# Big Brother 2.0:
# censorship, privacy and the Internet (part 2)

Kaido Kikkas
SPEAIT, Autumn 2023

# Going on…

- Last week, the main topic was censorship and its different aspects
- Today, we'll look at privacy and some tools that can be useful at preserving it

# Privacy

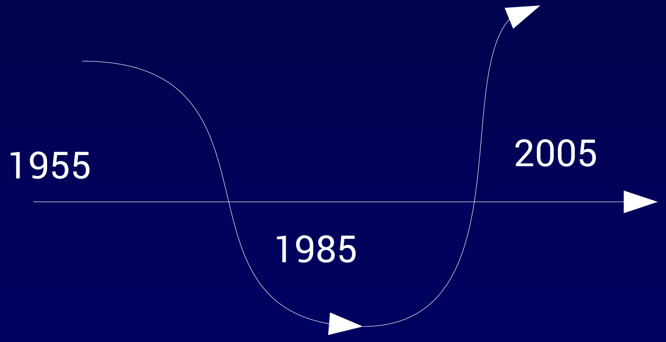
- Before the tech revolution, it was easy – just go away from others and see that no one sneaks
- Introducing distance put it in danger at once – couriers were intercepted, letters opened, cyphers broken, and long before any IT
- Today, we have got hi-tech on both sides

# From times of old

- The Talmud (Jewish law) mandates anyone building a house next to another to make windows either at least four cubits higher or lower than the neighbour's. Also, eavesdropping was expressly prohibited
- Some later rights defined:
  - Right to autonomy, to be left on one's own
  - Right to control information about oneself
  - Right to keep and privately forward secrets
  - Right to solitude, intimacy and anonymity
- The latest addition: Right to be forgotten (by Google a. o.)

# The sinusoid of online secrecy

- Along the development of the Internet:
  - Military – top secret
  - Research – some secret
  - Education and NGO – not much
  - Business – secre



# Works two ways

- On the one hand, Internet as a communication channels allows impersonality, anonymity and pseudonymity (“hiding behind the screen”)
- On the other hand – everything can be intercepted, collected, saved, processed, and used (including against you)
- Discovery will likely happen later, after the consequences have already arrived
- Differences between 'clean' and intercepted traffic are either hard to discover or do not exist

# Two concepts

- Private communication in a channel implies
  - **authenticity** – the message actually comes from where it claims to have come
  - **integrity** – the message arrives untampered

# My home is my castle?

- Compared to traditional privacy, online
  - the situation is much more difficult to control
  - there is mostly only hindsight
  - "Everything you say may be used against you" – directly or indirectly, at once or years later
  - identity theft is easier, consequences may be rather serious
  - legal protection is weaker

# Different players

- Wider public (‘ordinary people’) vs two camps of professional players:
  - those who make money by **keeping** privacy/security (guards, admins)
  - those who make money by **violating** privacy/security (from media and marketing to criminals)

- Cooperation is possible

# Data collection: the motive counts

- Data collection is ethically neutral, the “charge” comes from its usage:
  - One's personal doctor
  - Generic businesses
  - Advertisement agencies
  - Spammers
  - Criminals

# Why it matters

- Due to two qualities of the Internet:
  - Possible to track others without them knowing it
  - Possible to collect, analyze and preserve ever larger quantities of data
- Privacy takes consenting adults – but Internet is largely different
- As a result, privacy and security compete instead of cooperating

# …

- Collecting information is possible using fully legal channels
- Even the smallest blunders can be registered
- Preservation is not a problem – the info can be put in use at the best moment (e.g. before elections). Usually, just hinting works (next to impossible to prove!), but blackmail is also an option if needed

# The dossier effect on Internet

- Networks promote systematization of information
- Temptation to collect private information (just in case)
- Customer databases => dossiers (in the KGB sense)
- The state is not innocent either

- For perspective: Estonian Imre Perli and his infamous databases from the 1990s would probably be viewed as nothing special today

# Pseudonymity

- A small trivia: under which names do we know
  - Annie Mae Bullock
  - Jean-Claude van Varenberg
  - Reginald Kenneth Dwight?

- In many fields of society (especially culture) it is an acceptable way of ensuring objectivity
- Sometimes can save the author
- Online, it offers a handle/avatar which can be detached from the actual person, yet keep the continuity; middle ground between anonymity and revealed identity

# Anonymity vs comfort

- Everyday anonymity cases:
  - Testing of some diseases
  - Cell phone cards
  - Cash
- There are also cases where comfort beats security:
  - Using a random computer (in a hotel or cafe)
  - Laptops and smartphones (various bad practices)
  - WiFi (unsecured)
  - Facebook ...

# Anonymity in IT history

- In the really old times, it was unnecessary – everyone around was “us”
- Classical hacker tradition did not see a point either – it hindered paying a person with respect
- Expansion, emergence of business and increasing state interference made it vital as a tool for freedom of expression and whistleblowing
- Today, allows 'flying below the radar'

# Digital enclosure

- A concept introduced by Mark Andrejevic
- A society where every transaction leaves a digital footprint
- Imagine the world where Google controls the whole Internet…
- … and many people would be happy with that (just as many young people in China are today)

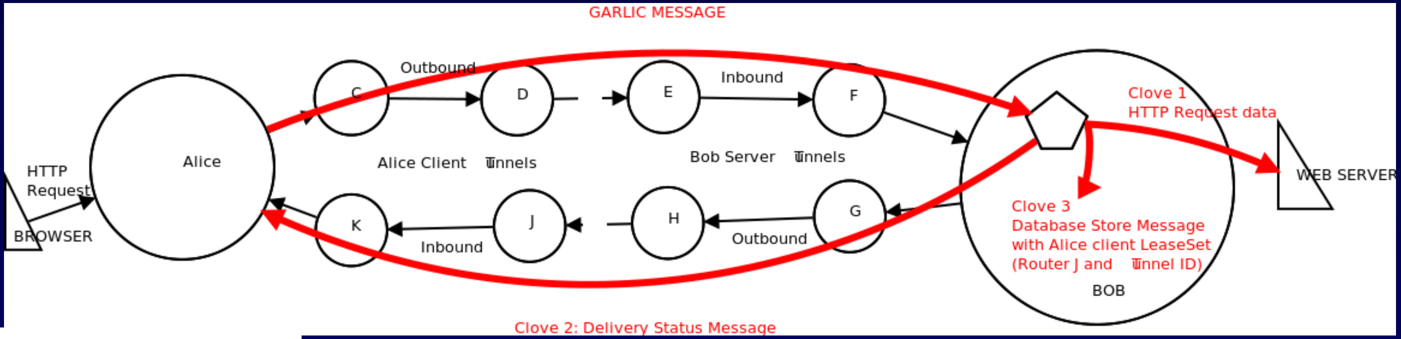
# Anonymous e-mail

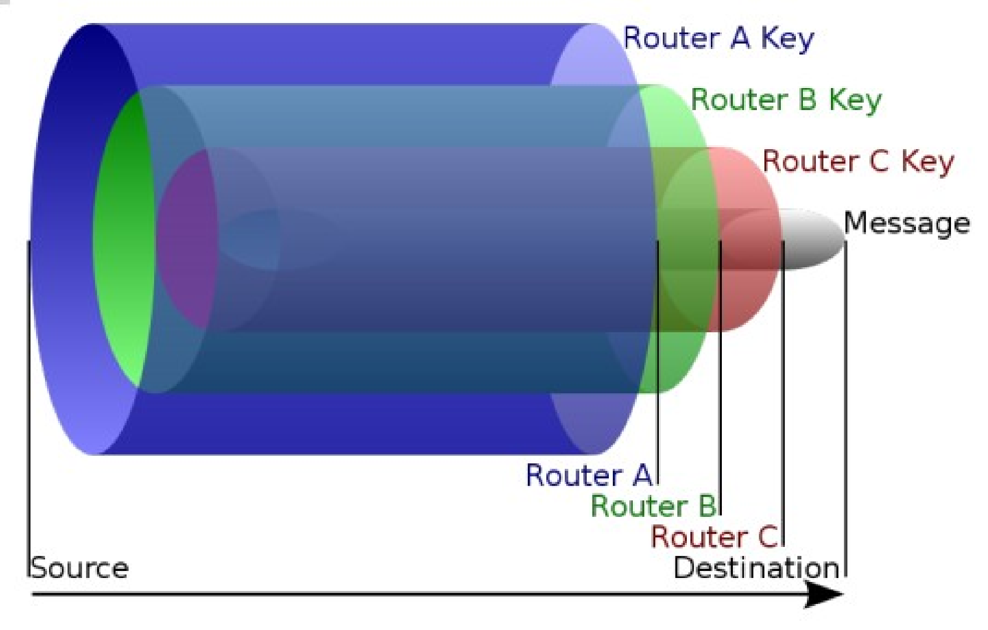
- Started in Helsinki 1995 with Johan “Julf” Helsingius and anon.penet.fi – a simple connection table, no crypto (type 0)
- 1996 closed down – The Observer blamed Julf's small server of forwarding 90% of all child porn online…
- Later developments were type 1 (Cypherpunk – one-way messages, public key crypto), type 2 (Mixmaster – cuts message to pieces and sends in random order) and type 3 (Mixminion – combo of 1 and 2)

# Onion and garlic

- Onion routing – message encrypted by layers
- Developed in the 90s at the US Navy Research Laboratory (Paul Syverson et al), further developed by DARPA and others
- Tor Project (*The Onion Routing*) – founded 2006 as an NGO project, original creators + EFF
- I2P (*Invisible Internet Project*) – since 2003. Anonymous e-mail, Bittorrent, I2P Messenger and other services. Garlic routing – adding message grouping to the onion system

# Figures





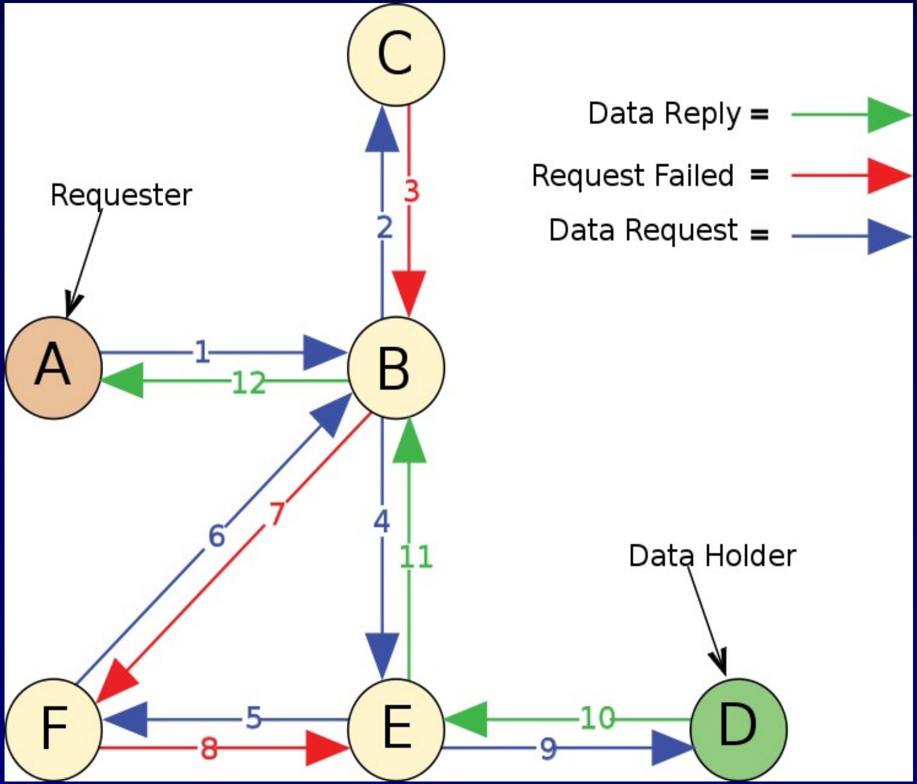
https://geti2p.net/en/docs/how/garlic-routing

https://en.wikipedia.org/wiki/Onion_routing

# The Internet Iceberg

- **Surface Web** – where search engines work (ct passive information mentioned at communication topic)
- **Deep Web** – what Google cannot reach (simple examples are everything behind passwords)
- **Dark Internet** – addresses that cannot accessed from ordinary Web (e.g. the original MILNET)
- **Freenets** – public networks dedicated to anonymity and freedom of expression (Ian Clarke 2000**)**
  - **Opennet** – allows connecting to strange**rs**
  - **Darknet** – closed, limited-access networks

# A Freenet query



http://upload.wikimedia.org/wikipedia/commons/a/ae/Freenet_Request_Sequence_ZP.svg

# Last but not least: ChatGPT

- Large *Language* Model ≠ Large *Intelligence* Model
- It is essentially Google on steroids - capable of processing huge volumes of textual material and giving the results a superficially intelligent appearance (not unlike human politicians posing as experts)
- Digital enclosure!
- Also, the results depend on
  - the worldview of those who ‘trained’ it (i.e. chose the texts)
  - the worldview of those who wrote those texts
- https://www.researchgate.net/publication/373188439_More_human_than_human_measuring_ChatGPT_political_bias (Motoki *et al*, Public Choice, August 2023)

# What to learn from Wikipedia

- (not from that encyclopedia, but from the project behind it!)
- When studying anything online:
  - Keep the NPOV (overall neutral point of view)
  - Bring out all the competing standpoints
  - All main assumptions/statements have to be sourced
  - Major/principal changes require discussion and consensus

# Some recommendations

- Read and follow as much different channels as possible
- Sometimes, the ones with radically different worldview from yours are the best teachers!
- Dare to
  - ask
  - doubt
  - criticize
  - LAUGH (including at yourself)
- Be able to a) think (also critically), b) read, c) write

# A couple of conclusions

- Censorship is bred by power – also online
- Censorware does not work
- Privacy is a little similar to weapons:
  - Limitations decrease some random misuse
  - Limitations also decrease self-defense ability of honest people (and by this, their dignity)
- Not only humans can be censored - or brainwashed
- The main goal is to raise awareness and create informed people. Those are a bit more difficult to turn into cattle ("Moo!" said The Plague in the *Hackers* movie)...

# For further reading

- Christian Parenti, *The Soft Cage*
- Mark Andrejevic, *iSpy* (the first half)
- Banned Books Online, https://onlinebooks.library.upenn.edu/banned-books.html
- Official Mixmaster Remailer FAQ, https://mixmaster.sourceforge.net/faq.shtml
- Why Censorware Sucks, https://attrition.org/misc/ee/why_censorware_sucks.txt
- https://tails.boum.org/

# Merry Christmas and a Happy New Year!

</lectures>