and Linkedin sites.
- QUANTUMCOPPER allows manipulation of file uploads and downloads.
- QUANTUMBOT takes over botnets
- NSA surveillance network reaches 75% of internet traffic transiting the US.

Cell Phone Location

- 5 billion records per day on locations of cell phones.

- Data on Americans acquired via international transit.

- Co-Traveler analytics discovers people in proximity to existing targets.

Tailored Access Operations

- “Getting the ungettable”
- Interdiction
- Catalog contains:
  - Persistent BIOS exploits for HP, Dell, Junos, Cisco equipment
  - Hardware implants with radios for bridging air gaps
  - Modulating radar reflectors embedded in VGA cables
  - Cell hacking and tracking hardware
  - Remote hacking via WIFI

Foreign Leaders

- Der Spiegel reported that the NSA tapped German Chancellor Angela Merkel's cell phone.

- NSA says Obama didn't know. Another leak said he did.

- Also the presidents of Mexico, Brazil, senior officials in the EU, etc.

- GHCQ tapped delegate's phones and set up fake internet cafes at the 2011 G20. NSA spied during the 2009 UN climate conference

Other Targets

- NSA spied on OPEC, Belgocom, Petrobras
- NSA records history of visits to porn web sites in order to hurt the reputations of “radicalizers”
- Eric Holder, the head of the Department of Justice was asked whether the DOJ was spying on Congress. He couldn’t say no.
- WSJ reports the CIA has a database of international money transfers including data on Americans.
- Mass collection of Facebook, IM, Email contact lists.

Abuses

- 2776 violations of regulations or court orders in one year according to an internal NSA audit.

- In some of those cases, the NSA decided not to tell the court.

- NSA employees sometimes task their romantic interests for surveillance. They call this “LOVEINT"

Aggression against Journalists

- David Miranda detained in UK airport for 9 hours
- GHCQ officers destroyed Guardian's hard drives with Snowden data
- Backpacker who attended discussion of Snowden leaks had his computer gear taken upon returning to NZ.
- UK is threatening Guardian staff with terrorism charges.
- "Snowden claims that he's won and that his mission is accomplished. If that is so, I call on him and his accomplices to facilitate the return of the remaining stolen documents that have not yet been exposed, to prevent even more damage to U.S. security."


NROL-39
NOTHING IS BEYOND OUR REACH

Oversight

- FISC approves 99% of all requests.
- Judges are selected by Supreme Court Chief Justice.
- 64% of FISC judges are white men originally appointed by Republican presidents.
- Courts have ruled standing to sue the NSA if you can't prove you've been spied on.
- Members of Congress asked security expert Bruce Schneier (who has seen the Snowden files) to brief them on the NSA's activities, because the NSA wouldn't tell them itself.

How might this be used?

- During the Cold War, the NSA spied on Senators
- COINTELPRO was an FBI program to spy on, infiltrate, and discredit political organizations and people (like MLK).
- Russ Tice, a former NSA employee claimed he saw surveillance of law firms, Supreme Court judges, military generals, and then-senator Obama.

Links to the

- Following opening of the NSA's Utah Data Center, the U announced a Data Center Engineering Certificate.

- U of U president attended the data center's opening.

- We build the tech.