CRIM6002
Surveillance and the Web

Research and Investigations online

Workshop 3

Dr Anita Lavorgna

Today

- The Internet and everyday life
- Online surveillance
  - privacy vs. security

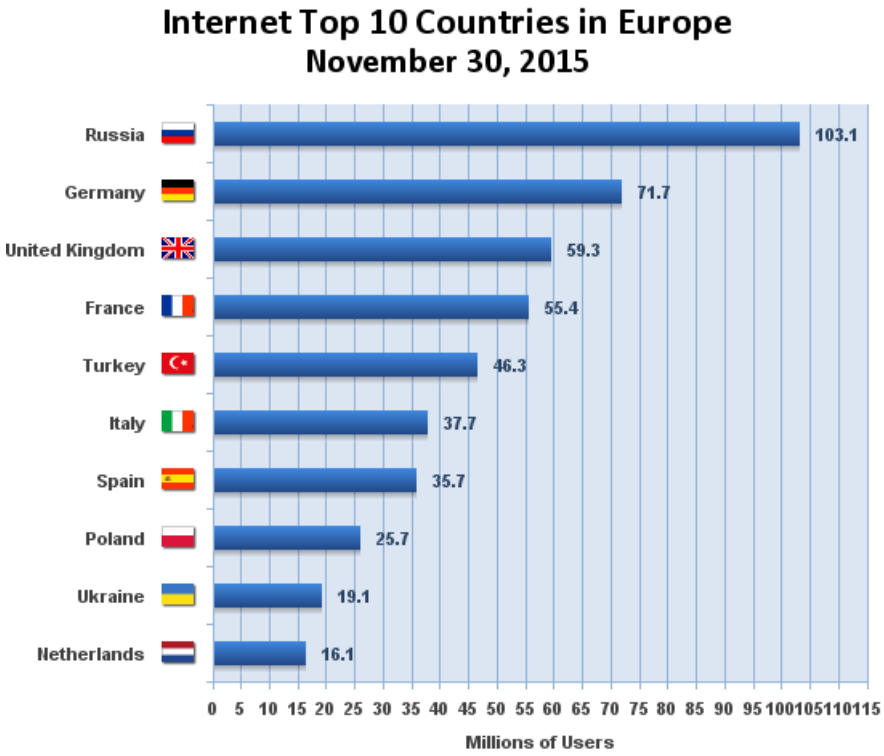
- Researching crime & deviancy online

The internet and everyday life

Around 40% of the world population has an internet connection today.
In 1995, it was less than 1%.

In Europe, 73.5% Internet penetration on Nov 15, 2015.

'Digital divide'



http://www.internetlivestats.com/

http://www.internetlivestats.com/internet-users-by-country/

http://www.internetworldstats.com/list3.htm

Think in how many ways the Internet permeates our lives…

- Digital economy, e-commerce
- Work and leisure (ubiquity, decentralisation, online social networks, consumption of cultural goods, online gaming, …)
- Politics and citizenship (Internet as a tool for political action, organisation, and motivation)
- Education and distance learning
- …

Process of '***hyperspatialisation***' (McGuire, 2007)

- Whether/to what extent the Internet is criminogenic
- **Online surveillance**

Surveillance

'Surveillance involves the observation, recording and categorisation of information about people, processes and institutions. It calls for the collection of information, its storage, examination and – as a rule – its transmission. It is a distinguished feature of modernity' (Ball and Webster, 2003).

INTENSIFICATION OF SURVEILLANCE in late-modernity

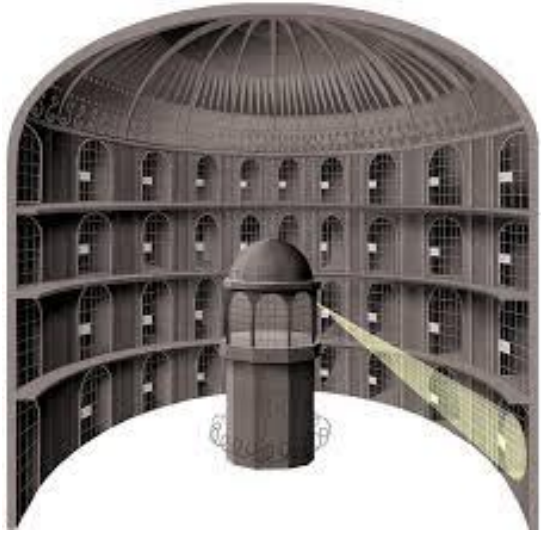
E.g. terrorism, post-September 11

'Surveillance society'. Surveillance as Janus-faced: it constraint us, but also it allows us to participate in society (e.g. National Insurance Number, your Student Number)

Panopticon

Jeremy Bentham, Utilitarianism

Michel Foucault (as a method of the modern discipline via surveillance)



Increasing studies on surveillance.
Please note: Anglo-centric focus.

Online surveillance

1. Surveillance *of* Internet interaction
2. Surveillance that ***uses*** the Internet

1. WHO
   - Criminals
   - Family, friends
     (e.g. 'lateral surveillance')
   - Workplace surveillance
   - Governments
   - Business companies

"Oh, look . . . they're reading '1984' in Ms. Smith's English class."

Example: surveillance in the workplace

- interception, recording and monitoring of e-mail
- monitoring of internet or intranet use
- tracking, following or video recording of worker movements or activities …

1. Openness
2. Consent
3. Consultation
4. Private spaces
5. Proportionality

Example: business companies

Technology evolves!

'To combat the cookie's flaws, advertisers and publishers are increasingly turning to something called fingerprinting. This technique allows a web site to look at the characteristics of a computer such as what plugins and software you have installed, the size of the screen, the time zone, fonts and other features of any particular machine. These form a unique signature just like random skin patterns on a finger. The Electronic Frontier Foundation has found that 94% of browsers that use Flash or Java – which enable key features in Internet browsing – had unique identities'.

(http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/#e1c3ea13e45c)

Personal information has an intrinsic 'value'

Online surveillance ('datavaillance')

	Surveillance target	Examples	Surveillance techniques	
			Automated	Non automated
Static	Personal data	Financial data, addresses, passwords, date of birth…	Cookies, spyware…	Wiretapping, data trading, data for ransom…
Dynamic	Communications	Conversations, messages…	Browser records, download histories…	Phishing, accessing PC directly…
	Behaviour	Opinion, intentions, preferences, previous history, spatial locations and movements…	Interception software for email, VoIP data…	Monitoring by using false identities

(Adapted from McGuire, 2009: 501)

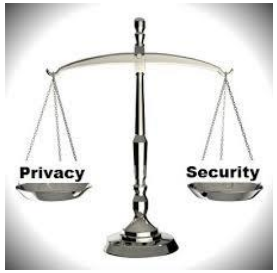
There are attempts to hide or disguise online interactions from scrutiny

- Closed networks for file sharing (darknets, trying to bypass the problem)
- Deleting digital traces
- Artificial invisibility (use of proxy servers)
- Encoding or encryption

Debate

- In what ways are our day-to-day uses of the Internet subject to surveillance?
- Are such surveillance measures justified by claims that hey are necessary for tackling crime/terrorism?

  Think in terms of balance/imbalance!



- Why is the regulation of privacy enhancing technologies such as encryption so difficult to address? Is it possible to meet the demands and needs of all social constituencies at the same time?
- What expectations of privacy are reasonable?
- Is there a new control elite?

The key issues revolve around the ***character*** and ***motivation*** of the surveillance (Ball and Webster, 2003)

E.g. Terrorism (see Brown and Korff, 2009)

Internet for:

- Social bonding, panning, executing acts
- Technical info in websites
- To increase public sympathy, Internet as an ideal propaganda tool
- For recruitment ('armchair jihadis')
- Sense of belonging

But also new opportunities for intelligence gathering!

Profiling, 'intelligence-led' searches

Substantial + procedural rules for gathering and handling the data

Researching crime & deviancy online

The Internet is also a source of data for academic research

- Manual collection of online traces
  - E.g. Virtual ethnography (passive/active)
- Automatic collection of online traces
  - Mirroring
  - Monitoring
  - Leaks

Use of Web crawlers

Technological challenges + Ethical considerations