UiO : Institutt for privatrett
Det juridiske fakultet

Lee A. Bygrave, Norwegian Research Center for Computers and Law

# Security by Design: The Emperor’s New Clothes in the Cybersecurity Space?

[Presentation for UniMelb, 26.10.2018]

# A perfect storm …

- IoT brings myriad of new security vulnerabilities, yet …
- security does not pay, yet …
- we pay a potentially large price for insecurity, and …
- security is not cheap either.

# SbD as nascent policy goal for EU

European Commission prioritises:

‘[t]he use of “security by design” methods in low-cost, digital, interconnected mass consumer devices which make up the Internet of Things’

- – European Cyber Security Strategy (September 2017)

- SbD already implicit in General Data Protection Regulation (GDPR) Article 25, espec. 25(2)

# GDPR Art. 25(2): ‘data protection by default’

‘The controller shall implement appropriate technical and organisational measures for ensuring that, by default, … personal data are not made accessible without the individual’s [i.e. data subject’s] intervention to an indefinite number of natural persons.’

# SbD as nascent policy goal for UK

Companies encouraged to ‘design [IoT] products and services with security in mind, from product development through to the entire product lifecycle’

- UK Department for Digital, Culture, Media & Sport, *Security by Design* (March 2018)

- Draft Code of Practice issued; with <threat> of legislation

# SbD as policy goal for Australia

- Predominantly industry-led discourse
- IoTAA = key player; explicitly 'promotes a "security by design" approach to IoT'
  - *IoT Security Guideline v1.2* (November 2017); sets out comprehensive 'IoT Trust Framework'

- Broad security requirements under, i.a., data privacy law and *Telecommunications and Other Legislation Amendment Act 2017*, but no express 'SbD' element

# SbD as new statutory requirement for California

**IoT Security Act: TITLE 1.81.26. Security of Connected Devices (in effect from 1 January 2020)**

(a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

(2) Appropriate to the information it may collect, contain, or transmit.

(3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure

# Californian IoT Security Act (2)

**TITLE 1.81.26. Security of Connected Devices**

…

(b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:

> (1) The preprogrammed password is unique to each device manufactured.
>
> (2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

# SbD: The New Kid on the Block?

- ECMS → DRMS → PETs → PbD → DPbD → SbD
- Broader lineage of 'Value-Sensitive Design' (e.g., Wiener 1954; Friedman 1997; Spiekermann 2016)
- Inflation? (cf. 'Administrative Law by Design': Motzfeldt 2017)

# The legal-regulatory vision

- *Ex post* → *ex ante* application of legal norms
- Use of law to buttress hardwiring (cp. copyright law with data protection law)
  - Cf. 'legal protection by design' / 'ambient law' (Hildebrandt 2015)

# SbD: semantics

- What = security?
  - – More than safeguarding CIA?
- What = ‘by design’?
  - – Polysemantic character of ‘design’
  - – Intentional security vs incidental security
  - – How ‘hard’ does the hardwiring have to be?
    - Cp. debate over status of P3P

# Methodological challenges (1)

- By what standards do we measure differing degrees of security?
  - Cp Cavoukian 2009: ‘*Privacy by design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any IT system or business practice.’ What is meant by ‘maximum degree of privacy’?
  - What would = max. security?
  - SbD functionalities ≥ legal reqs.?

# Methodological challenges (2)

- Paucity of operational principles as opposed to rhetorical flourish
- Cp. Cavoukian's PbD principles
  - 'Proactive not Reactive; Preventative not Remedial
  - Privacy as the Default
  - Privacy Embedded into Design
  - Full Functionality: Positive-Sum, not Zero-Sum
  - End-to-End Lifecycle Protection
  - Visibility and Transparency
  - Respect for User Privacy.'

# SbD: practical problems (1)

- IS often end up being used beyond what designers can predict
- Discord between how designers of IS conceptualise functionalities and aims of system and how users conceptualise (and experience) these.
  - ‘users and designers do not …share the same model of the task domain’ (Dourish 2001: 131).
- IS development has many stages and endpoint is often unclear

# SbD: practical problems (2)

- Poor market traction
- Poor traction/understanding amongst ICT engineers
  - Security only just becoming mandatory component of computer science degree courses!
  - Potential clash with ‘mimimum viable product’ approach?
- Insufficient focus on communicative and behavioural (user-centric) aspects of design

# SbD: political issues

- Does SbD ‘design away’ politics?
- Does SbD make value choices too easy for consumers?
- Can SbD get in the way of consumer satisfaction?
  - e.g., Sony PS3 dispute

# SbD: political issues (2)

- Does SbD add to ‘security theatre’?
- Whose vision/standards of security does SbD promote?
- Can SbD undermine civil liberties?
  - SbD may reinforce ‘securitisation’ of government policy in authoritarian direction

# SbD: legal-regulatory challenges

- Very few ‘hard law’ codes expreslly addressing SbD
- Notable exception = GDPR, but has significant weaknesses (highlighted later)
- Emerging SbD rules have narrow focus (IoT)

# GDPR Art. 25: shortcomings

- Few hardwiring incentives (apart from sanctions; yet stiff sanctions unlikely applied)
  - But reasonable efforts to hardwire are important re measuring fines (Art. 83(2)(d))
- Stunted ‘regulatory conversation’ (Black) with ICT engineers
- Further on shortcomings: see Bygrave 2017
- Traction on GAFAM?
  - Norwegian Consumer Council: ‘Deceiving by Design’ (June 2018)

# Some judicial support for SbD

- ECtHR in *I v Finland* (2008) – implementing technological measures to ensure confidentiality of pasient data is positive obligation under ECHR Art. 8
- CJEU in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* – traffic data retention
- CJEU stops PIT (in form of DPI) in *SABAM* cases of 2011 and 2012.

# References

- Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) *Oslo Law Review* 105
- Dourish, *Where The Action Is: The Foundations of Embodied Interaction* (MIT Press 2001)
- Friedman (ed), *Human Values and the Design of Computer Technology* (Cambridge University Press 1997)
- Hildebrandt, 'Legal Protection by Design: Objections and Refutations' (2015) 5(2) *Legisprudence* 223.
- Motzfeldt, 'The Danish Principle of Administrative Law by Design' (2017) 23(4) *European Public Law* 739
- Spiekermann, *Ethical IT Innovation: A Value-Based System Design Approach* (Taylor & Francis 2016).
- Wiener, *The Human Use of Human Beings: Cybernetics and Society* (Doubleday Anchor 1954).