The problem with mass surveillance

Linus Nordberg, DFRI
linus@dfri.se

2019-11-23
ULUG, Uppsala

:DFRI
https://dfri.se

About me

- 30 years of software development and systems administration
- 20 years of software and network security
- 10 years of privacy advocacy and activism
- Heavily engaged in Tor Project, doing online anonymity
- Co-founder of DFRI, Swedish digital rights organisation

Part I – Our rights

- The Universal Declaration of Human Rights Article 12
- The Charter of Fundamental Rights of the European Union Article 7 and 8
- “How the business model of Google and Facebook threatens human rights”, report by Amnesty (2019)

Everyone has got something to hide

- Doesn't have to be illegal or even immoral
- Privacy is relational, depending on your audience
- Control over how you expose your thoughts
- To form your own self

Everyone has got something to hide

- Doesn't have to be illegal or even immoral
- Privacy is relational, depending on your audience
- Control over how you expose your thoughts
- To form your own self

Everyone has got something to hide

- Doesn't have to be illegal or even immoral
- Privacy is relational, depending on your audience
- Control over how you expose your thoughts
- To form your own self

Everyone has got something to hide

- Doesn't have to be illegal or even immoral
- Privacy is relational, depending on your audience
- Control over how you expose your thoughts
- To form your own self

“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

Privacy on two levels – individual and societal

- Lack of privacy is a threat on an individual level as well as a societal level
- Panopticon, or todays online panspectron, leads to changed behaviour
- Self censoring leads to stagnation of society and to decline of democracy

Privacy on two levels – individual and societal

- Lack of privacy is a threat on an individual level as well as a societal level
- Panopticon, or todays online panspectron, leads to changed behaviour
- Self censoring leads to stagnation of society and to decline of democracy

Privacy on two levels – individual and societal

- Lack of privacy is a threat on an individual level as well as a societal level
- Panopticon, or todays online panspectron, leads to changed behaviour
- Self censoring leads to stagnation of society and to decline of democracy

We're doing it wrong

- Legal security is based on the presumption of innocence
- European data retention laws
- More data leads to higher risks
- Privileged groups tend to risk less

We're doing it wrong

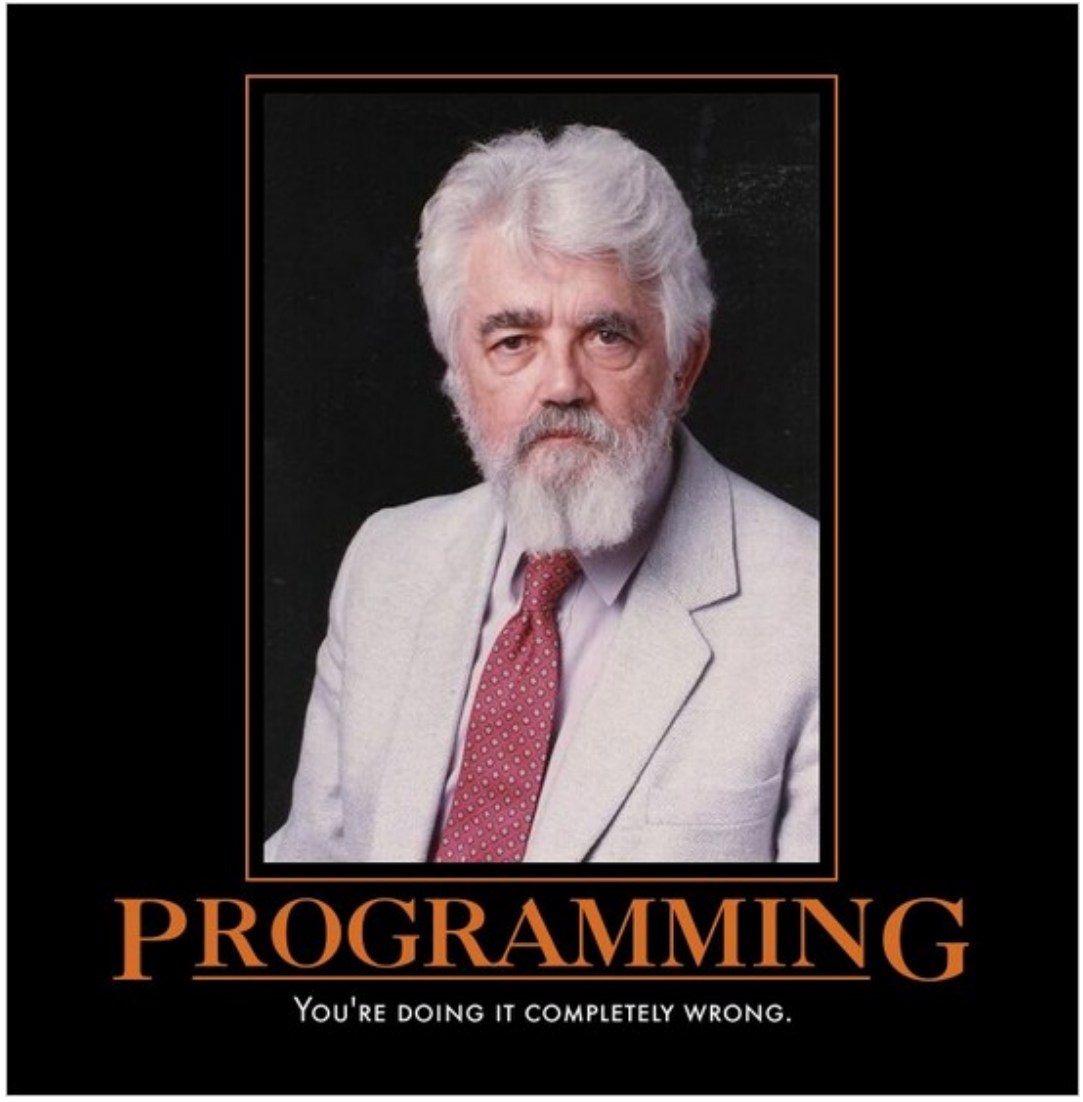
- Legal security is based on the presumption of innocence
- European data retention laws
- More data leads to higher risks
- Privileged groups tend to risk less

We're doing it wrong

- Legal security is based on the presumption of innocence
- European data retention laws
- More data leads to higher risks
- Privileged groups tend to risk less

We're doing it wrong

- Legal security is based on the presumption of innocence
- European data retention laws
- More data leads to higher risks
- Privileged groups tend to risk less



John McCarthy, inventor of Lisp and the term “artificial intelligence”.

Metadata

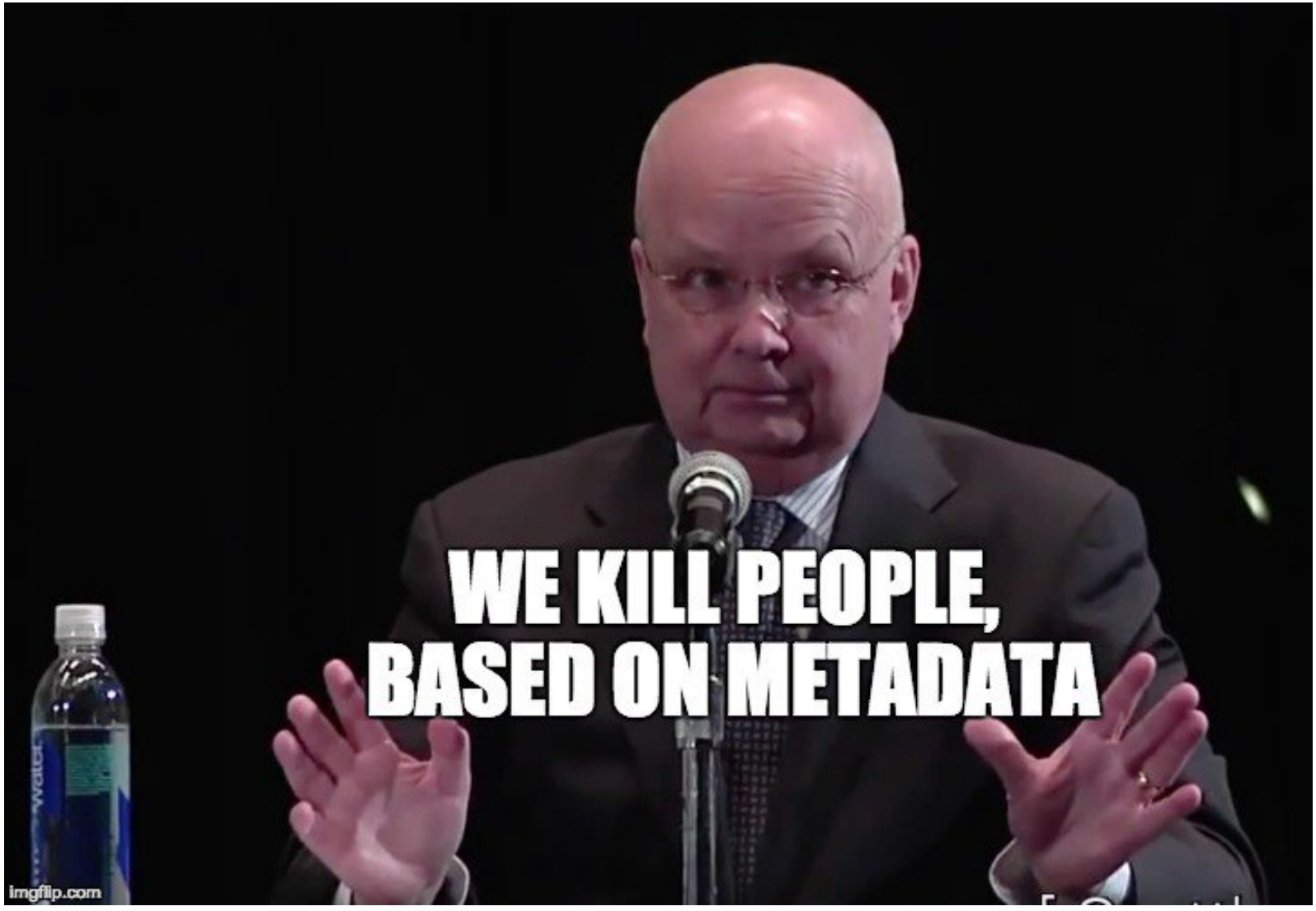
- Metadata is data about data
- Immensely useful when drawing sociograms
- Often enough to identify individuals

Metadata

- Metadata is data about data
- Immensely useful when drawing sociograms
- Often enough to identify individuals

Metadata

- Metadata is data about data
- Immensely useful when drawing sociograms
- Often enough to identify individuals



Michael Hayden, former NSA and CIA director

The ad economy of the internet

- An internet economy based on advertising
- We pay with our data
- RTB – Real-time bidding
- Data is valuable, storage is cheap
- User data is the new oil, in more than one way

The ad economy of the internet

- An internet economy based on advertising
- We pay with our data
- RTB – Real-time bidding
- Data is valuable, storage is cheap
- User data is the new oil, in more than one way

The ad economy of the internet

- An internet economy based on advertising
- We pay with our data
- RTB – Real-time bidding
- Data is valuable, storage is cheap
- User data is the new oil, in more than one way

The ad economy of the internet

- An internet economy based on advertising
- We pay with our data
- RTB – Real-time bidding
- Data is valuable, storage is cheap
- User data is the new oil, in more than one way

The ad economy of the internet

- An internet economy based on advertising
- We pay with our data
- RTB – Real-time bidding
- Data is valuable, storage is cheap
- User data is the new oil, in more than one way

Internet design

- The internet was built without privacy in mind
- Multiple levels of tracking, not only IP addresses
- Control over infrastructure gives even more opportunities
- Exploitation technology is used to leverage even further

Internet design

- The internet was built without privacy in mind
- Multiple levels of tracking, not only IP addresses
- Control over infrastructure gives even more opportunities
- Exploitation technology is used to leverage even further

Internet design

- The internet was built without privacy in mind
- Multiple levels of tracking, not only IP addresses
- Control over infrastructure gives even more opportunities
- Exploitation technology is used to leverage even further

Internet design

- The internet was built without privacy in mind
- Multiple levels of tracking, not only IP addresses
- Control over infrastructure gives even more opportunities
- Exploitation technology is used to leverage even further


QUESTIONS
DISCUSS

Part II – Hands on technical solutions

- Let's talk a bit about a few attempts at technical solutions to the above problem.
- The focus is on the internet but the problem of mass surveillance is of course present on many other platforms, like bank records, cell phones and CCTV.
- This presentation can be found at `https://dfri.se/wiki/presentations/2019-11-23-dfri-ulug.pdf`

PGP – Pretty Good Privacy

- For verification of software packages
- For encrypted and signed email
- Web of trust
- Cumbersome to use and errorprone but the best we've got at the moment

Tor Browser

- Protecting your browsing habits from being scooped up
- Protecting your IP address by sending your data over the Tor network
- Application level protections, like cookies, fingerprinting and enforcing HTTPS
- PGP key used for signing Tor Browser packages: EF6E 286D DA85 EA2A 4BA7 DE68 4E2C 6E87 9329 8290
- `https://www.torproject.org/download/`

Tor Browser on a handheld

- Android: Tor Browser from the Guardian Project's repo
- iPhone/iPad: Onion Browser (Tigas Ventures LLC)

Tails

- Linux (Debian) system with Tor and other security tools pre-installed and pre-configured
- Run from a USB stick
- Leaving no traces on the computer it's being run on
- `https://tails.boum.org/`

Instant messaging

- Signal (Open Whisper Systems) protects your text messages from being snooped on
- But uses your phone number as identfier
- Threema is an alternative
- Both using third party infrastructure
- Jabber (XMPP) can be self-hosted
- Briar needs no servers at all!

Voice and video calls

- Wire.com does chat, voice and video
- Nextcloud Talk, can be self-hosted
- Mumble, easily self-hosted but no video

Nextcloud

- File sync and share
- Contacts, calendar and events
- Calls, chat and online meetings

Social networking

- Federated self-hosted social networking
- Mastodon for “microblogging”, like Twitter you know.

What more do we need?

- `https://dfri.se/wiki/presentations/2019-11-23-dfri-ulug.pdf`
- Your input here

Contribute

- Get involved – DFRI.se
- Non Swedish alternatives – EDRi.org
- Run a Tor relay, see `https://community.torproject.org/relay/`

Further reading

Books

- Kallocain, Karin Boye
- Little Brother, Cory Doctorow
- Data and Goliath, Bruce Schneier
- The Age of Surveillance Capitalism, Shoshana Zuboff

Websites

- `https://www.dfri.se/`
- `https://www.edri.org/`
- `https://www.eff.org/`
- `https://www.torproject.org/`