UiO : Det juridiske fakultet

Lee A. Bygrave, NRCCL

Security by Design: Aspirations and Realities in a Regulatory Context

[XXXVI Nordic Conference on Law and IT; 10 Nov. 2021]

Friends you can trust …

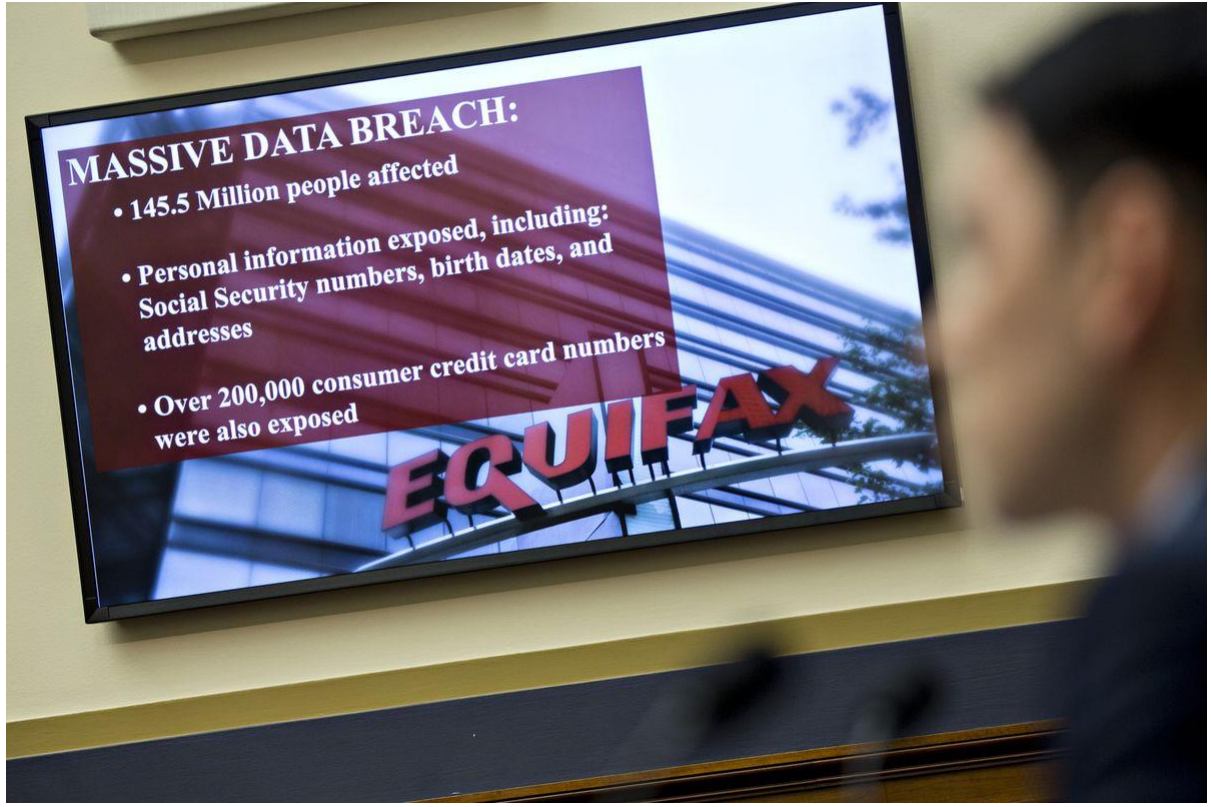
‘A market for lemons’

A perfect storm

+

=

Security by disaster



Security by Design (SbD) as public policy ideal in Europe

2013: European Commission invited stakeholders 'to stimulate the development and adoption of … security-by-design and privacy-by-design principles by ICT product manufacturers and service providers'

- 'Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace' (JOIN(2013) 1 final)
- NB: OECD embraced SbD already in 2002 (!) – see principle of 'security design and implementation' in 'Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security' (25 July 2002)

IoT focus

2017: Commission prioritizes '[t]he use of "security by design" methods in low-cost, digital, interconnected mass consumer devices which make up the Internet of Things'

- 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' (JOIN(2017) 450 final)

Norway: IKT-sikkerhetsutvalget

‘Ansvaret for IKT-sikkerhet … bør i større grad flyttes fra forbrukeren til produsentene og leverandørene. For å oppnå dette, bør det blant annet stilles krav om innebygd sikkerhet («Security by design») i tilkoblede produkter og tjenester’

– NOU 2018: 14, ‘Sikkerhet i alle ledd’, p. 11 (see too pp. 87, 88, 96)

Legal manifestations

- EU Cybersecurity Act
- Electronic Communications Code

EU Cybersecurity Act, recital 12

‘Organisations, manufacturers or providers involved in … design and development of ICT products, ICT services or ICT processes should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised (“security-by-design”)’

EU Cybersecurity Act, recital 13

‘Undertakings, organisations and the public sector should configure the ICT products, ICT services or ICT processes designed by them in a way that ensures a higher level of security which should enable the first user to receive a default configuration with the most secure settings possible (“security by default”).’

EU Cybersecurity Act, Art. 51(1)

European cybersecurity certification scheme established pursuant to the Act ‘shall be designed to achieve’, i.a., that ‘ICT products, ICT services and ICT processes are secure by default and by design’

ECC, recital 97

‘In order to safeguard security of networks and services, … where necessary, encryption should be mandatory in accordance with the principles of security and privacy by default and by design.’

- So SbD is now a principle in EU law?

SbD = principle in respect of personal data

- Arts. 32, 25, 24 and 5(1)(f) GDPR (and equivalents in LED and EUIDPR)
- ECtHR: *I v Finland* (2008)
  - need for ‘practical and effective protection to exclude any possibility of unauthorised access’ (para. 47)
- CJEU: *Digital Rights Ireland* (2014)
  - ‘Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data’ (para. 40)

Sectoral SbD requirements o/side data protection law

- Medical Devices Regulation 2017
- Digital Content Directive 2019
- Financial Markets Directive 2014
- eIDAS Regulation 2014
- NISD 2016
  - cf. stronger salience of SbD ideals in Art. 18 of proposed NIS2 Directive

SbD as principle in respect of non-personal data?

- Tjaa … variation re. sector and actor
- E.g. NISD
  - Applies to ‘operators of essential services’ and ‘digital service providers’
  - ‘[t]echnical and organisational measures imposed on operators of essential services and digital service providers should not require a particular commercial information and communications technology product to be designed, developed or manufactured in a particular manner’ (recital 51)
    - Does this rule out SbD? [Arnbak: yes. Me: no]

Proposal for EU law on ‘Cyber Resilience’

Across ‘the pond’ …

TITLE 1.81.26. Security of Connected Devices (Cal. Civil Code Pt. 4 Div. 3) [in effect from 1 Jan. 2020]

§ 1798.91.04(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

What is behind SbD's popularity?

- Intuitive appeal
- Scandal and economics
- Prior design constraints
- Regulatory (and rhetorical) trends

SbD: The New Kid on the Block?

- Copyright: ECMS → DRMS
- Privacy: PETs → PbD → DPbD
- Broader lineage of ‘Value-Sensitive Design’
  - e.g., Wiener 1954; Friedman 1997; Spiekermann 2016)
- Inflation?
  - e.g. ‘administrative law by design’ (Motzfeldt 2017); ‘fair use by design’ (Elkin-Koren 2017); ‘ethics by design’ (European Parliament 2019)

The legal-regulatory vision

- *Ex post* → *ex ante* application of legal norms
- *De facto* 'automation' of legal norms
  - Cf. notion of 'ambient law' (Hildebrandt & Koops)
- Use of law to buttress hardwiring

Semantics

- What = security?
  - More than protection of ‘CIA’?
  - Relationship to ‘safety’?
- What = ‘by design’?
  - Polysemantic character of ‘design’
    - McKay, Marshall and Heath 2010
  - Intentional security vs incidental security
    - Cp. ‘Security by disaster’ and ‘security by accident’
  - How ‘hard’ does the hardwiring have to be?
    - Cp. debate over status of P3P

Methodological challenge(s)

- 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 = maximum security?

Methodological challenge(s) and law

- SbD functionalities ≥ legal reqs.?
- Legal requirements …
- Near-complete security that is result of best effort?

EU Cybersecurity Act, recital 12

‘Organisations, manufacturers or providers involved in … design and development of ICT products, ICT services or ICT processes should be encouraged to … protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised (“security-by-design”)’

The role of proportionality

- ‘appropriate’ measures in light of contextual factors
  - See e.g. Art. 32 GDPR
- Security that is result of best reasonable effort
  - ‘an obligation of means’ (not ‘result’) (van Alsenoy 2016)
- Cf. Case C-340/21, *VB v Natsionalna agentsia za prihodite* (pending)

Practical challenges

- IS often end up being used beyond what designers can predict
  - Amara's law: 'We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run'.
- Discord) between how designers of IS conceptualise functionalities and aims of system and how users conceptualise these.
  - 'the users and designers do not, in fact, share the same model of the task domain' (Dourish 2001)
- IS as amorphous, inchoate structures

Practical challenges (2)

- Poor market traction
  - Collision with perceived innovation needs?
- Poor traction amongst ICT engineers
  - Security only just becoming mandatory component of computer science degree courses!
  - Security regarded as neither engineers' responsibility nor pleasurable (Spiekermann and others 2019)
  - Potential clash with 'agile' software programming and 'minimum viable product' approach

Politics of SbD

- Does SbD ‘design away’ political problems?
- Can SbD get in the way of consumer satisfaction?
  - Cf. Sony’s PS3 ‘security’ measures
  - NB. California’s IoT Security Act does not ‘impose any duty upon the manufacturer of a connected device to prevent a user from having full control over a connected device, including the ability to modify the software or firmware running on the device at the user’s discretion’ (§ 1798.91.06(c))

Politics of SbD (2)

- Whose vision of security does SbD promote?
- Can SbD reinforce ‘securitization’ of govt policy in authoritarian direction?
- Does SbD add to ‘security theatre’?

Organizations you can trust …