What's in your file?

James O'Keefe

Boston Security Meetup

Feb. 11, 2016

State Surveillance - Local

- Local police can know where you go and who you see:
  - Automatic License Plate Readers (ALPRs)
  - Public surveillance cameras
- Who you talk to on the phone, where you are, your text messages and phone calls (Stingrays on ground or airborne circling a city near you);
- Leave no poor person unsurveiled:
  - Electronic Benefit Transfer cards (EBT) used for monitoring people receiving government assistance
  - Day laborers in Los Angeles get their fingerprints scanned

State Surveillance – Legal?

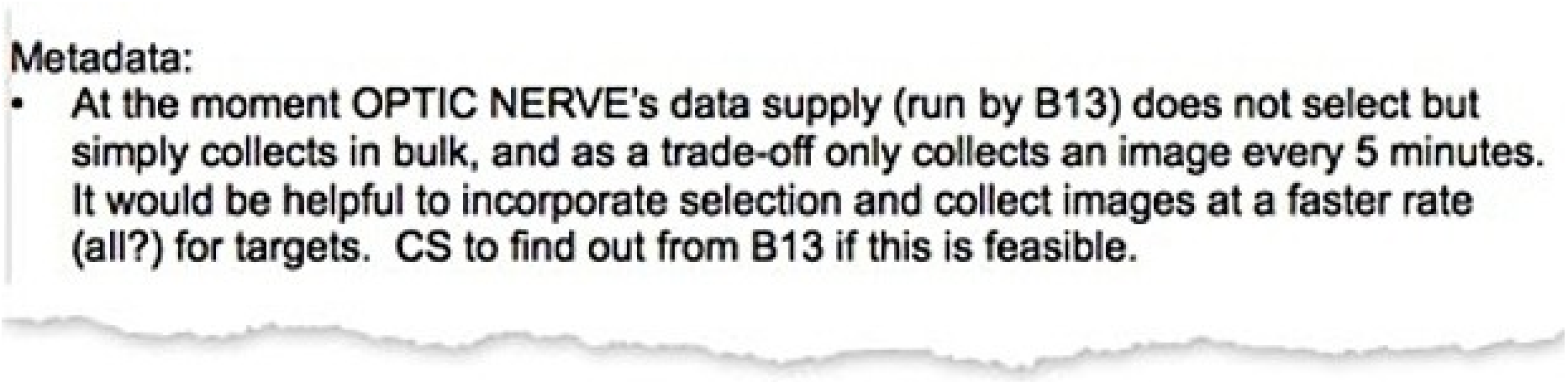
- Foreign Intelligence Surveillance Act (FISA) – 1978 / 2008
- Executive Order 12333 – bulk collection abroad
- USA PATRIOT Act – 2001 – bulk collection at home (Section 215)
- USA Freedom Act – 2015 – some limits on Section 215
- Cybersecurity Information Sharing Act (CISA) – 2015 – that are soon watered down

NSA Leads the Way!

- Internet data including e-mail (PINWALE)
- Intercepting Internet meta data (MARINA)
- Meta data for hundreds of billions of telephone calls made through biggest US phone carriers (MAINWAY)
- At least 200 million text messages/day worldwide as of 2011 (Dishfire)
- All searchable in Xkeystore
- NSA got Deep Packet Inspection

Give Video Some Love

- Skype video accessible since 2011
- UK Government Communications Headquarters (GCHQ) captures Yahoo webcam images in bulk (Optic Nerve)



Metadata:

- At the moment OPTIC NERVE's data supply (run by B13) does not select but simply collects in bulk, and as a trade-off only collects an image every 5 minutes. It would be helpful to incorporate selection and collect images at a faster rate (all?) for targets. CS to find out from B13 if this is feasible.

- 7.1% contained nudity on average.

Sharing Is Caring

- NSA has lots of friends
  - Five Eyes - Australia, Canada, New Zealand, the United Kingdom, and the United States
  - Sweden
  - Germany
  - France
  - And many others
- And if NSA cannot get it legally, they can ask a friend. GCHQ is a great one.

Government Got Your Back?

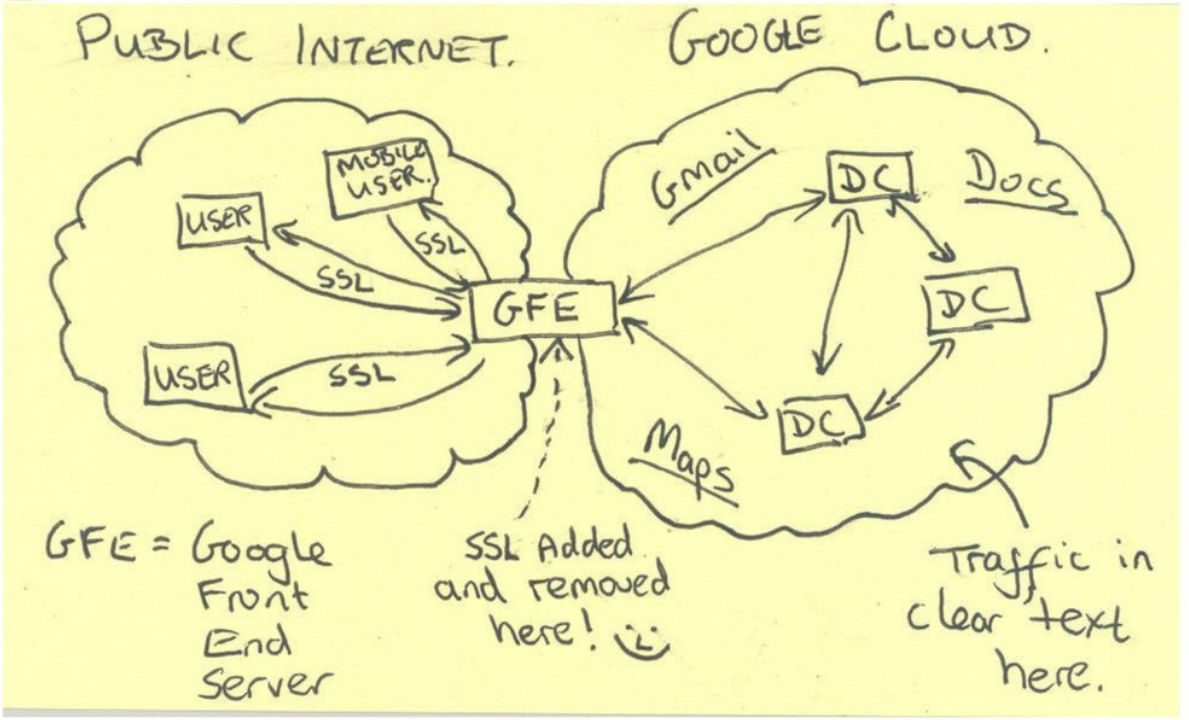
- Heartbleed bug in OpenSSL's SSL/TLS encryption support for two years
- Shellshock Unix 'bash' bug decades old
- Poodle bug yields more SSL vulnerability
- Backdoor in Juniper Network's ScreenOS allowed access to OS and ability to decrypt their VPNs for over three years

Probably Not

- NSA cracks Google & Yahoo data center links

TOP SECRET//SI//NOFORN

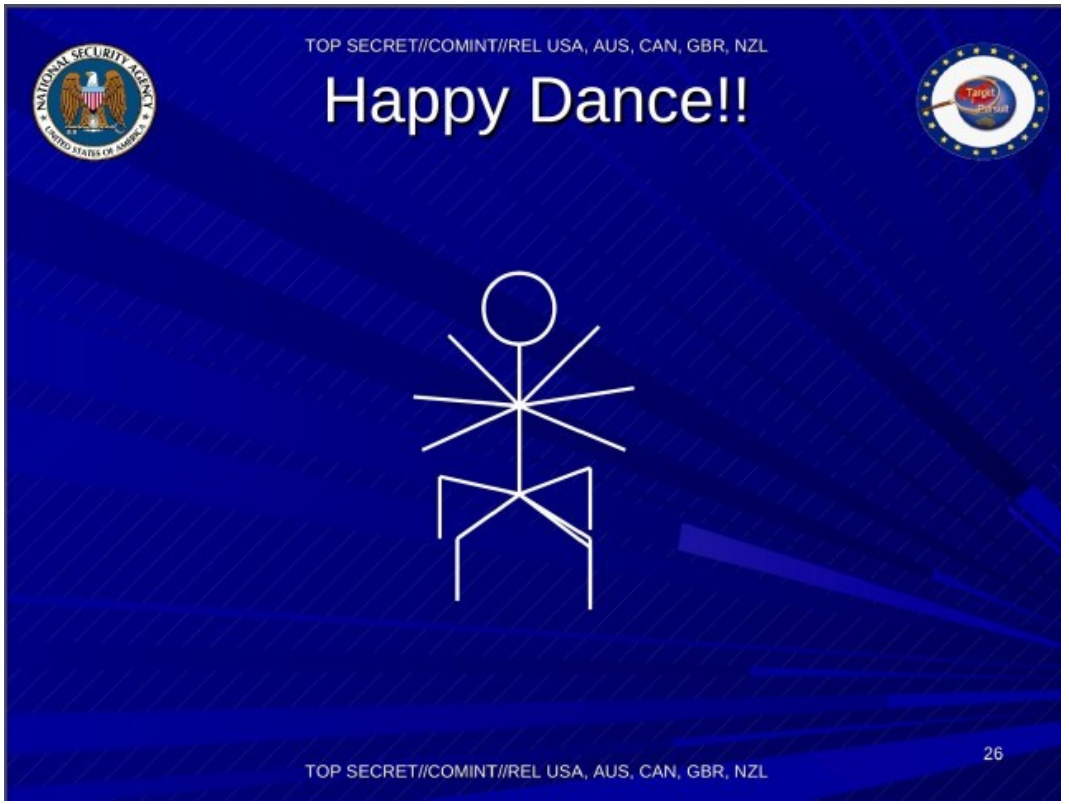
Current Efforts - Google



TOP SECRET//SI//NOFORN

Probably Not²

- National Security Agency's Office of Target Pursuit (OTP) maintains a team of engineers dedicated to cracking the encrypted traffic of virtual private networks (VPNs)



(Probably Not)^3

- National Security Agency (NSA) has been undermining encryption standards (BULLRUN)
- $250m-a-year US program works covertly with tech companies to insert weaknesses into products
- Weakened NIST encryption standards
- Random number generator Dual_EC_DRBG contains a back door from the NSA. RSA used it until September 2013
- $10 million dollar contract to RSA to adopt Dual_EC_DRBG

Corporate Surveillance

- Enables government surveillance
- Corporations get your data
- Sell it to the government
- Profit!

Corporate Surveillance

- Your debts. Credit reports are so old school
- What you buy
- What you search – for ads
- What pages you visit – for ads
- Everything on social media – for ads & other targeting
- What you eat and how active you are (Fitbit …)
- Who you know (Google Contacts/Mail, mobile apps)
- Where you go (mobile apps)

Big Data - Big Brother

- Target knows if you are pregnant
- Uber knows if you had a one night stand
- Facebook plays social engineering games on your feed
- Xbox – Always listening
- Apple – Hi Siri

Big Data – Insecure Data

- Target
  - 40 million debit/credit records
  - contact info for 70 million customers
- JP Morgan Chase - contact info for 76 million customers
- Ashley Madison – 32 million registered users
- Anthem – 80 million patient records
- US Office of Personnel Management (OPM) - 21.5 million personal records, a million fingerprints (better not use Touch ID on your iPhone without a pin)

Internet of Spying Things

- Your car knows how you drive (your insurance company is very pleased)
- Don't pay your car payment? Car won't turn on
- Your baby monitor is searchable on the web
- Wifi-enabled pacemaker – What could go wrong?
- Encryption is job 10.1 – Time to market baby!
- New surveillance vector – Cause ISIS uses Nest

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

- Edward Snowden

Join the cryptoparty list:

https://lists.mayfirst.org/mailman/listinfo/cryptoparty_masspirates.org/

Slide deck will be at:

https://jamesokeefe.org

I have Pirate Party buttons

jokeefe@jamesokeefe.org