Privacy Under the Era of Mass Surveillance

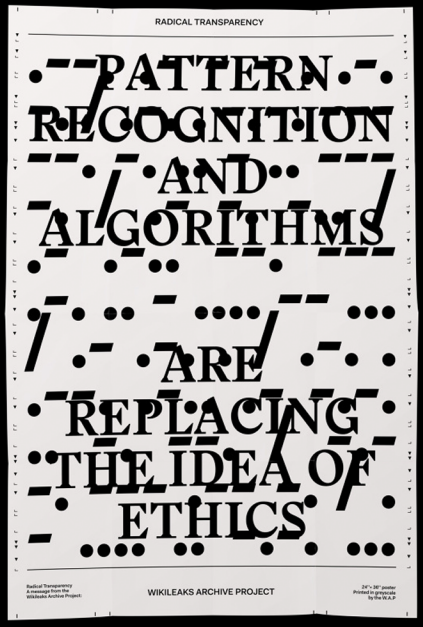
+ What is Mass Surveillance?
+ Who allows & conducts it?
+ Who gets targetted?
+ How to secure your:
  - Identity
  - Browser
  - Computer
  - Communications
  - Phone
  - Activism

there is no transparancy without awareness

What is Mass Surveilance?

Contrary to popular assumption the development of stronger oversight mechanisms in the United States, actually lead to greater secrecy, self-regulation, and abuse of power rather than security and protection.

The rise in this era of mass surveillance is a parallel systematic procedure conducted by internet companies such as Google and Facebook and government entities such as the NSA, CIA, and the FBI.



History of Surveillance

The field of computer security & traffic analysis was first studied, often in secretive organizations, to guarantee properties of interest to the military. Since then we've seen advances in the security and analysis needs of commercial circles: computers, networks, private individuals and civil society.

• 1919 - 1929: The Black Chamber/MI-8 the first U.S. peacetime intelligence agency

• 1939: FBI Index List: 10M Americans { wire taps, cable taps, mail tampering, garbage filtering and infiltrators}

• 1945: SHAMROCK: Major communications W.U/RCA gathered all telegraphic data

• 1956: COINTELPRO: program in the 1950s and '60s, when the FBI spied on, harassed, and tried to discredit leftists, civil rights leaders, and anti-war protestors.

• 1962: NSA: President Truman Establishes the National Security Agency

• 1973: Supreme Court Rules Warrants Are Required for Domestic Intelligence Surveillance

• 1975-76: Frank Church Committee Hearing: Intelligence abuses by the FBI, CIA, IRS and NSA. The committee exposed how agencies spied on American citizens for political purposes during the Kennedy, Johnson and Nixon administrations.

• 1978: Foreign Intelligence Surveillance Act (FISA) Signed Into Law, Protecting Americans from Domestic Spying. Setting up the Foreign Intelligence Surveillance Court to consider requests for secret warrants for domestic spying.

• 2001: Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act: Used to expand domestic surveillance capabilities

• 2007: Protect America Act: Amendment to the FISA, removes the warrant requirement for government surveillance of foreign intelligence targets "reasonably believed" to be outside of the United States

•2008: Foreign Intelligence Surveillance Act of 1978 Amendments Act: Has been used as the legal basis for mass surveillance programs disclosed by Edward Snowden in 2014

Mass Surveillance is a Global Issue

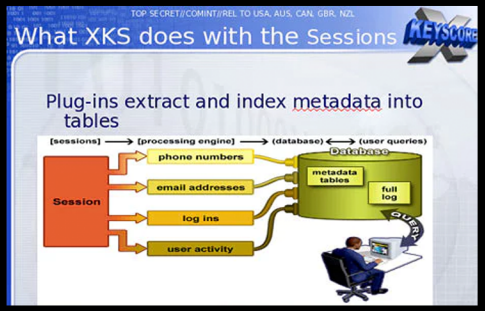
In 2014, the world was hit with a shadow reality due to Edward Snowden's Global Surveillance disclosures. Edward Snowden is a former Central Intelligence Agency employee and a National Security Agency contractor. As a contractor for the NSA, Edward saw first hand the abuse of power and control of the United States against it's own people and several other countries. "Many of the programs were aimed at the American population, but dozens of countries around the planet — including democracies typically considered US allies, such as France, Brazil, India and Germany— were also targets of indiscriminate mass surveillance "

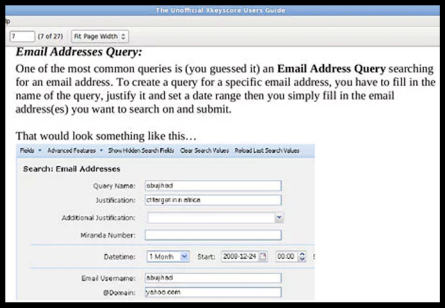
In response to the NSA's activities Snowden copied and leaked global surveillance programs conducted by the United States NSA, and NSA's allies the "Five Eyes" composed of Britain, Canada, Australia and New Zealand.

dont.send.us.flowers
send.us.secrets

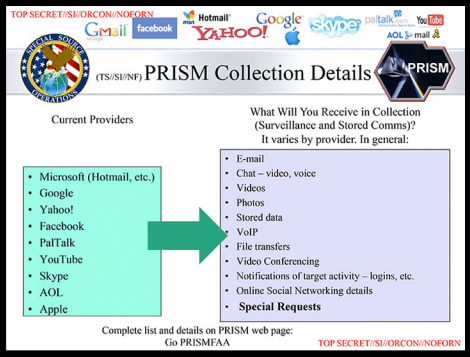
Mass Surveillance Systems

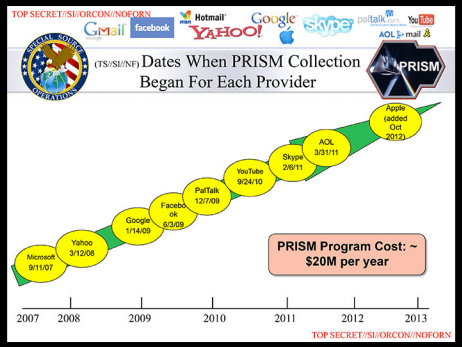
XKeyscore: used for searching and analyzing global Internet data, uses user metrics to flag certain data, such as race, sex, ethnicity, and geolocation

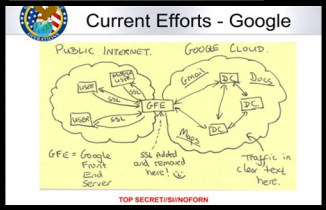




PRISM: collects internet communications from at least 9 major US internet companies. "the number one source of raw intelligence used for NSA analytic reports"

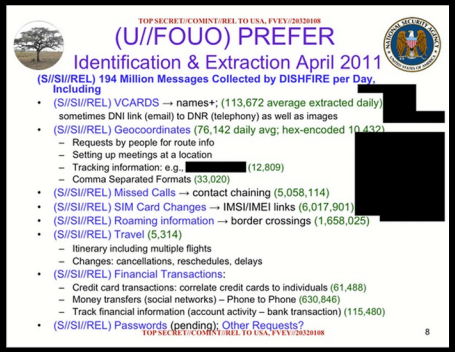


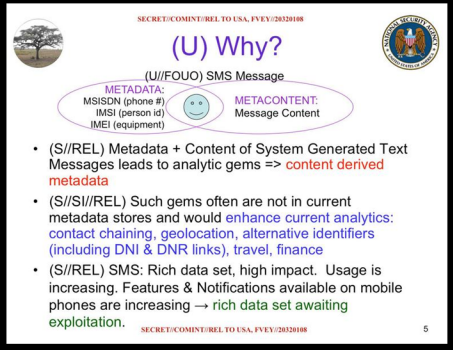


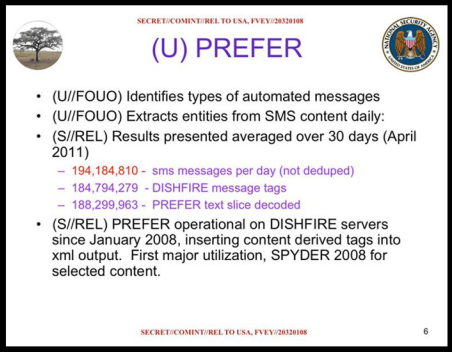


Dropmire: surveillance of foreign embassies and diplomatic staff, including those of NATO allies. At least 38 foreign embassies were under surveillance starting from 2007

DISHFIRE/Prefer: Collection system and database run by the (NSA) and the UK's Government Communications Headquarters (GCHQ) that collects hundreds of millions of text messages on a daily basis from around the world

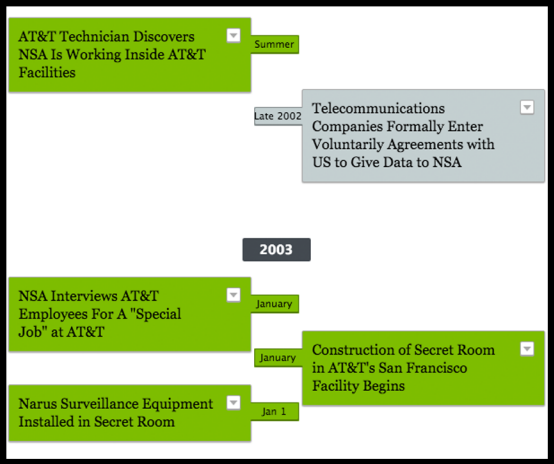


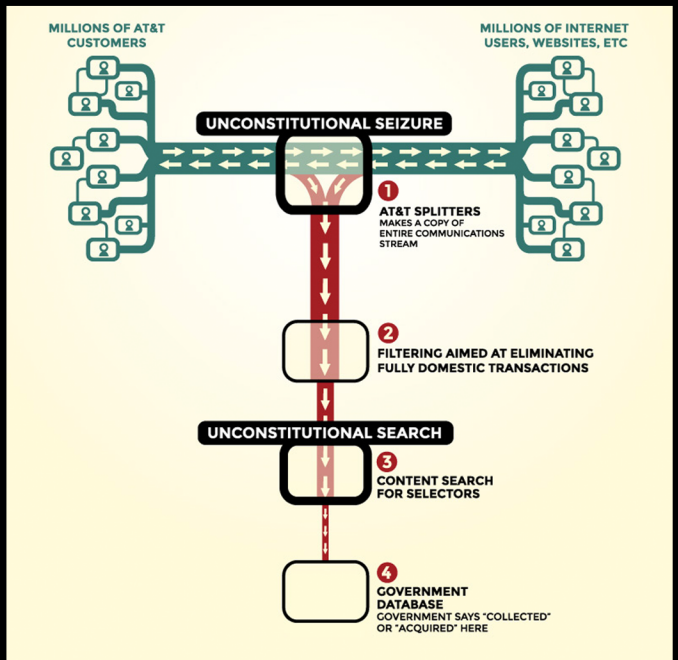




TEMPORA: "Mastering The Internet" uses intercepts on the fibre-optic cables that make up the backbone of the Internet to gain access to large amounts of Internet users' personal data, without any individual suspicion or targeting.

AT&T, MCI, Sprint, Verizon





BULLRUN: is a highly classified program to crack encryption of online communications and data. The most expensive program ~800M

Digital Collection System Network (DCSNet): is the Federal Bureau of Investigation (FBI)'s point-and-click surveillance system that can perform instant wiretaps on almost any telecommunications device in the US

MYSTIC: collects the metadata as well as the content of phone calls from several entire countries. MYSTIC operates under the legal authority of Executive Order 12333

BOUNDLESSINFORMANT

OVERVIEW
(LAST 30 DAYS)

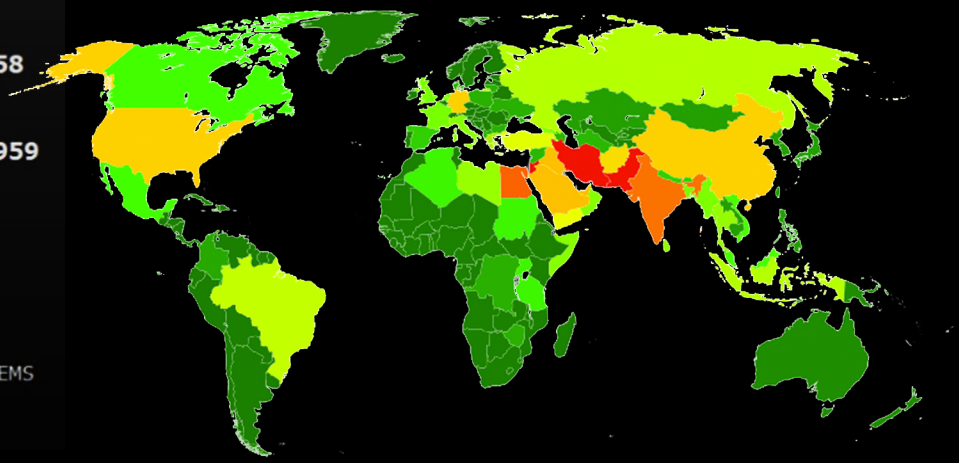
TOTAL DNI
97,111,188,358

TOTAL DNR
124,808,692,959

SIGADS
504

CASE NOTATIONS
27,798

PROCESSING SYSTEMS
2,431



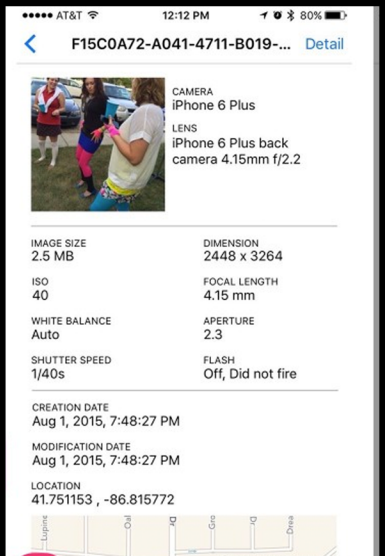
JANUARY, 2007
USA: 3B

TOP 5
PAKISTAN
AFGHANISTAN
IRAN
JORDAN
INDIA

BoundlessInformant is counting and analysing DNI (internet) and DNR (telephony) metadata records passing through the NSA's signals intelligence systems, and are therefore not showing how much content of internet and telephone communications is intercepted

Your meta-data knows you better than anyone else.

Metadata is the information about information.
Communication metadata collects information about the senders and receivers. This includes, phone numbers, email addresses, screen names etc. Attached with this information is information on the time, duration and location of the communication. On top of this it stores information about the device used for the communication. This includes make, model, OS, and just about anything else it can collect.
Metadata is collected for almost anything digital, or "smart" hardware, otherwise known as the Internet of Things.
For example, metadata that often goes without mention is photo metadata which is commonly known as EXIF data. Similarly to communication metadata, photo metadata stores everything it can. For example this includes, GPS location, make/model, time and even the application used to edit the photo.



Google Play: Exif Eraser

iOS: Photo Secure

Windows: GIMP or Photo Properties

MacOS: ImageOptim

Online Trackers

Analytics:

Google Analytics as well as hundreds of tracking companies can collect a lot of data about how people use a website/app. At its most basic, these companies can view the following:

- Time of visit, Pages visited, Time spent on each page
- Referring site details (URL the user came through to arrive at this site)
- Type of web browser
- Type of operating system (OS)
- Flash version, JavaScript support, screen resolution, and screen color processing ability
- Network location and IP address.
- Scroll Depth
- Clicks on links, videos, document downloads

Cookies

Browser Fingerprinting

Mobile Devices

Deep Packet Inspection

History Sniffing

Internet Privacy Tools

HTTPS Everywhere

DuckDuckGo: Secure Search Engine

uBlockOrigin: Advanced Ad Blocker

Google Analytics Opt-out Add-on

Privacy Badger: Blocks Trackers

Ghostery: Blocks Trackers

uMatrix: Advanced blocking

WebRTC Leak Prevent

ZenMate VPN *(free)* : PIA VPN *(paid)*

Use Incognito/Private

iOS: Purify: Ad + Tracker blocker

Android: WARP Browser

TAILS: TOR + Secure OS

Communications Privacy Tools

1Password: Secure system allows you to generate strong passwords and securely save and autofill passwords.

PGP Encrypted Email: Proton Mail / Mail Fence

Signal or Wickr Me: Encrypted Messaging App

SIGAINT: a darknet-only service that forces all its users to log in using Tor to read or send email

Riseup.net: provides email, mailing list, VPN, and other similar services to activists around the world. Accounts are free, but you do need invite codes from two friends who already use Riseup in order to create an account.

nCryptedCloud: Encrypted Documents/Cloud Services: Google Drive, OneDrive Dropbox

OnionShare: securely share files

Slack: messaging tool, create private slack name group, group members should not sign up with edu emails, or gmail, proton mail recommended, dont connect with google drive etc..

Social Media Tips

- Follow the internet privacy tips + change and generate stong passwords with 1password.

- Turn on 2-Factor Authentication(2FA): For all your accounts (turnon2fa.com/tutorials)

- Find out what you're leaking to Google:
  myactivity.google.com
  + change your google privacy + location settings

- Find out if you've been a victim of a hack:
  haveibeenpwned.com

- Remove Your Mailing Address From Data Broker Sites:
https://yoursosteam.wordpress.com/2015/08/30/remove-your-mailing-address-from-data-broker-sites/

- Check and update your security/privacy/sharing settings on all your social media sites. Remember that many sites automatically sign you up with the least secure settings.

- Consider having different accounts for different purposes. Set up vulnerable accounts with, encrypted email, VPN/TOR, and a burner phone number.

- Google yourself, your usernames, aliases, emails, numbers etc.

Activist Security Tips

• Use Encryption and Blocking methods, suggested on the previous slide.

• Enable Airplane Mode + don't forget to disable unnecessary location services.

• Have your lock screen on at all times.

• Take Photos/Videos without unlocking your phone

• Remove Fingerprint Lock + Enable 8-16 length password

• Back-up Your Data, and preferrably remove private documents and clear message threads before direct actions.

• If you're really concerned, don't bring your phone at all and consider a prepaid, disposable phone: & don't go back and use the same phone at home, remember cell towers track your location.

• Bike or Walk to actions: Automated License Plate Reader Systems (ALPRs) automatically record the license plates of cars driving through an area, along with the exact time, date, and location they were encountered.

• If you're participating in civil disobedience, mask your identity, dress differently, cover your face with bandanas, hoodies, etc. Remember you're up against facial recognition technology.

Computer Tips

Encypt your computer + Back-up files and keep personal vulnerable files on an encrypted drive.

macOS

FileVault : Encrypt your OS

Little Snitch: Host based firewall used to monitor applications, preventing or permitting them to connect to attached networks through advanced rules.

http://feross.org/spoofmac/ : Spoof your mac address

Keka: Easy tool to compress and password protect files

Windows

VeraCrypt: Encrypt your OS