securityandtrust.lu

Data Protection

November 12, 2015

Cesare Bartolini

Interdisciplinary Centre for Security, Reliability and Trust (SnT),
University of Luxembourg

UNIVERSITÉ DU LUXEMBOURG

Outline

1. Privacy in history
2. Privacy vs. data protection
3. Data protection theory and practice
4. Data protection and IT
5. Engineering data protection

Outline

1. Privacy in history
2. Privacy vs. data protection
3. Data protection theory and practice
4. Data protection and IT
5. Engineering data protection

Ancient Greece

- Political participation
- Privacy based on gender and wealth
- Private vs. public
- *No loneliness?*

Middle Ages

- Moving to town. . .
- No loneliness tolerated
- No concept of privacy
- *Not at all*

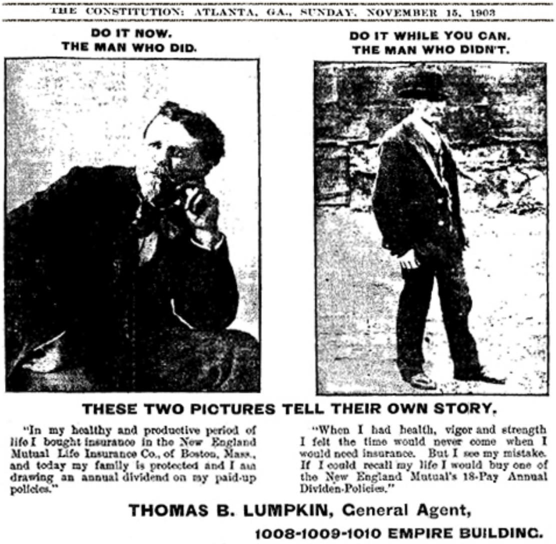
Enlightenment

- Books and literature
- No noise, please
- Privacy is valued and appreciated

USA, nineteenth century

- Yellow journalism (Pulitzer)
- Victorian ritual of self-presentation (*Barbas*)
- Intrusions, unauthorized use of image (Pavesich case)
- Warren and Brandeis

Pavesich v. New England Insurance Co.



THE CONSTITUTION: ATLANTA, GA., SUNDAY, NOVEMBER 15, 1903

DO IT NOW.
THE MAN WHO DID.

DO IT WHILE YOU CAN.
THE MAN WHO DIDN'T.

THESE TWO PICTURES TELL THEIR OWN STORY.

"In my healthy and productive period of life I bought insurance in the New England Mutual Life Insurance Co., of Boston, Mass., and today my family is protected and I am drawing an annual dividend on my paid-up policies."

"When I had health, vigor and strength I felt the time would never come when I would need insurance. But I see my mistake. If I could recall my life I would buy one of the New England Mutual's 18-Pay Annual Dividen-Policies."

THOMAS B. LUMPKIN, General Agent,
1008-1009-1010 EMPIRE BUILDING.

New England Insurance Co. ad

Social revolution

- Dehumanizing workplace
- *True self*
- Personality ideal
- Non-spontaneous display of private self
- Personality as a *product*
- Hollywood
- Instant celebrity

Outline

SnT
securityandtrust.lu

1. Privacy in history
2. Privacy vs. data protection
3. Data protection theory and practice
4. Data protection and IT
5. Engineering data protection

Warren and Brandeis

- *The Right to Privacy*, 1890
- 8132 citations (Google Scholar)
- Marriage of Warren's niece
- "The press is overstepping in every direction the obvious bounds of propriety and decency"
- Beginning of privacy torts

Dean Prosser

- *Privacy*, 1906
- Classification of privacy torts
  - Intrusion
  - Public disclosure of private facts
  - False light in the public eye
  - Appropriation
- Mainly for public figures
- Milestone for future decisions

Bloustein

- *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 1964
- Betrayal of Warren and Brandeis
- Monetary value vs. human dignity
- Not four torts but just one
- "Liberty as individuals to do as we will"

Death of the torts

- *Newsworthiness*
- Example: Sidis, 1941
- All privacy torts lost to newsworthiness

Federal laws

- Privacy Act, 1974
  - Mostly concerning agencies and disclosure

Federal laws

- Privacy Act, 1974
    - Mostly concerning agencies and disclosure
- Electronic Communications Privacy Act (ECPA), 1986
    - Wiretapping limitations extended to electronic communications

Federal laws

- Privacy Act, 1974
  - Mostly concerning agencies and disclosure
- Electronic Communications Privacy Act (ECPA), 1986
  - Wiretapping limitations extended to electronic communications
- Health Insurance Portability and Accountability Act (HIPAA), 1996
  - Protection of medical data against unauthorized access

Federal laws

- Privacy Act, 1974
  - Mostly concerning agencies and disclosure
- Electronic Communications Privacy Act (ECPA), 1986
  - Wiretapping limitations extended to electronic communications
- Health Insurance Portability and Accountability Act (HIPAA), 1996
  - Protection of medical data against unauthorized access
- Gramm-Leach-Bliley Act (GLBA), 1999
  - Data security and integrity in financial services

Federal laws

- Privacy Act, 1974
  - Mostly concerning agencies and disclosure
- Electronic Communications Privacy Act (ECPA), 1986
  - Wiretapping limitations extended to electronic communications
- Health Insurance Portability and Accountability Act (HIPAA), 1996
  - Protection of medical data against unauthorized access
- Gramm-Leach-Bliley Act (GLBA), 1999
  - Data security and integrity in financial services

Then came the PATRIOT Act.

And now for something completely different

- European Convention on Human Rights (ECHR), art. 8
- *Hessisches Datenschutzgesetz*, 1970
- Convention n. 108, 1981
- Data Protection Directive (DPD), or Directive 95/46/EC, 1995
- Electronic Privacy Directive (EPD), or Directive 2002/58/EC, 2002
- Charter of Fundamental Rights of the European Union, art. 8, 2009
- Recommendations and opinions of the European Data Protection Supervisor (EDPS)
- General Data Protection Regulation (GDPR), 2015 (maybe)

Data protection 101

- Focus on protecting the personal data
  - Damage in itself, not for the monetary value
- Judicial enforcement
- Applies to any form of data processing
  - Paper archives
  - Electronic processing

Data protection reform

- Stefano Rodot\'a, *Elaboratori elettronici e controllo sociale*, 1973
- Birth of new technologies
  - Social networks
  - Ubiquitous computing, IoT
  - "Bounces"
- Need for a uniform legislation
  - GDPR
  - Directive for criminal investigation

European law

Primary law

- Treaty on European Union (TEU)
- Treaty on the Functioning of the European Union (TFEU)
- Charter of Fundamental Rights of the European Union
    - Which is not the European Convention on Human Rights

European law

Primary law

- Treaty on European Union (TEU)
- Treaty on the Functioning of the European Union (TFEU)
- Charter of Fundamental Rights of the European Union
    - Which is not the European Convention on Human Rights

Secondary law

- Regulations
- Directives
- Decisions
- ... (recommendations, framework directives...)
- http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm

Directive vs. Regulation

Directive

- Sets a minimum standard
- Must be implemented in Member State law
  - Italy: legislative decree
- Not directly applicable
- Self-executing

Directive vs. Regulation

Directive

- Sets a minimum standard
- Must be implemented in Member State law
  - Italy: legislative decree
- Not directly applicable
- Self-executing

Regulation

- Sets a uniform legislation
- Directly applicable in Member State law
- Does not need implementation
  - Some Member States initially did
- Generic provisions

Data protection principles

- Data subject, controller, processor
- Consent
- Purpose limitation
- Sensitive data
- Right of access
- Right of opposition
- Data Protection Authority (DPA)
- Data transfer
- Necessity (Germany & Italy)

New in the GDPR

- Data minimization
- Data Protection Officer (DPO)
- Right to erasure
- Privacy by Design (PbD)
- Privacy by Default
- Inquisitive powers
- Exemptions (journalism, research, healthcare. . .)

Europe vs. US

EU

US

EU law vs. US operators

- EU law applies in EU (*really?*)
- Most controllers are US-based
- Cookies

EU law vs. US operators

- EU law applies in EU (*really?*)
- Most controllers are US-based
- Cookies

The EDPS idea

- You use cookies
- You store data on the data subject's computer
- So you use EU-based equipment
- Then you are subject to EU law and must protect personal data

EU law vs. US operators

- EU law applies in EU (*really?*)
- Most controllers are US-based
- Cookies

The EDPS idea

- You use cookies
- You store data on the data subject's computer
- So you use EU-based equipment
- Then you are subject to EU law and must protect personal data

Meanwhile, in the US, the NSA requests access

What would you do?

International Safe Harbor Privacy Principles

- Introduced in 2000
- Set of 7 rules
- Allow US companies to process data in EU
- Then came 2001

PATRIOT Act + Snowden + Max Schrems

Safe Harbor now

Outline

1. Privacy in history

2. Privacy vs. data protection

3. Data protection theory and practice

4. Data protection and IT

5. Engineering data protection

What *is* data protection?

It is the right of the individual that personal data pertaining to him or her are processed in a fair and transparent manner.

What *is* data protection?

It is the right of the individual that personal data pertaining to him or her are processed in a fair and transparent manner.

Conflicts with...

- Freedom of expression
- Access to documents
- Freedom of arts and science
- Protection of property

Data protection is *not* privacy

Can't shop if my data are "private"

Main problem

- Data protection law is EU
- Most controllers are US-based
- No application
- Subject to US laws
- US privacy policies

Consent

The law requires the data subject's consent.

Consent

The law requires the data subject's consent.
A lot of processing without consent.

Try these!

- Ghostery
- Lightbeam

Actual consent

- By means of privacy policies
- EU vs. US
- Information flooding = no information
- "Herod clause"
- *Take or leave*

Purpose limitation

Data processing only for the specified purpose to which the data subject has consented.

Purpose limitation

Data processing only for the specified purpose to which the data subject has consented.

- Lack of transparency and clear information
- Inefficient supervision
- Hard to track violations

Right of access

The law grants access to one's own personal data

Right of access

The law grants access to one's own personal data

Max Schrems has shown the problems of the right of access.

Right of opposition

The law grants the right of opposition:

- if there is a prejudice
- in any case against advertising

Right of opposition

The law grants the right of opposition:

- if there is a prejudice
- in any case against advertising

- "Unsubscribe"
- Registry of opposition

Third parties

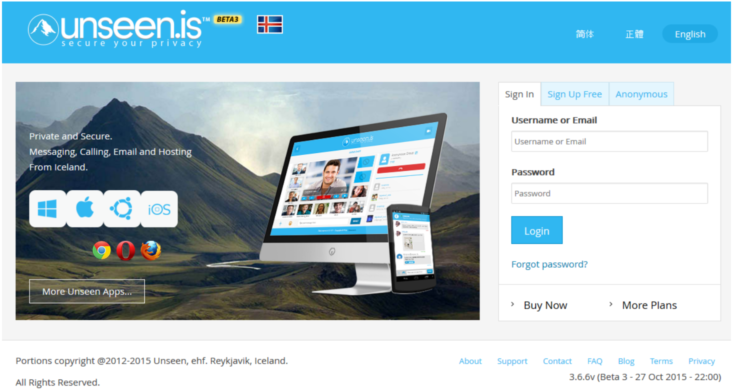
Several requirements for transferring to third parties.

Third parties

Several requirements for transferring to third parties.

- Many transfers from without EU
- NSA

After Snowden. . .



unseen.is™ BETA3
secure your privacy

简体 正體 English

Private and Secure.
Messaging, Calling, Email and Hosting
From Iceland.

More Unseen Apps...

Sign In | Sign Up Free | Anonymous

Username or Email

Username or Email

Password

Password

Login

Forgot password?

› Buy Now › More Plans

Portions copyright @2012-2015 Unseen, ehf. Reykjavik, Iceland.

All Rights Reserved.

About Support Contact FAQ Blog Terms Privacy

3.6.6v (Beta 3 - 27 Oct 2015 - 22:00)

Try to whois/traceroute this!

Cookies

- EU is overattentive about cookies
- Many opinions by the EDPS
- Cookie notices
- Problem: cookies are almost necessary in modern web

Profiling

Law: no decision based solely on profiling.

Profiling

Law: no decision based solely on profiling.

- Dangers of profiling (*Hildebrandt*)
- Crossing information for profiling (*Ohm*)
- Identity is not required
- Profiling virtual persons

DPAs

Authorities have reactive powers.

DPAs

Authorities have reactive powers.

- Inefficient
- Slow
- Few IT experts

What is missing?

Personal opinion

Data protection should be partitioned into two categories:

- "Typical" processing
  - Shops, IT/mail providers, booking services, chats. . .
  - Codes of conduct (Articles 38–39 of the GDPR)
  - Streamline the legal requirements if they comply
- "Non-typical" processing
  - Unique services, advertisement, financial services
  - Anything that is not recognized as secure
  - Thorough checking (consent, documentation, etc.)
  - Display little significant information

Outline

securityandtrust.lu

1. Privacy in history
2. Privacy vs. data protection
3. Data protection theory and practice
4. Data protection and IT
5. Engineering data protection

"Privacy"

Common misconception

- Data protection = privacy
- Secrecy, concealment

"Privacy"

Common misconception

- Data protection = privacy
- Secrecy, concealment

Consequently...

- "I have nothing to hide" (*Solove*)
- "They were free to decline" (*Smith v. Chase Manhattan Bank*)
- No single act
- US case

Subset of security

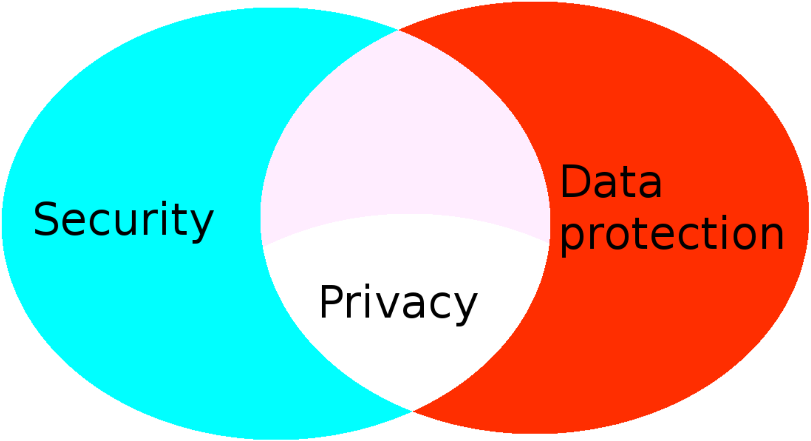
Also for IEEE

Subset of security

Also for IEEE

But the law is the other way around.

A more realistic view



Distinguishing between privacy and data protection

Dangers

- Tracking tools
- Profiling techniques
    - Respawning cookies
    - Flash cookies
    - Canvas watermarking
- Claudia Diaz, *The Web never forgets*, 2010
- Defenses
    - The Onion Ring (TOR)

Dangers

- Tracking tools
- Profiling techniques
  - Respawning cookies
  - Flash cookies
  - Canvas watermarking
- Claudia Diaz, *The Web never forgets*, 2010
- Defenses
  - The Onion Ring (TOR)

PEBCAK

Standards

What do companies need?

Standards

What do companies need?

Problems

- Few standards or privacy
  - ISO 27018:2014
- Something in security standards
  - ISO 27001:2013
  - CSA matrix
  - ...
- No standards for data protection

Techniques

- Separation of roles (organizational)
- Anonymization
  - *k*-anonymity
  - *l*-diversity
  - *t*-closeness
  - Differential privacy
- Paul Ohm, *Broken promises of privacy: Responding to the surprising failure of anonymization*, 2010

Languages

Several languages for privacy policies:

- W3C Platform for Privacy Preferences (P3P), 2002
- W3C A P3P Preference Exchange Language (APPEL), 2002
- Enterprise Privacy Authorization Language (EPAL), 2003
- eXtensible Access Control Markup Language (XACML) Privacy Policy Profile, 2010
  - urn:oasis:names:tc:xacml:2.0:resource:purpose
  - urn:oasis:names:tc:xacml:2.0:action:purpose

Outline

1. Privacy in history
2. Privacy vs. data protection
3. Data protection theory and practice
4. Data protection and IT
5. Engineering data protection

Addressing the problem

Many stakeholders involved:

- Legislator
- Controller
- Processor
- DPO
- Data subject
- Auditor
- DPAs
- Standard committees

Perspectives

1. Identify the requirements
   - Requirements engineering
   - Tropos, i*, SysML...
2. Comply with the law
   - Define the data protection policy
   - Show the highlights to the user
   - Natural Language Processing (NLP) could be useful here
3. Design for data protection
   - Modeling tools
   - Software engineering
   - Verification and validation (V&V)
4. Maintain
   - Regression
   - Monitoring

Data protection by design/by default

- Article 23 of the GDPR
- By design: have data protection in mind from early stages
    - Often mentioned as Privacy by Design (PbD)
- By default: settings for the dumb user
    - Often ignored

My recent work

- Define an ontology for data protection
  - With a focus on the controller's legal requirements
- Integrate it into a design model
  - Unified Modeling Language (UML)
  - WS-BPEL
  - Business Process Model and Notation (BPMN)

My recent work

SnT
securityandtrust.lu

- Define an ontology for data protection
  - With a focus on the controller's legal requirements
- Integrate it into a design model
  - Unified Modeling Language (UML)
  - WS-BPEL
  - Business Process Model and Notation (BPMN)

What next?

- Improve the ontology
- Model requirements elicitation
- Define a testing/compliance methodology

Thank you for your attention