Domestic Surveillance and You

A critical examination of the facts

Terms Checklist

Metadata: Data about data. Federal law does NOT protect your metadata. It *can* be collected and stored, and it is.

IP: a somewhat unique identifier that computers use to find each other through the internet. A bit like an address; you can move, but it’s not always simple. More related to what you use to connect and where you are when you connect to the internet than a specific computer.

Server: a large, stationary computer, usually owned by a company, that hosts a website or lots of information, usually accessed over a network or the internet.

What Metadata really means (real quick)

- Phone Metadata: whenever two phones call one another, the numbers are logged and tracked. The time, date, and duration of the call are recorded. Information about the SIM card is captured and stored. It also takes the IMSI (international mobile subscriber identification) number and records it. In some cases, GPS information related to where you made a call from is also considered metadata.
- Email Metadata: Who you send emails to, including CC and BCC. The subject line, timestamp, and IP address of the computer being sent from are also metadata.

From the beginning (some quick context)

- Mass surveillance is not new, simply enhanced by technology
- Mass surveillance generally skirts (or sometimes breaks) the law
- The NSA is not the only organization involved in mass surveillance, and has had predecessors who have done similar things at various times
- While we generally think of things like telephone wiretaps, internet monitoring, or camera systems, it’s important to recognize that it also includes and has historically involved in person spying, financial monitoring, physical theft of documents, pattern of life analysis, mail theft, blackmail, and threats
- Mass surveillance is often used to watch people who are not only terrorists, but also politically unpopular or otherwise disliked, even in the US.

Some early examples of domestic surveillance

- 1795, Buncombe County
- Secret Service
- Confederate Signal Corps
- Counter Intelligence Corps (WWII)

Project VENONA (1941-1980)

- Run by precursor to NSA
- Focused on intercepting Soviet cables and decrypting them using a very serious cryptographic error
- The FBI, intelligence agencies, and Army explicitly kept the president from knowing about the program for security reasons
- Run by the Army Signal Intelligence Service (SIS)
- Very little solid information on how the cables were collected, but it is possible they were acquired via mass surveillance

PROJECT SHAMROCK (1945-1975)

- The NSA was given access to microfilm copies of every single telegram that was sent to, from, or through Western Union, and some of its sub companies such as ITT and RCA.
- Any “useful or interesting information” was passed on to the FBI, the BNDD, or DoD
- There were no warrants or any court authorization of any kind.

PROJECT SHAMROCK (1945-1975)

- An interception of every telegraph entering, leaving, or transiting the United States.
- Although ostensibly for searching out and decrypting for foreign surveillance, it also explicitly targeted American citizens.

OPERATION CHAOS (1964-1973)

- Domestic CIA program that began looking for foreign influences involved in anti-war movement and potential espionage but ended up attempting infiltration of the counterculture movement as a whole.
- Opened mail to and from USSR, to and from people on watchlists, identified and surveilled “radical groups”, anti-war movement members, and black nationalist groups, along with “groups who may pose a threat to CIA agents or property”.

PROJECT MINARET (1967-1973) **Cont. of SHAMROCK**

- A program targeting both foreign people and organizations as well as US citizens in the US whose actions "may result in civil disturbances or otherwise subvert the national security of the U.S."
- Collected virtually all ingoing and outgoing communications of almost every kind based on a selected watchlist of people and organizations
- Distributed information collected from this to the FBI, CIA, Secret Service, Bureau of Narcotics and Dangerous Drugs(precursor to DEA), and the DOD.

COINTELPRO

- Run by the FBI to enable “protecting national security, preventing violence, and maintaining the existing social and political order by "disrupting" and "neutralizing" groups and individuals perceived as threats.”
- This included black nationalist groups, political liberals, communists and socialists, and political dissidents.
- The FBI also specifically targeted MLK, Malcolm X, and other key figures, "to pinpoint potential troublemakers and neutralize them ***before*** they exercise their potential for violence [against authorities]." (bolded/italicized for emphasis)
- At times coordinated with the CIA, NSA, and DOD to prepare a military response to rioters and protesters.

Carnivore

- FBI program design to intercept certain internet or electronic communications, initiated in the early nineties to late eighties.
- Used a computer physically mounted to an ISP’s network.
- Had an advanced content filter system that essentially scanned all passing emails with a complex content detection system

Narus Insight

- After Protests over the Carnivore system by multiple rights groups, the government quietly changed the name to DCS1000, before scrapping it for a new program called Narus Insight
- Insight is a commercially produced system with more surveillance feature than Carnivore
- It is a complex supercomputer directly attached to AT&T's internet backbone server in San Francisco
- Specifically designed to intercept or block certain messages as designated by the software settings
- CALEA compliant

Which brings us to the CALEA (implemented in 1994)

- Federal law requiring telecommunications companies to allow “back door” federal access to phone calls or other communications, internet or otherwise
- Allows for, or has been argued to allow for, warrantless phone taps, VoIP taps, and email interception

Oh, and ECHELON, can’t forget that.

- Established in the early sixties to monitor the Soviet Union’s communications traffic.
- By the late 80’s it had been adapted to civilian and commercial communications
- Purportedly capable of intercepting and reading or listening in on the vast majority faxes, phone calls or texts, email, public phone switchboards and even satellite transmissions.
- Prompted the use of encryption in EU member state businesses, as the technology involved was likely used to steal industrial secrets from those businesses.
- If you can’t guess from what I just said, this capability was in use in the 90’s…. a full decade before 9/11.

Warrantless Wiretaps

- Did NOT begin post 9/11.
- Began in June of 2000, over a full year before 9/11

MARINA (on to the fun stuff)

- This is a system that holds and retains all of your personal internet metadata for at least 1 year, even if you are NOT designated as a suspicious person or a foreign terrorist.
- Internet metadata includes everyone you communicate with, why, when, and how. It also includes things you might not expect, such as GPS tracking information embedded in photos you have taken(EXIF data), or other personal data embedded into documents.
- The majority of metadata is used in life pattern analysis systems; your data is plugged into a large and complex database, and then used to make educated guesses about who you are and what you do or believe
- This is just a system for managing *your* metadata. Solely the management and study of your data, not the collection.

MAINWAY

- Essentially MARINA for phones
- This database stores information for 5 years or more, significantly longer than MARINA

PRISM

- Collects the metadata fed into MARINA, along with significant amounts of actual, “real” data, including google searches and in some cases facebook or social media information.
- Program forced internet companies to turn over more data, including the decryption of encrypted data, or face legal action.
- May or may not have involved hacking into a very large number of universities, hospitals, and businesses in foreign countries to acquire more data, but this cannot be confirmed or denied

The Gemalto hacks

- In 2010 and 2011, the NSA and GCHQ (government communications headquarters, the UK equivalent of the NSA) hacked into a Netherlands company called Gemalto, the largest producer of SIM cards in the world.
- Although the reports are very conflicting, the generality is that the NSA and GCHQ may have stolen a vast sum of encryption keys off that allow them to theoretically decode securely encrypted messages sent over 2G phone networks.

YOU ARE BEING TRACKED

License Plate Readers Explained

ACLU BECAUSE FREEDOM CAN'T PROTECT ITSELF

License plate tracking

- A complex system of cameras that capture your license plate via a specialized camera and software, then record it to a database
- very very handy for metadata analysis, because it shows specifically where someone physically is even without a stingray device or if they aren’t carrying a phone

Stingray

- Remote access phone tool
- Can:
    - See all your texts
    - record all your calls
    - force your phone to connect to it and give up your encryption keys
    - break into your phone and steal stored data
    - install malware or malicious software
    - track your movement and record it
    - be used on you at any time. without a warrant.
- The CIA worked with the US marshal service to test it…. by strapping units to small planes and flying them over cities and towns to scoop up data.

Uh-oh. Let's repeat that again.

The CIA and FBI. Strapping stingrays to planes. And flying them over your house. Yeah. That happened.

Domestic/Urban Surveillance Flights

These planes also come equipped with:

- Stabilized Electro-optical sensor arrays (really big cameras)
- Infra-red cameras
- Motion Tracking software

Shell corporations

Why does this matter?

- If the above reasons aren’t enough for you, these planes (and a few helicopters, possibly) are not only used for general surveillance tasking, but also to monitor protests or “potential criminal activity”.
- At least one was provided to Baltimore PD to help watch the recent unrest in the area.

“The exact number, basing location, and types of aircraft operated by the FBI's Surveillance and Aviation Branch is classified.”(Ars Technica,)

But why? Where does the Stingray Data go?

For the most part, we have no idea why. But the data goes to the FBI, the ATF, the DEA, local police departments, the US marshals…. Well, maybe. The FBI uses them, local and state police officers use them, the DEA uses them, and the ATF may have acquired a few as well. But the data collection itself has essentially zero accountability.

Metadata Analysis

it’s plugged into a specialized supercomputer system that uses it to analyze your:

- movement
- calling and texting patterns
- your internet usage
- emails
- purchasing habits.

“Wait, WHAT?”

Yep, that’s Metadata analysis: a super complex program guesses what you do for a living, where you live, who you’re dating, what your political beliefs are, your sexual orientation, where you like to go for lunch, how much money you make, what your hobbies are….

“But that’s an insane amount of information!”

Yes. In fact, it’s so much, the NSA is running out of space to record it all. So that’s where the UDC comes in.

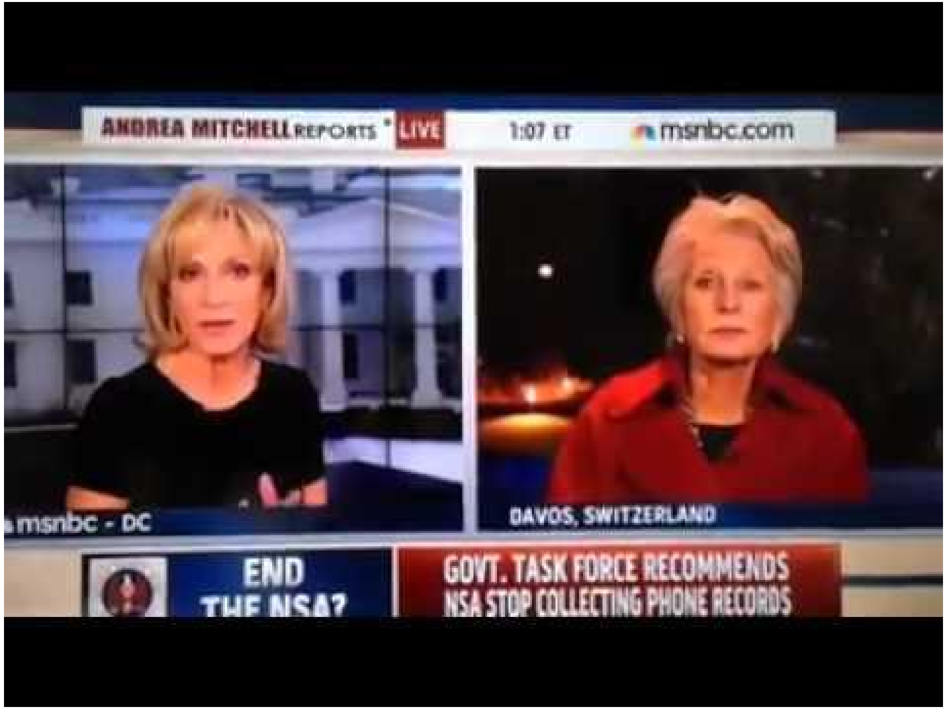
Oh, right, you don’t know what that is yet.

It’s a freaking huge server farm, designed to process, assess, and store YOUR metadata. And by your metadata, I mean everyone's. Forever.

The facility has been speculated to contain *exabytes* of storage space. An exabyte is is 1 million gigabytes.

Lets look at that again.

Which brings me to…. Yeah, the government is probably actively trying to hide this from us.



Jane Harman

- Former congresswoman from California
- Initially supported warrantless wiretaps
- The previous video was her attempting to suggest that we should seriously investigate current NSA programs for legality and civil rights violations

Stingray court cases

One quick example on why this really really matters.

Silk Road 2.0 , in a nutshell.

The FBI:

- Cannot or will not account for how it accessed the Silk Road servers in a plausible manner
- How it discovered or found the Silk Road servers in the first place
- Prosecutors have openly suggested that even if they did actually hack into silk road contrary to what the FBI testified to in court, it would still have been a legal search, while still carefully denying that they hacked into the site in what would widely be regarded as not only perjury, but also illegal hacking.
- The FBI admits that it collected Robert Ulrich’s metadata, but NOT his “actual” data.

Other notable comments related to the topic

- "What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law. I am a huge believer in the rule of law, but I am also a believer that no-one in this country is beyond the law." - James Comey, current FBI director, on why smartphones should not be encrypted in a manner that stops the FBI from accessing the contents

So, let’s review.

- The government is currently tracking all your texts, phone calls, and internet browsing.
- It is currently tracking your current location based on your cellphone’s GPS and your car’s license plate.
- All of this data is already in a server where it will remain for at least 1-5 years
- Not only is this server searchable without a warrant, it is designed to help agents profile you based on your data.
- The NSA is not drawing down this capability; it is actually expanding it and attempting to increase it’s ability to profile people based on their internet traffic, phone usage, and physical location.
- The government is likely attempting to cover up or withdraw from public view the majority of these things through media manipulation or by simply refusing to acknowledge it.
- This has been going on for decades.

Link List

http://arstechnica.com/tech-policy/2015/04/alleged-getaway-driver-challenges-stingray-use-robbery-case-dropped/

http://arstechnica.com/tech-policy/2014/11/prosecutors-drop-key-evidence-at-trial-to-avoid-explaining-stingray-use/

https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html

Copy of the NDA:

https://www.documentcloud.org/documents/1727748-non-disclosure-agreement.html#document/p3/a212440

Link list (continued)

http://www.huffingtonpost.com/2015/06/02/fbi-surveillance-flights_n_7490396.html

http://arstechnica.com/tech-policy/2015/05/the-fbis-secret-air-force-watched-the-streets-of-baltimore/

http://apnews.myway.com/article/20150602/us--fbi_surveillance_flights-e2320f0d2a.html

http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abIV0cO64zJE

More links

http://www.wired.com/2014/09/the-fbi-finally-says-how-it-legally-pinpointed-silk-roads-server/