Web Technology 2015

Lecture 6. Encrypted and anonymous communication (part 1)

Staas de Jong

Universiteit Leiden > LIACS > Media Technology

Notes beforehand...

- *Today:* there will not be enough time for the subject of Anonymous communication.

- *Proposed solution:* Use WTR presentation slot #10, and move it to the front.

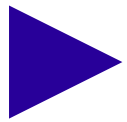
  (+) Perfect introduction to first two student research projects!

  ⇒ **Q:** Which of the other WTR presentations to reschedule to a week later?

Live participatory example: Basic client/server programming

- Using:
  - gedit: a plaintext editor.
    Mac OS X, Windows alternatives: nano, Notepad.
  - Firefox: a web browser – with JavaScript support.
    Alternatives: Chrome, Safari, ...
  - Apache: a web server – with PHP5 support.
    On Mac OS X & Linux: present by default / easy to install.

- Let's begin, with today's DIY assignment...

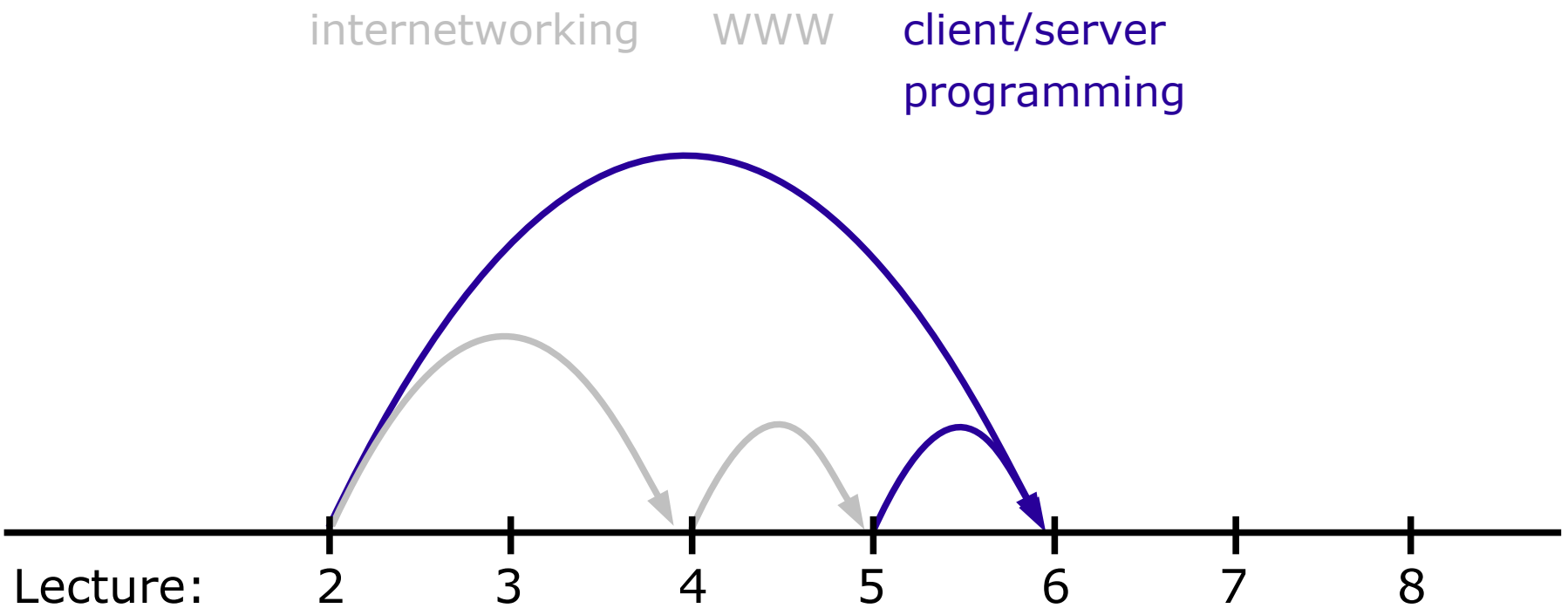


Live participatory example: Basic client/server programming

- Just recapitulated, from scratch:
  - Hypertext: *a basic HTML document.*
  - Interactive hypertext: *a basic HTML form.*
  - Client-side programming: *a JavaScript form checker.*
  - Server-side programming: *capture & store form data with PHP.*

Topical overview

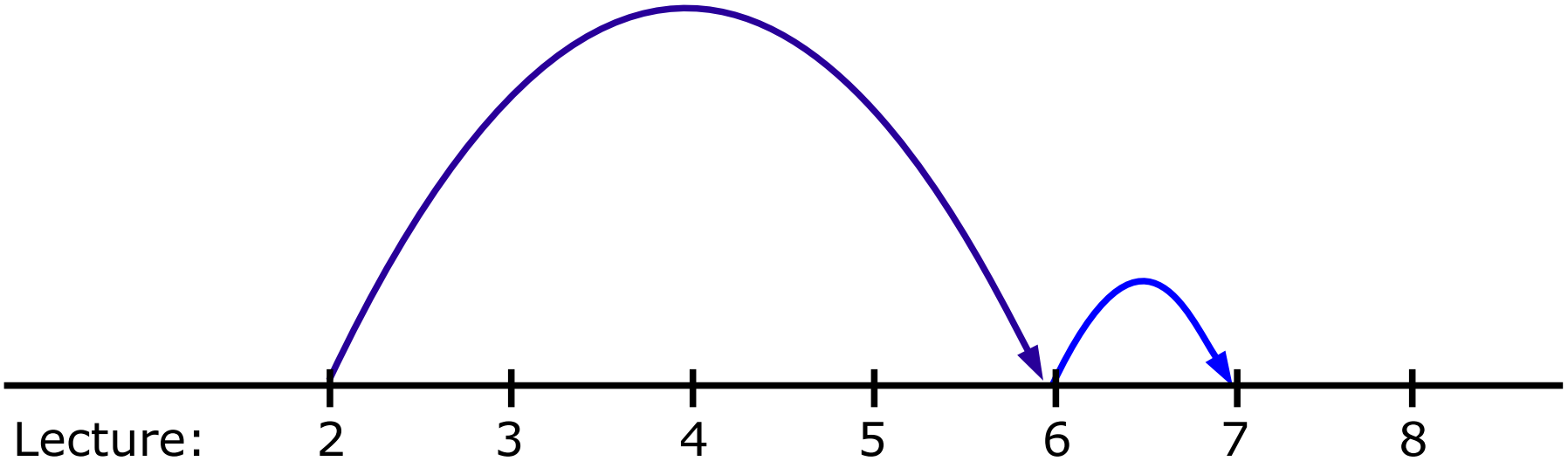
- *Sessions 2-5:* from copper wires
  to client/server programming



Topical overview: today

fundamental subjects

advanced subject



Context: Privacy

- Article 12 from the Universal Declaration of Human Rights:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.

Everyone has the right to the protection of the law against such interference or attacks."

↑ Adopted by the UN General Assembly in 1948. See also *http://www.un.org/en/documents/udhr/index.shtml#a12*

Context: Privacy – the lecturer's view

- *Privacy ~*

  constraints on the knowledge
  that other individuals and social groups have
  of the actions by an individual.

- *(Lack of) privacy* ⇒

  affects the power relationships
  between the individual
  and other individuals / social groups.

↑ *Reason:*

knowledge of an individual's actions
can be used to *exert control* over that individual.

Context: Privacy & power, concrete examples

social group	type of knowledge	type of control	
parents of an infant	*"everything"*	*"everything"*	
plane ticket company	*page views (NB: IP-based!)*	*price increase*	[1]
insurance company	*fitness / medical data*	*admission*	
PRC government	*(keywords in) online conversations*	*delete posts, block account, arrest*	[2]
US government	*2011 case: geolocation of two US citizens*	*lethal drone strikes without trial*	[3]

1 See *http://nos.nl/artikel/640166-booking-heeft-hotel-in-zn-macht.html*

2 See *http://in.reuters.com/article/2011/09/19/idINIndia-59420220110919* and *http://arxiv.org/abs/1303.0597v1*

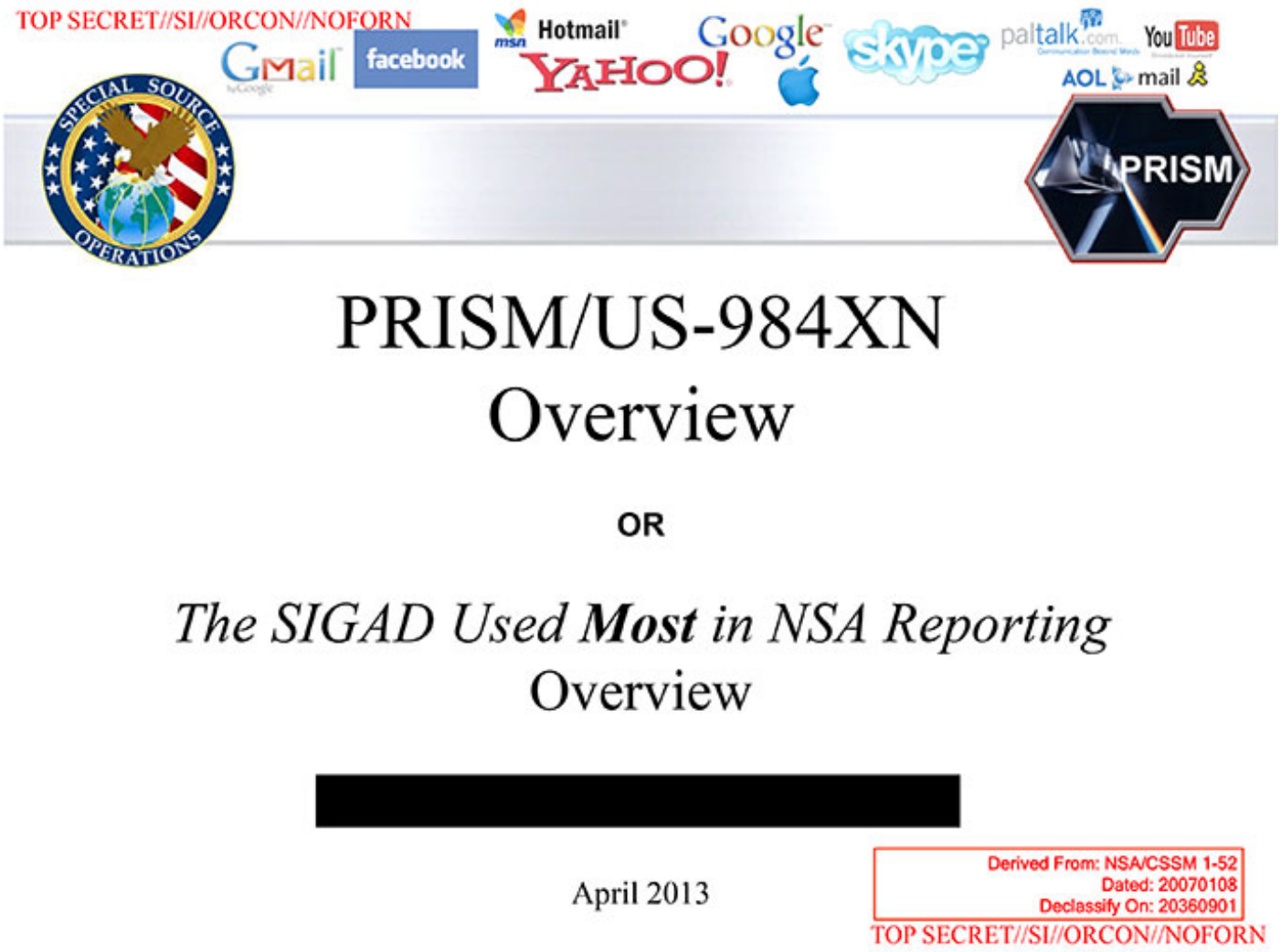
3 See *http://www.theatlantic.com/politics/archive/2013/05/the-killed-at-16-transparency-test-obama-owes-us-answers-about-this-dead-american/276276/* and *http://www.thenation.com/article/173980/inside-americas-dirty-wars?page=full#]erdana*

Context: Internet mass surveillance

"On the Internet, nobody knows you're a dog."

- *Early on (e.g. 1993):* the Internet was synonymous with private & anonymous communication.
  ←
- *Today:* Not anymore!

Context: Internet mass surveillance

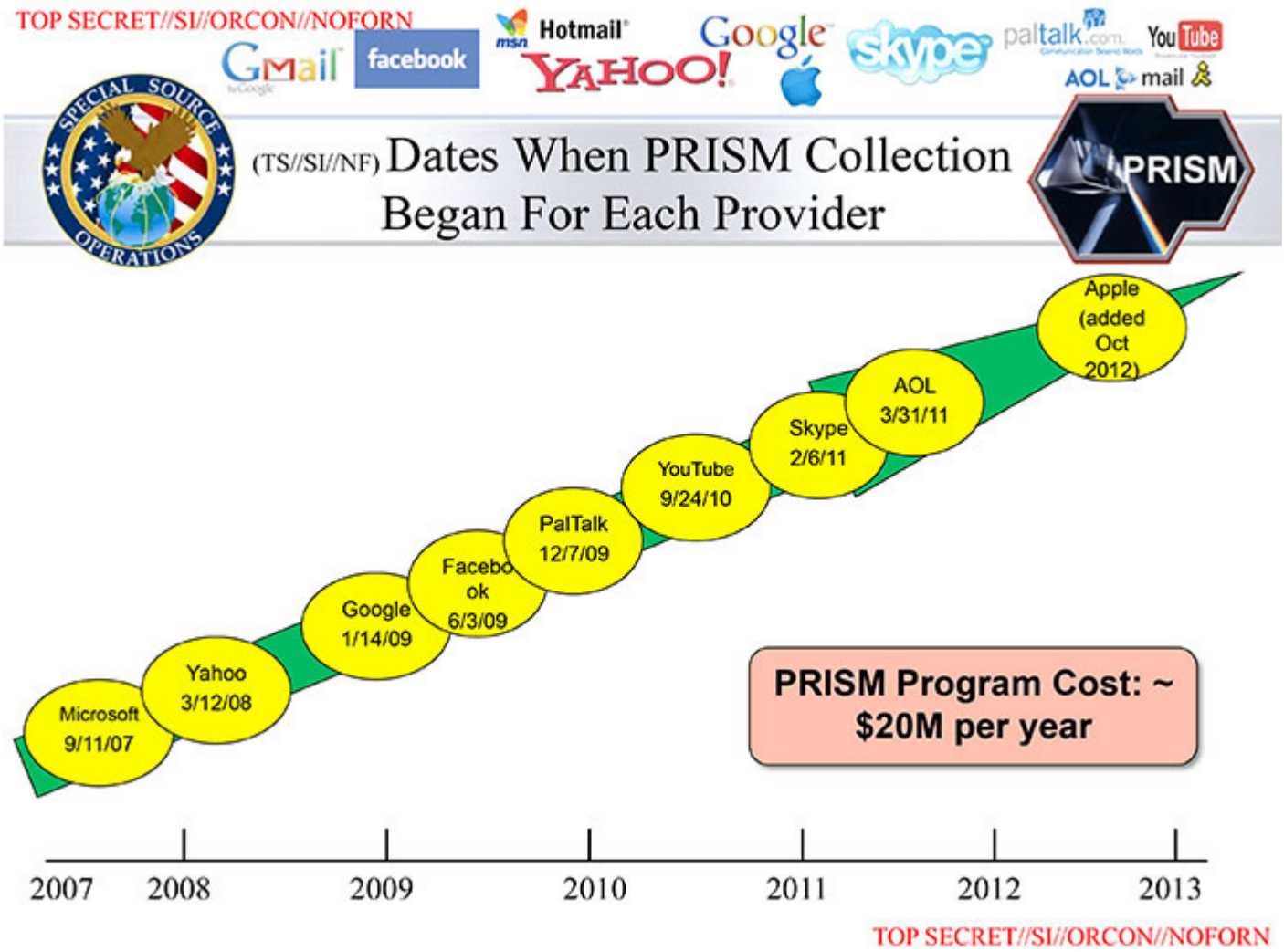


Source: *Edward Snowden,*
via The Guardian & The Washington Post.

Context: Internet mass surveillance

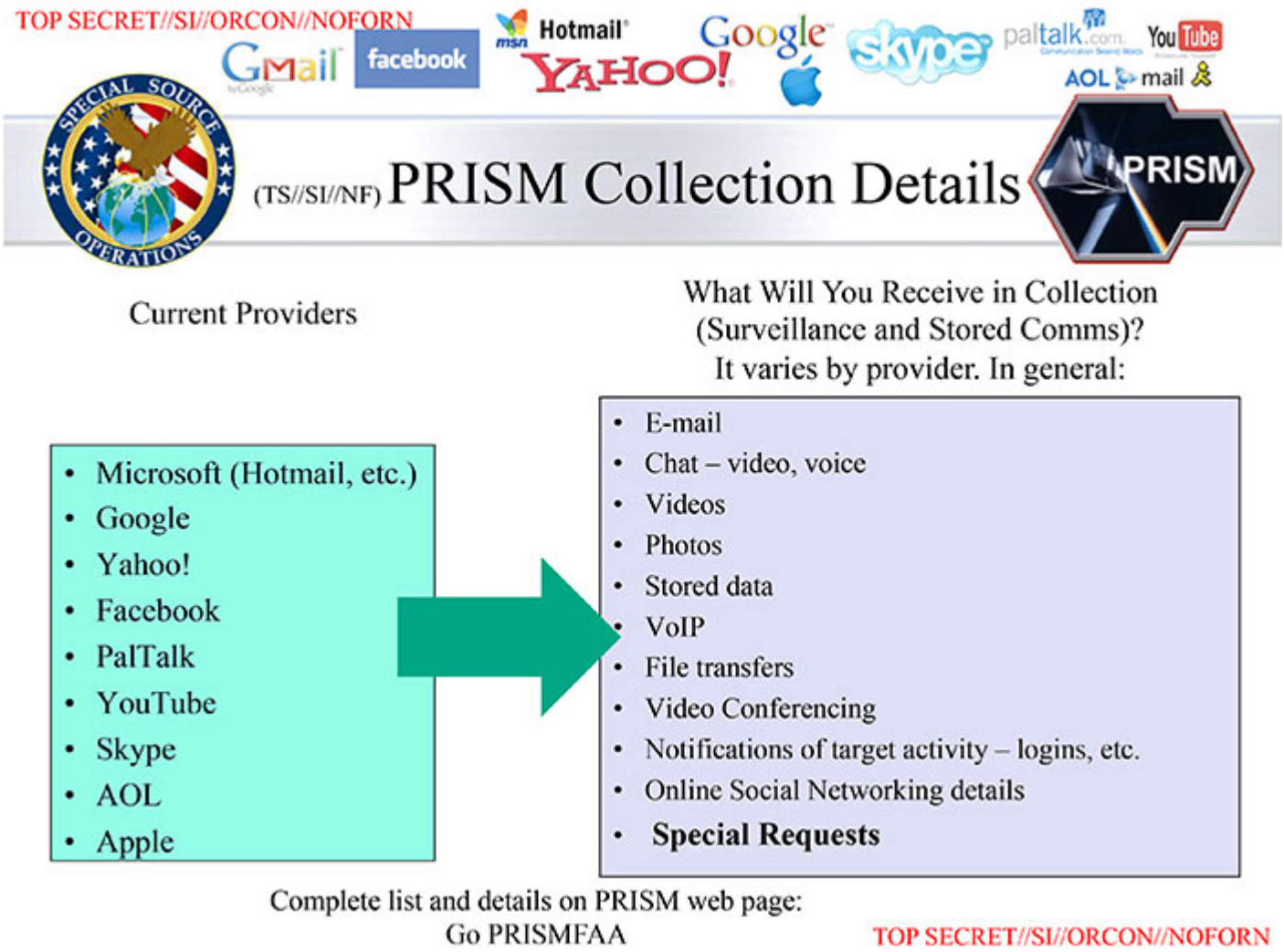
Source: *Edward Snowden, via The Guardian & The Washington Post*.

Context: Internet mass surveillance



Source: *Edward Snowden, via The Guardian & The Washington Post*.

Context: Internet mass surveillance



Source: *Edward Snowden, via The Guardian & The Washington Post*.

Context: Internet mass surveillance

- NSA approach, short video explanation:

  http://www.theguardian.com/world/video/2013/nov/26/nsa-gchq-surveillance-made-simple-video-animation

- **NSA long-term main strategy** appears to be:
  - ***Store everything:*** blanket storage – collect and store everyone's every communication.
  - ***Decrypt later:*** since the trend is ever-stronger decryption capabilities.

- Infrastructure being built:

  http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/

Context: Your projects

- Your (future) scientific / artistic / technological projects:
  - may use internet technologies
  - may function based on personal – even intimate – data
  - may gather scientific data that needs to be handled ethically.

⇒ Personal privacy and Internet mass surveillance need to be taken into account.

Countering Internet mass surveillance

- A whole range of issues may be reduced to two technology-based questions...

- How to hide *what* is communicated?

  - E.g.: http://www.aljazeera.com/news/europe/2014/02/uk-spied-millions-intimate-webcam-chats-20142271956348 2970.html

- **But also:** How to hide *who* communicates?

  - Many individual activities are moving from unsurveilled public space into surveilled cyberspace.

  - In this context, compare e.g. buying apples in a supermarket to buying plane tickets online...

Countering Internet mass surveillance

⇒ Then, given NSA main strategy:

Q: How to hide what is communicated, and by whom,
in the face of an opponent that has total knowledge of all the IP traffic involved ?


BREAK!