# Designing Privacy and Security: Beyond the Technical Perspective

**Charles D. Raab**

**Professorial Fellow**

**Director of CRISP (Centre for Research into Information, Surveillance and Privacy)**

**University of Edinburgh**

ENISA/DG CONNECT/UNIVERSITY OF LUXEMBOURG

***Annual Privacy Forum 2015: 'Bringing Research and Policy Together'***

Luxembourg, 7-8 October 2015

# To Begin: Privacy by Design and by Default

**Council of the EU, Brussels, 11 June 2015 (OR. en) 9565/15 Compromise Text of General Data Protection Regulation**

*Article 23* ***Data protection by design and by default***

1. (…) Having regard to available technology and the cost of implementation and taking account of *the nature, scope, context and purposes of the processing* as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall implement (…) technical and organisational measures appropriate to the processing activity being carried out and its objectives, such as data minimisation and pseudonymisation, in such a way that the processing will meet the requirements of this Regulation and protect the rights of (…) data subjects.

2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary for each specific purpose of the processing are processed; this applies to the amount of (…) data collected, the extent of their processing, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.

# What Must We Know about PbD? (1)

CRISP, *Designing Privacy In: Setting the Research Agenda* (March 2015)

- Any evidence that businesses value PbD?
- Any evidence that PbD actually protects privacy?
- How does an organisation in a supply chain negotiate appropriate privacy levels for their business model?
- Who in the organisation is tasked with PbD? Is a champion necessary?
- Is PbD scalable? Can it be implemented across the whole organisation or even between organisations?
- What inhibits the adoption of PbD by designers and companies (i.e., resources, lack of understanding, perceptions of competitive environment, etc.)?
- How can PbD performance be certified, measured and monetised?
- What corporate reporting mechanisms and techniques need to be developed for effective PbD practice?

# What Must We Know about PbD? (2)

CRISP, *Designing Privacy In: Setting the Research Agenda* (March 2015)

- What regulatory and legal instruments are appropriate to encourage PbD?
- Should PbD be seen only as a way of complying with data protection law?
- Could PbD play a role in building relationships between data controllers and data subjects?
- When and why do organisations begin to bother about privacy?
- Can self-audit be encouraged? Can accountability for PbD be engineered?
- How can privacy be promoted as part of an organizational culture?
- Are voluntary international standards possible? Can they be incentivised?
- Can the media, pressure groups, and NGOs play a role in promoting and monitoring PbD?

# What Must We Know about PbD? (3)

CRISP, *Designing Privacy In: Setting the Research Agenda* (March 2015)

- How is privacy experienced, felt and acted upon by service users?
- Why and how do individuals care about privacy?
- How can we learn what they require in terms of privacy protection?
- How can PbD research be used to educate the public about privacy, their rights, and their data management?
- How can public understanding of privacy and privacy rights be improved?
- Are companies' reputations really at stake if they do not adopt PbD?
- What are the trust issues in the value/supply chain around PbD?
- What would a privacy friendly internet look like?

***But what is 'privacy'?***

# Privacy: Individual Value

- No single definition or conceptualisation
- Deontological and consequentialist value
- Seven types (Finn, *et al.,* 2013): privacy of:
    - the person
    - behaviour and action
    - communication
    - data and image
    - thoughts and feelings
    - location and space
    - association
- Context-dependent (Nissenbaum, 2010)

# Individual Privacy

- Conventional privacy paradigm: individualistic, classical liberal, rights-oriented only
- Leads to (tendentious) 'privacy v. public interest/security/etc.' construct
- Privacy is indeed an individual right: fundamental but not absolute
- But privacy's importance goes beyond that of the individual: a crucial underpinning of interpersonal relationships, of society itself, and of the workings of democratic political system
- To consider privacy only as an individual right is to ignore its value in these other dimensions
- When individual privacy is protected, the fabric of society, the functioning of political processes and the exercise of important freedoms are thereby protected. When it is eroded, society and the polity are also harmed; it is in the public interest, and not only in the interest of the individual, to protect privacy

# Privacy: Social Value

- Common value: all have common interest in right to privacy but may differ on specific content of their privacy or what they think sensitive
- Public value: privacy instrumentally valuable to democratic political system, e.g., for freedom of speech and association, and for setting boundaries to state's exercise of power
- Collective value: economistic conception of privacy's value as collective, non-excludible good that cannot be divided and that cannot be efficiently provided by market (Regan, 1995)
- Many other writers (Westin, 1967; Solove, 2008; Schoeman, 1992; Bygrave, 2002; Goold, 2009; Steeves, 2009; Raab, 2014, 2012; …)
- Society, not just the individual, is better off when privacy exists
- Based on understanding privacy's importance for society, social and political relationships; not only for individual rights or values

# But What About Security?

- Is privacy the only important value in policy-making?
- Does PbD interfere with other public goods that should be pursued, such as national security?
- Are national security interests antagonistic to PbD and PETs?
- How can national security be reconciled with:
  - data minimisation?
  - anonymity/pseudonymity?
  - '…the extent of their processing, the period of their storage and their accessibility'?
  - 'only (…) personal data (…) which are necessary for each specific purpose of the processing are processed; this applies to the amount of (…) data collected, the extent of their processing, the period of their storage and their accessibility [through data-sharing]'?

# Definitions of 'Security'

- '[T]he condition (perceived or confirmed) of an individual, a community, an organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made).' (adopted by CEN BT/WG 161 on Protection and Security of the Citizen, January 2005; cited in Martí Sempere, 2010: 6)

- '[A] fundamental *good* without which societies cannot prosper.'(Martí Sempere 2010: 2; emphasis in original)

- 'The concept of security has for too long been interpreted narrowly: as security of territory from external aggression, or as protection of national interests in foreign policy or as global security from the threat of a nuclear holocaust. It has been related more to nation-states than to people….Forgotten were the legitimate concerns of ordinary people who sought security in their daily lives. For many of them, security symbolized protection from the threat of disease, hunger, unemployment, crime, social conflict, political repression and environmental hazards…In the final analysis, human security is a child who did not die, a disease that did not spread, a job that was not cut, an ethnic tension that did not explode in violence, a dissident who was not silenced. Human security is not a concern with weapons–it is a concern with human life and dignity. …Human security is *peopLe-centred.* ' (UNDP, Human Development Report 1994: 22-23)

# ‘Security’

- As with privacy, many ways of understanding this or its cognate, ‘safety’
- Individual or personal security
- ‘Collective’ security at many levels: international, national, local, neighbourhood, social group
- Objective security: probabilities of risk
- Subjective security: feelings of (in)security
- Which of these should prevail, and how can be reconciled?
- ‘A man’s home is his castle’: privacy and liberties/freedoms can be regarded in some respects as valuable because of the security and safety – not least, of personal data – they provide for individuals, groups and societies (cf. *Liberty and Security in a Changing World:* 14)
- If so, the relationship between privacy and security is far more complex and cannot be glossed over by a rhetoric of the ‘opposed’ rights or values of security and privacy

# Security/Safety: Types

- Physical security: to safeguard the physical characteristics and properties of systems, spaces, objects and human beings
- Political security: protection of acquired rights, established institutions/structures and recognized policy choices
- Socio-Economic security: economic measures to safeguard individuals
- Cultural security: to safeguard the permanence of traditional schemas of language, culture, associations, identity and religious practices
- Environmental security: to provide safety from environmental dangers caused by natural or human processes
- Radical uncertainty security: to provide safety from exceptional and rare violence/ threats not deliberately inflicted by an external or internal agent but can still threaten drastically to degrade the quality of life
- Information security: to protect information and information systems from unauthorized access, modification or disruption
- Human security: to cope with various threats in the daily lives of people
- National security: to protect the integrity of sovereign state territory and assets

(Source: partly drawn from PRISMS FP7 project, Deliverable 2.1: *Preliminary report on current developments and trends regarding technologies for security and privacy*, 28 February 2013: 11-12)

# Security/Safety: Levels

- Grand (macro)
  - terrorism
  - organised crime
  - war
  - immigration
  - environmental hazards
  - nuclear accidents
  - earthquakes
  - epidemics
  - *tsunamis*
  - defence of sovereign territory
  - critical infrastructure protection
- Everyday (micro/ meso)
  - loose stair carpets
  - slippery bathtubs
  - kitchen fires
  - playground accidents
  - car crashes
  - unemployment
  - homelessness
  - workplace hazards
  - 'serial killer', 'obtrusive beggar', 'mugger', 'stalker', prowler' 'poisoner of water or food' (Bauman, 2006)

# Conflict Between Privacy and Security/ Safety?

- ‘[t]he realm of rights, private choice, self-interest, and entitlement…[*versus*] corollary social responsibilities and commitments to the common good… [their neglect has] negative consequences such as the deterioration of public safety…’ (Etzioni 1999: 195)

***But what does this ignore?***

# Security/Safety and Privacy: Individual and Public Interest

- If both privacy and security are contested and inter-related concepts, the idea that they can be 'balanced' or 'traded-off' must also come under sceptical scrutiny
- Whether 'balancing' is between one individual right and another, or between an individual right and a collective right, or between an individual right and social or collective utility/interest, requires specification if 'balancing' – even if inescapably built into our mindset – is to be removed from the realm of shorthand and slogan

security (public interest) v privacy (individual interest)

OR

security (public interest) v privacy (public interest)

**

security (individual interest) v privacy (public interest)

OR

security (individual interest) v privacy (individual interest)

# Intelligence and Security Committee of Parliament: Call for Evidence (2013)

- 'In addition to considering whether the current statutory framework governing access to private communications remains adequate, the Committee is also considering the appropriate balance between our individual right to privacy and our collective right to security.'
- Rhetorical and imprecise, impeding deeper understanding of what is at stake for the individual, society and the state
- Three difficulties:

    'privacy'

    'security'

    'national security v. personal privacy' framing

# Review Group on Intelligence and Communications Technologies
# *Liberty and Security in a Changing World* (12/12/13)

'We suggest careful consideration of the following principles: [pp.14-16]

'1. The United States Government must protect, at once, two different forms of security: national security and personal privacy.

'In the American tradition, the word "security" has had multiple meanings. In contemporary parlance, it often refers to national security or homeland security. One of the government's most fundamental responsibilities is to protect this form of security, broadly understood. At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ". Both forms of security must be protected.'

# 'Balance'?

- 'The idea of "balancing" has an important element of truth, but it is also inadequate and misleading. It is tempting to suggest that the underlying goal is to achieve the right "balance" between the two forms of security [national security and personal privacy]. …But some safeguards are not subject to balancing at all. In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, and gender.' (Review Group on Intelligence and Communications *Technologies, Liberty and Security in a Changing World* (12/12/13))
- Conventional privacy paradigm proposes 'balancing' as policy aim (but thumb on scale)
- Unsatisfactory about 'balance' (e.g., Loader and Walker, 2007: 54-56; Hildebrandt, 2013; Waldron, 2003; Dworkin, 1977; Zedner, 2009; Raab, 1999; others)

  Noun? Verb?

  How to 'balance'? What to 'balance'?

  Common metric?

  Who should do it?

  Consensus, or exercise of power?

# ‘National Security v. Personal Privacy’ ?

- ‘How much security should we give up to protect privacy?’ is rarely asked
- Assumptions about risk, equilibrium and a common metric for weighing are not clear and doubtfully warranted
- Can we know and agree how much (and whose) privacy should or should not outweigh how much (and whose) security?
- ‘Balancing’ is silent about the method by which a balance can be determined and challenged, and about who is to determine it
- Whether ‘balance’ refers to the method, or to its outcome, is often ambiguous; legal case decisions are one source for understanding, and perhaps disputing, the weighing process and the arguments used, for instance about necessity and proportionality
- Remains to be seen how these understandings can be disseminated in the much more closed conditions of the intelligence and security service where strategic and operational decisions have to be made, and also brought to bear in their oversight and scrutiny

# Security/Safety and Privacy: Affinities

- Privacy *itself* is a security/safety value, often promoted as such
  - protective, defensive, precautionary, risk-aversion value
  - serves selfhood, autonomy, dignity, sociality
  - in face of technologically assisted policy initiatives
  - in society driven by counter-terrorism, law-enforcement, preoccupation with personal safety
  - provides secure refuge for individuals and groups
    - for inward-looking purposes
    - for external sociality and participation
    - guarding against spatial or informational encroachments
- Privacy advocates (often fear-driven) invoke precautionary principle, criticising state security policies and surveillance technologies
- 'Privacy impact assessment' based on precautionary risk-minimisation
  'securitisation' of information systems in interest of privacy
- Both privacy and security of society or state can therefore be seen as two 'takes' on public interest, changing nature of argument

# Privacy, Security, and PbD

- Information security is also (part of) information privacy, provided through technological means
- Designing-in, and defaulting to, privacy is to provide a collective good to be enjoyed by all who use the technology or system, not a good to be chosen as an 'extra' by the individual who happens to care about privacy
- '[M]any technologies and information systems exacerbate social differences….This social division is likely to happen unless privacy's collective value is explicitly recognized in organizational practice and built into the construction of information and communications technologies and systems. However, this value could be subverted if some people were better able than others to buy protective information technologies for their own use, in keeping with the individualist paradigm. This would be the information society's equivalent of "gated communities".' (Bennett and Raab, 2006: 41-2)
- This further underlines the affinity between privacy and security, whether individual or collective
- It brings *equality* into view as a neglected dimension of these debates

c.d.raab@ed.ac.uk