Privacy and Politics

Legal Valley, Arnhem

Bart Jacobs
bart@cs.ru.nl
7 March 2017

Outline

Where we are, so far

Who is this guy?

- Professor at Nijmegen (NL), in computer security
  - studied mathematics & philosophy (not law!)
- security research with societal relevance, eg. in **e-passports**, **voting**, **road pricing**, **smart meters**, **e-ticketing**, **privacy**
- regular role in media on security/privacy/intelligence issues, and occasionally in parliamentary expert meetings
- member of the Cyber Security Board in NL, but also of the Advise Board of Bits of Freedom, and Expert Board of Indepedent Intelligence supervision committee

Plan for today

(1) Some background on security and privacy

(2) Tenets (*Stellingen*)
- Basic truths about the digital world

(3) Fallacies
- Common misconceptions and framings

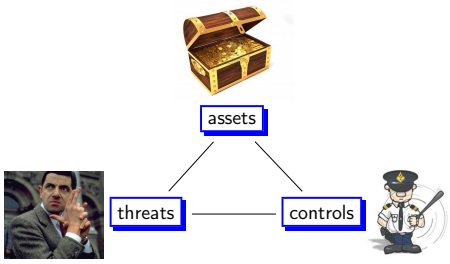
(4) Recommendations
- Own opinions and suggestions

Where we are, so far

What is computer security about?

My favourite definition:

regulating access to digital assets



Personal data is among the assets that you may want to protect

Societal relevance

- Traditional view:
  - computer scientists are architects of the digital world
- Modern view:
  - computer scientists are architects of the social world

Computer security and privacy issues can make or break developments in:

- communication
- transportation
- health care
- finance & insurance
- government *etc.*

Privacy and contexts, after Helen Nissenbaum

- We naturally live in different contexts
  - home, work, sports club, in church, with friends . . .
- We naturally want to keep information in context
  - what we tell to our doctor should not end up in a supermarket
- People get upset when contextual integrity is broken
  - recall anger: about selling customer financial data (ING), about speeding data ending up at the police (TomTom), about school children's performances in online tests ending up at publishers
- When explained like this, almost everybody cares about privacy
- The Google's and Facebook's of this world make us use the same identifier everywhere or track us via Like and cookies
  - they break-up contexts, and destroy our basic privacy intuitions
  - Mark Zuckerberg: "Having two identities for yourself is a lack of integrity" ☹☹☹

Privacy differences between EU and US

- **EU**
  - Privacy is a fundamental right (National/Charter/Convention)
  - It gives opacity (obscurity, impenetrability): a sphere of unmonitored freedom
  - Breaking this sphere can only happen if there is a law for it
- **US**
  - In practice a matter of negotiation
  - Laws exist, but mostly per sector (health care, finance, . . .)
  - Privacy requires others to refrain from infringements ("The right to be let alone", Warren and Brandeis, 1890)

EU Judges are the new privacy heros

The European Court of Justice ("Luxembourg") is very influential, based on the EU Charter of Fundamental Rights

- data retention directive invalid: telecoms no longer obliged to store everyone's metadata
- right to be forgotten introduced: search engines must remove stigmatising links on request
- Safe Harbour agreement rejected: European data are not safe in the US.

This shows the need for a NL constitutional court, as protection against national politicians

Where we are, so far

Tenet I

Power relations in society are determined by (access to) data flows

- In the past, if you wanted to understand power: "follow the money!"
- Nowadays: "follow the data!"
- The Google / Facebook / Amazon's have understood this all too well
- Learn to think in terms of data flows — and also of how to protect these flows

Tenet II

If we wish to keep some level of privacy, we will have to use technical means to protect it

- This goes much further than privacy-by-design-and-default and security-by-design requirements, as in the GDPR
  - those principles apply to general ICT-systems, with other goals
- Tenet I is about ICT-systems dedicated to privacy protection
  - it is insufficiently acknowledged by the privacy movement
- following Nissenbaum: ICT-systems must keep data in context
  - More generally, EU fundamental rights must be embodied in technology

Aside: my own research is based on this tenet, especially IRMA and PEP, see also `www.privacybydesign.foundation`

Tenet III

ICT is highly political; its developments can (and should) be steered by regulation

- Very few politicians seem to recognise the political nature of ICT.
- Leaving all choices to "Silicon Valley" is also a political choice
- Large tech-firms lobby heavily **not** to intervene.
- Who is defending the public cause/interests in the digital world?
  - see also Rathenau report (*Opwaarderen*, feb'2017)

Tenet IV

The early-day optimism about the internet giving individual freedom and transparancy of the powerful has turned out to be so naive

- The internet has become a tool for mass surveillance
  - in the commercial sector, eg. via tracking cookies
  - in the public sector, as we learned from Snowden
- Individuals have become transparent, via Facebook and profiling, instead of the people in control
- the prevalent business model is economically and politically destructive, leading to excessive, concentrated wealth and power
  - if Zuckerberg decides to run for president, he can make it happen himself — that's Berlusconi on steroids, via personalisation
- Pervasive profiling has led to filter-bubbles and easy manipulation — e.g. via fake news and differential pricing

(Read e.g. Evgeny Morozov or Andrew Keene)

Where we are, so far

Fallacy I

Everyone puts everything on Facebook anyway

- Usually this a precursor to a very privacy-unfriendly proposal
- Some people are careless indeed, but many are not
  - usually, after some deception, kids become rather careful
- If some people choose to go around naked, that is no excuse to force others to be naked too.

Fallacy II

We will seek a **balance**
between security and privacy

- Especially popular among politicians
  - if you see this, you can bet on it that privacy will lose
- Contrasting security and privacy is the lazy solution
  - remember: privacy is essential for personal security
- What we need is both privacy and security
  - that is where real innovation lies!
  - indeed, tough regulation often inspires innovation

Fallacy III

We're good, since we've got user **consent**

- The consent mechanism fails in so many ways
  - many people agree blindly (always hit 'OK')
  - conditions are often unreadable 'legalese'
  - conditions are sometimes simply illegal, dumping responsability on users
  - there is no real choice left, if the product (eg. a TV or car) has already been bought
- The consent mechanism fails epically in health care
  - agreement of sick people hardly reduces one's own responsability
- Many IT-giants are moving into healthcare:
  - margins are highest
  - sick people don't whine about privacy

Fallacy IV

We simply need all data for better healthcare

- First: be careful of such "big data cowboys", see the NL tax office scandal (Zembla, 1 feb. 2017)
- Variations & generalisations: "useful data must be usable"
  - **but**: useful for whom? For whose benefit? Don't be naive!
- Sure, everyone wants better healthcare, but also healthcare without:
  - discrimination
  - risk-based selection
  - secondary usage of the data
  - breaking contextual integrity
  - big-IT becoming controller instead of processor
  - lock-in dependence on data handlers (think of big-pharma)

  But all of this is part of the "better healthcare" vision!

Fallacy V

If we cannot use all data, we loose from
US companies who can, without restriction

- Twisted representation of a serious problem
  - well-intending companies should not be scrutinised and penalised whereas cowboys get away
- What's really needed is a level playing field
  - GDPR will apply broadly, to every one doing business in EU
  - broad and uniform enforcement will be needed

Fallacy VI

We send you only the ads that **you** want to see

- NO, NO, NO — so naive again!
- They send you the adds that they want you to see!
  - and they adapt the prices to what they think you will pay
  - moreover, they selectively show you options
- This is called price discrimation or targeted pricing

Where we are, so far

Recommendation I

See privacy and data protection as the new "green", powering innovation

- When the first environmental protection laws appeared in the 1980s, after several big pollution scandals, industry complained bitterly about economic loss through these laws
- Nowadays "green" is widely accepted and a driver of economic growth: innovation through tough regulation
- We should copy the success of the green movement
  - The GDPR prepares the ground

Recommendation II

Protect people, possibly even against themselves

- Freedom is most advantageous for people with money and data
- Sometimes you have to protect people against themselves
  - in civilised countries it is forbidden to sell your own organs (*buiten de handel geplaatst*)
  - maybe it should also be forbidden to sell your own medical data
- Counter-power against "Big-IT" requires some level of enlightened paternalism and also duty of care

Recommendation III

Privacy protection must be an integral part of the cyber security agenda

- The next cabinet will most likely invest much more in cyber security
  - current slogan: *NL is a safe place to do business*
- Add slogan: *privacy protection is a license to do business*
  - required by GDPR, which will have huge impact
- Follow German rule: in all ICT-projects 10% of the budget must go to security and privacy.

Recommendation IV

Recognise and defend the "public interests" in the digital world

- The healthcare sector is being colonised by Google, Apple, Philips . . .
  - who in politics defends that personal data should remain in a medical context?
- Same story for cars, or TVs, toys, internet-of-things, . . .
  - if you buy a Tesla, you have to sign that all your data goes to Tesla; will this be the norm?
- The essence of smart cities is plundering data of citizens and municipalities
- Strengthen the law, and its enforcement
  - e.g. disconnect/delete buttons

Recommendation V

Introduce new rights to receive information, without any monitoring or profiling

- Traditional freedoms of expression focus on sending information
- In a time of filter-bubbles we need new rights to receive,
  - without personalised pre-selection
  - without monitoring
- We need a right not-to-be-profiled, just like a right-to-be-forgotten

Recommendation VI

Treat big-IT as utilities and break them up

- Use the power of the law, existing and new, . . .
- . . . based on a critical vision and a sharp view on what is happening.

Where we are, so far

Main point

Individual dignity, autonomy, freedom and privacy are at stake!

Thanks for your attention. Questions/remarks?