De Publieke Zaak in de Digitale Wereld
(Public Interests in the Digital World)

Piratenweekend, Delft
Bart Jacobs
bart@cs.ru.nl
28 Jan. 2017

Outline

Introduction
Computer Security and privacy
Tenets
Recommendations
PPNL only

Where we are, so far

Introduction
Computer Security and privacy
Tenets
Recommendations
PPNL only

Plan for today

(1) Some background on security and privacy
   • "back to school"
(2) Tenets (Stellingen)
   • basic observations about the digital world
(3) General political recommendations
   • feedback and discussion is much appreciated
(4) A few specific points for PPNL

Please note:
► Had the Christenunie invited me, I would have gone too ... 
► ...and I would have given basically the same talk.

Who is this guy?

► Professor at Nijmegen (NL), in computer security
  • studied mathematics & philosophy (not law!)
► doing a mix of theoretical and practical work: e.g. both
  • quantum security, via ERC Advanced Grant
  • attributes-based authentication, see irimacard.org
► focus on protection & abuse of ICT
► security research with societal relevance, e.g. 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 Advice
  Board of Bits of Freedom, and Expert Board of Independent
  Intelligence supervision committee
► I cherish my independence

Where we are, so far

Introduction
Computer Security and privacy
Tenets
Recommendations
PPNL only
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.

Computer security is interdisciplinary

- **Mathematics**: cryptology as basic toolkit for encryption, signing, authentication, etc.
- **Computer security**: the software, hardware, networks that make things work
- **Management / economics / psychology**: which incentives work?
- **Law / ethics / politics**: what is/should be allowed, esp. against cybercrime and for data protection

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
- government etc.

Cybercrime, cyberwarfare, cyberespionage

- You’re an old-school loser if you’re still planning a career as a physical bank robber
- the bad guys have gone digital, in fraud, extortion, blackmail, sabotage, ...
- espionage has become almost exclusively digital — and political manipulation too
- warfare has gone digital ...

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 cookies
  - they break-up contexts, and destroy our basic privacy intuitions
- Mark Zuckerberg: “Having two identities for yourself is a lack of integrity”

A picture says it all
Privacy versus data protection (in EU)

- **Privacy**
  - Right for citizens
  - Strongly entwined with identity and autonomy
  - Data protection is one mechanism to guarantee privacy

- **Data Protection**
  - Right for data controllers: if they stick to certain rules, then they can process data
  - Processing must be based on one of six legal grounds (consent, contract, legal obligation, vital interests of data subject, public task or legitimate interest of data controller)
  - Rules for data subjects involve: rights to see, correct, delete
  - Strongly entwined with control and informational self-determination

Where we are, so far

- **Introduction**
- **Computer Security and Privacy**
- **Tenets**
- **Recommendations**
- PPPL only

Tenet I

- 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, including BOF
- 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 II

- 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 III

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

- Very few politicians seem to recognize the political nature of ICT.
- remember: architecture is politics
- 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?

Tenet IV

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

- The internet has become a tool for mass surveillance, esp. in the commercial sector
- Individuals have become transparent, via Facebook and profiling, instead of the people in control
- The prevalent business model is economically destructive, leading to excessive, concentrated wealth and power
- 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

Introduction

Computer Security and privacy

Tenets

Recommendations

PPNL only

Recommendation I

Both

Demand both security and privacy

▶ Often a choice is presented: either privacy or security
  • this is too simplistic
▶ Sometimes also there is talk about a finding a balance between security and privacy
  • if you hear this, you can bet that privacy will lose
▶ Contrasting security and privacy is the lazy solution
  • the combination of security and privacy is often possible but requires an innovative technical solution
  • this is the kind of innovation that we need
▶ Remember also: privacy is essential for personal security

Recommendation II

Align

Seek alliance with the agenda towards more cyber security. Try to get personal data of citizens acknowledged as a strategic national asset.

▶ The next cabinet will most likely invest much more in cyber security
  • Slogan: NL is a safe place to do business
▶ Make sure that personal data protection is an integral part of this package
  • refer to the General Data Protection Regulation (GDPR), which will have huge impact
▶ Add slogan: privacy protection is a licence to do business
▶ Follow German rule: in all ICT-projects 10% of the budget must go to security and privacy

Recommendation III

Law

Recognise and exploit the power of the law, especially in Europe. The European Court of Justice ("Luxembourg") is very influential, based on the EU Charter of Fundamental Rights

▶ CJEU judges are the privacy hero's, not national politicians
  • 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.
▶ Get your main points into laws; laws have impact.
▶ And indeed, NL needs a constitutional court too.

Recommendation IV

Power

Organise power structures for your cause.

▶ In the next cabinet, the Internal Ministry will probably control all public ICT
  • it might set up an ICT-authority, with real power
  • make open source, for all public services, part of that agenda
  • and of course, privacy protection too
  • increase the Data Protection Authority budget five-fold
▶ Think big: claim this Internal Ministry!

Recommendation V

Connect

Make your story concrete and recognisable for many people

▶ The healthcare sector is being colonised by Google, Apple, Philips, ..., looking for high margins and sensitive personal data
  • who in politics defends that personal data should remain in a medical context?
▶ Same story for cars, or TVs, 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, right-not-to-be-profiled, ...
Recommendation VI

Green
Advocate privacy and data protection as the new “green”

- 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.
- Try to copy the success of this movement. The GDPR prepares the ground.

Recommendation VII

Protect
Don’t just talk about privacy, freedom and autonomy, but also about protecting people.

- Recall the original naiveté about the internet.
- Freedom is most advantageous for people with much money and data.
- Sometimes you have to protect people against themselves:
  - that’s why it is forbidden to sell your own organs
  - maybe it should also be forbidden to sell your own medical data
- In the US, privacy is a matter of negotiation; here in Europe it is constitutionally protected. Organise this protection.

Recommendation VIII

Blame
Put the blame for the current state of weak security and privacy in ICT where it can be fixed: be careful not to put the responsibility with the victims.

- Software vulnerabilities are at the core of our many security (and also privacy) problems.
- Make the producers of crapy software liable:
  - certainly resist campaigns to make people more aware
  - blaming and shaming works best
  - full disclosure of vulnerabilities is counterproductive — responsible disclosure and repair seems to work
- Work towards duty of care (zorgplicht) in ICT, with open norms.

Where we are, so far

Introduction
Computer Security and privacy
Tenets
Recommendations
PPNL only

How to distinguish yourself as PPNL

(1) Present yourself as the only party with a digital agenda, addressing the data-based power inequalities in society
(2) Use humor, especially in the social media, hoping that (one of) your messages goes viral
De piratenpartij heeft al meer dan 1000 keer zo veel
leden als de PVV

In het volgende kabinet claimt de PPNL het
ministerie van defensie: fantastisch, een piraat die de
marine leidt!