Challenging mass state surveillance

with transparency, obfuscation and accountability

Andrew Clement
Fac. of Information, Univ. of Toronto
The New Transparency: Surveillance and Social Sorting
http://IXmaps.ca http://iprp.ischool.utoronto.ca/

Dig.IT CRYPTO 2.0

IT University of Copenhagen
Oct 4, 2016

What is
mass internet surveillance?

"Collect it all" from traffic and servers

PRISM collection

TOP SECRET//SI//ORCON//NOFORN

(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

TOP SECRET//SI//ORCON//NOFORN

PRISM collection

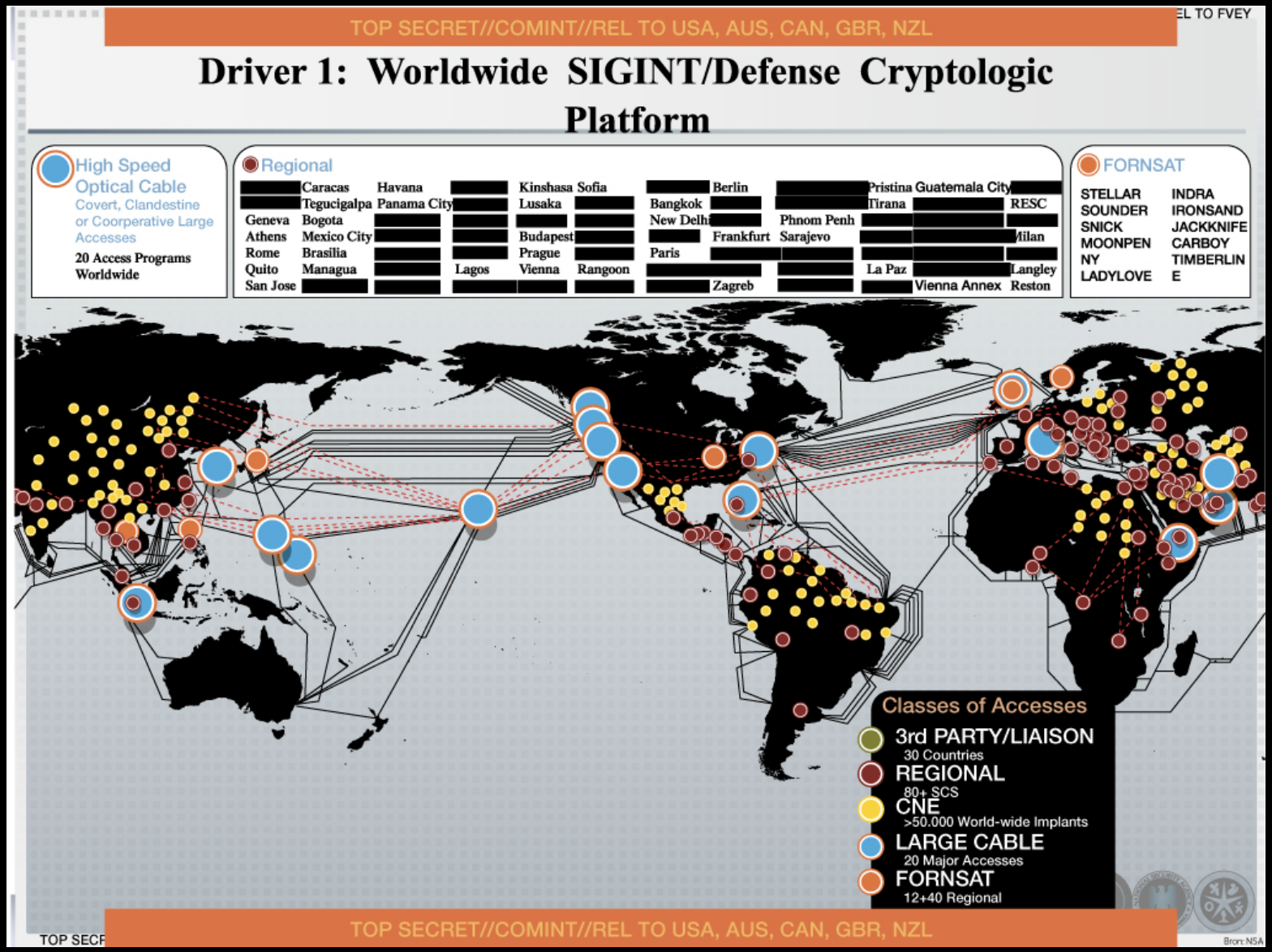
TOP SECRET

- 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**

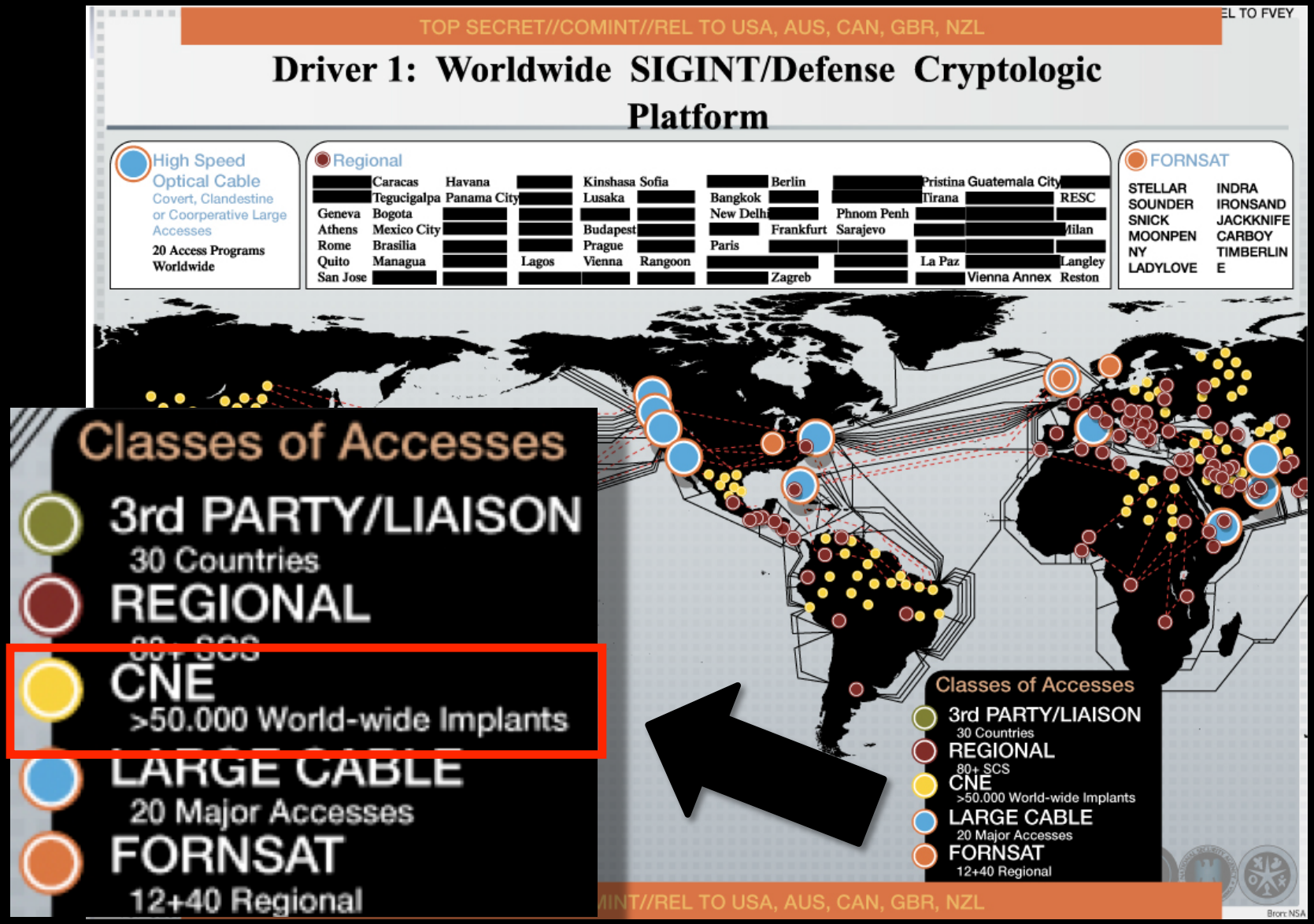
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

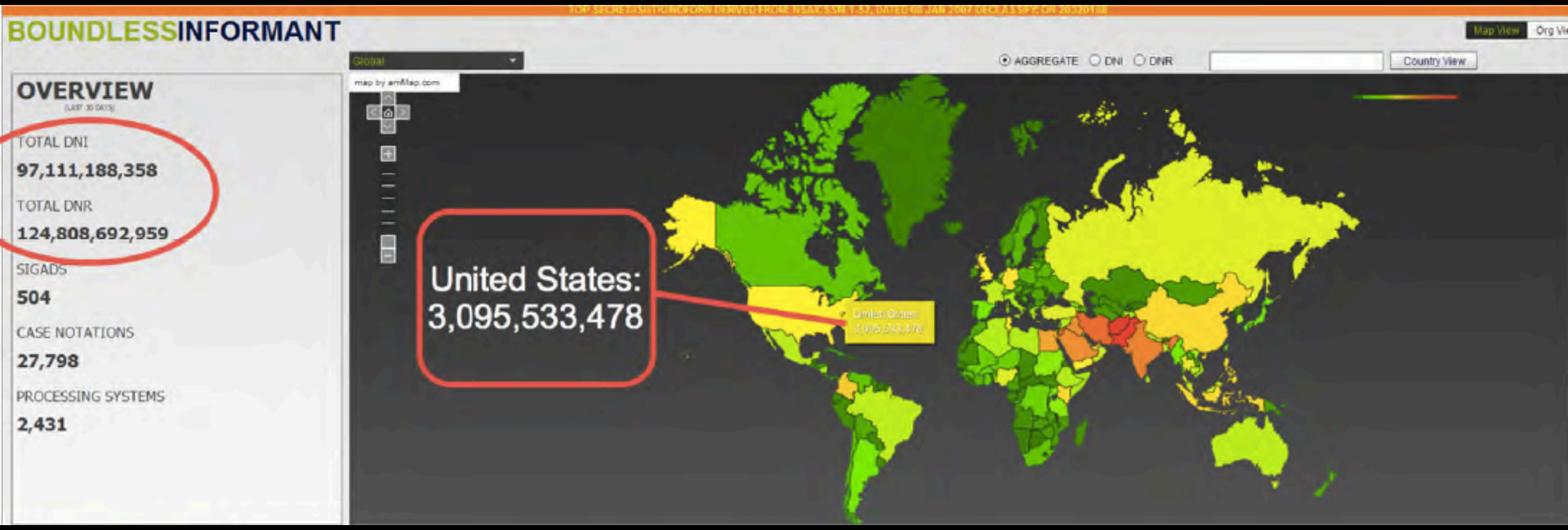
"Collect it all"



"Collect it all" + "Exploit it All"



BOUNDLESS INFORMANT (Mar 2013)



Denmark - 23 million telephone metadata records (in cooperation with the Danish government)

Who does
mass internet surveillance?

NSA 'partner' countries

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Approved SIGINT Partners

Second Parties

Australia
Canada
New Zealand
United Kingdom

Coalitions/Multi-lats

AFSC
NATO
SSEUR
SSPAC

Third Parties

Algeria
Austria
Belgium
Croatia
Czech Republic
Denmark
Ethiopia
Finland
France
Germany
Greece
Hungary
India
Israel
Italy
Japan
Jordan
Korea
Macedonia
Netherlands
Norway
Pakistan
Poland
Romania
Saudi Arabia
Singapore
Spain
Sweden
Taiwan
Thailand
Tunisia
Turkey
UAE

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

NSA 'partner' countries (30)

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Approved SIGINT Partners

Second Parties

Australia
Canada
New Zealand
United Kingdom

Coalitions/Multi-lats

AFSC
NATO
SSEUR
SSPAC

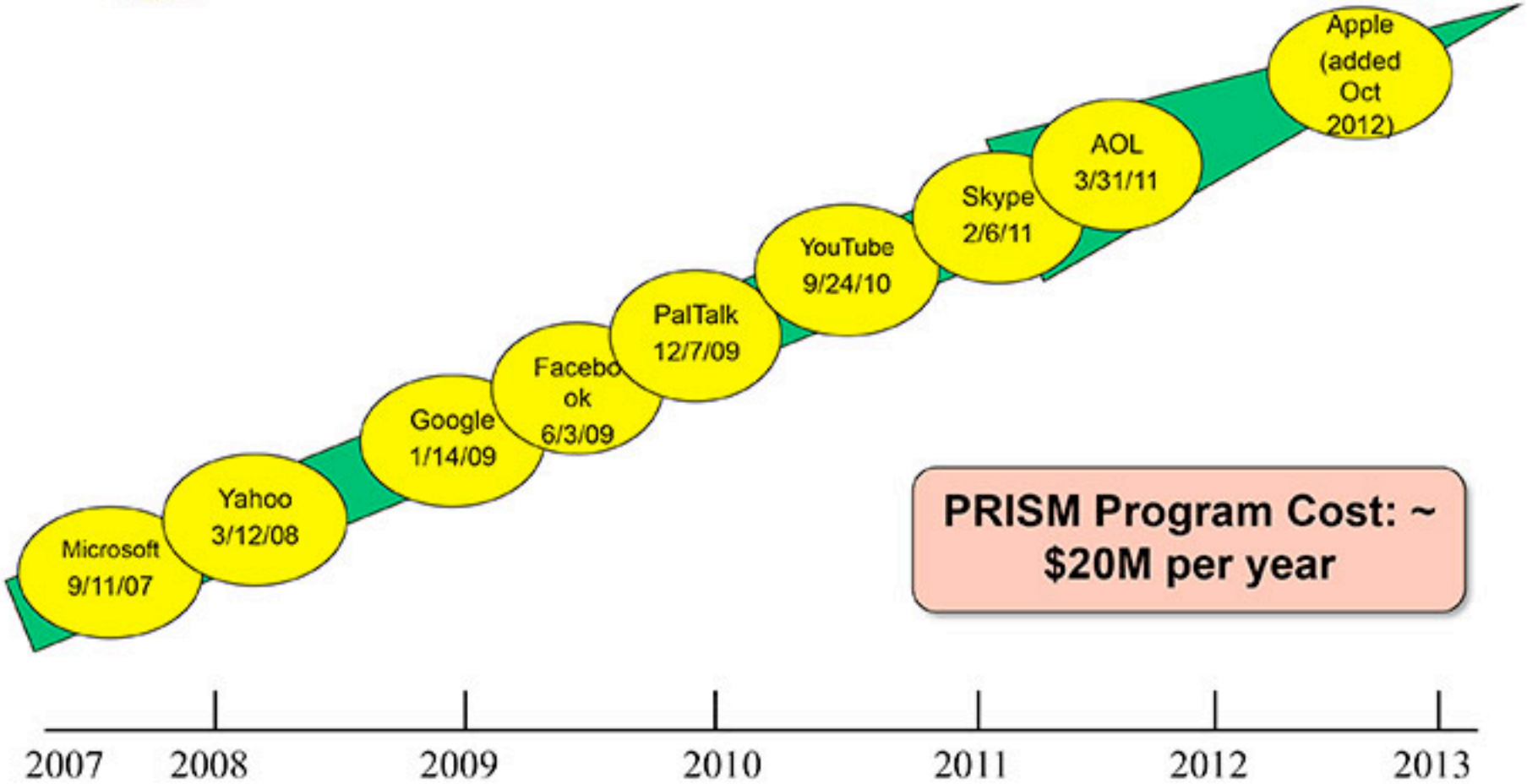
Third Parties

Algeria
Austria
Belgium
Croatia
Czech Republic
Denmark
Ethiopia
Finland
France
Germany
Greece
Hungary
India
Israel
Italy
Japan
Jordan
Norway
Pakistan
Poland
Romania
Saudi Arabia
Singapore
Spain
Sweden
Taiwan
Thailand

Denmark

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ $20M per year

Five Eyes 'partner' carriers (80+)

- ATT (Fairview)
- Verizon (Stormbrew)
- British Telecom (Remedy?)
- Cable & Wireless > Vodaphone (Gerontic)

- +
- Cogent? Level 3? Bell Canada?, Tata, ….

What is the problem with
mass internet surveillance?

What are the problems with
mass internet surveillance?

Problems ...

Personal privacy

Free expression

Free assembly

...

but Rights vs. Security?

(a false tradeoff)

A police surveillance state?

Technology is currently available

"to create a ubiquitous, omniscient police surveillance state."

"[The NSA has] created, along with other government agencies, the potential for a police surveillance state."

"Once you turn on the police intelligence state, you can never turn it off."

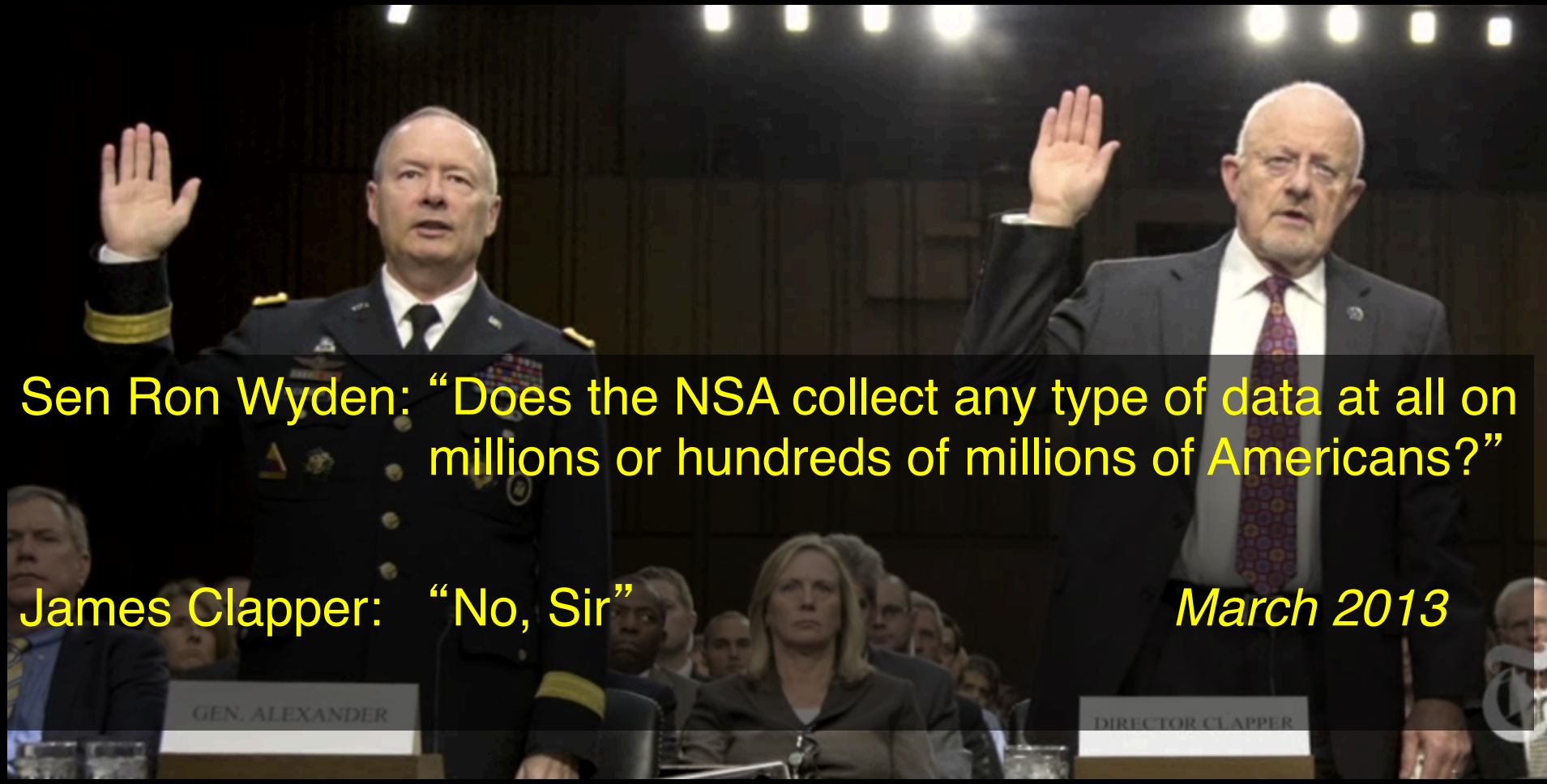
Richard Clarke, Feb 24, 2014
CSA Summit 2014: NSA Surveillance a Pre-cursor to Police State, Says Former US Cyber Czar

Spy chiefs lying before Congress

NSA Director:
Gen. Keith Alexander

Director of National Intelligence:
James Clapper, Jr.

Spy chiefs lying before Congress



Sen Ron Wyden: "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?"

James Clapper: "No, Sir"

March 2013

NSA Director:
Gen. Keith Alexander

Director of National Intelligence:
James Clapper, Jr.

The (democratic) system is broken

"The disclosures that Edward Snowden revealed don't only expose a threat to our privacy but to our democracy itself."

Laura Poitras, 2015/2/22

What can we do about
mass internet surveillance?

?

SALON NEWS POLITICS ENTERTAINMENT LIFE TECH BUSINESS SU

MONDAY, MAR 10, 2014 01:30 PM ART

Edward Snowden: NSA "setting fire to the future of the Internet"

"[T]here's a policy response that needs to occur but there needs to be a technical response that occurs."

Counter-surveillance

Render this secret surveillance apparatus more transparent and accountable

IXmaps

see where your data packets go

Home | Tour | Explore | Contribute | Transparency | News | FAQ | About

Who's looking at your data?

The U.S. National Security Agency (NSA) engages in warrantless internet surveillance. Mark Klein, a former AT&T technician turned whistleblower has revealed that the NSA has installed surveillance equipment at AT&T's main switching centre in San Francisco capable of intercepting all the data passing through it. The NSA is strongly suspected of operating similar spying facilities in 15-20 other U.S. cities. For example, one of our routes shows that data packets from Toronto to the San Francisco Art Institute pass through several such suspected sites. Learn more about who's looking at your data...

IXmaps – Internet mapping platform

IXmaps

see where your data packets go

- Crowdsourced traceroute generation & collection
  > 150K TRs ~ 26K IP addresses
  > 600 contributors/origins ~ 4K destinations
- Systematic geo-location of individual data packet hops
- Map traceroute paths via GoogleMaps (> OpenStreetMap)
  – NSA surveillance, Google data centres, submarine cable overlays
- Custom filtering of traceroutes
  – NSA interception, 'boomerang routing,' ISP, city, ….
- Links hops/routers to ISPs + privacy transparency scores

SNOWDEN SURVEILLANCE ARCHIVE

The Snowden Digital Surveillance Archive

Archive | Portable Archive | Glossary | Help | Preferences | About

http://snowdenarchive.ca/ http://cjfe.org

Open, indexed, searchable archive of published Snowden documents for journalist, academic and lay research

Technical/political responses

Encryption (preferably end-to-end)

- Pretty Good Privacy (PGP/GPG) + ….

Obfuscation

- Tor (the onion router)

Anonymity rights on-line (eg ICANN WhoIs proposal)

Keep cloud hosting local

- Avoid outsourcing to US corps, esp PRISM program providers

Avoid US (boomerang) routing

- Build internet capacity to keep domestic traffic local and route around US & Five Eyes partners

Level 3
Global Crossing
Verizon, Cogent, E
++

Professional/political responses

Insist on transparency and accountability

- Discuss and develop official positions within professional associations (eg PROSA.dk)
- Corporations, esp internet companies
  - eg Transparency reporting about gov access, routing, privacy protections
- Government agencies
  - Independent oversight bodies

Work with Civil Liberties organizations

See where your packets go!
(and contribute to the database)

http://IXmaps.ca

These slides at : http://bit.ly/IXmapsCrypto

Project team:
Andrew Clement, Antonio Gamba, Colin McCann, Jonathan Obar & Dawn Walker
Faculty of Information, University of Toronto

Funding:
Social Sciences and Humanities Research Council (SSHRC)
Office of the Privacy Commissioner (OPC) of Canada
Canadian Internet Registration Authority (CIRA)