Privacy, Security, Surveillance and Regulation

Charles D. Raab

Professorial Fellow

School of Social and Political Science

University of Edinburgh

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

Turing Fellow, Alan Turing Institute

Presented in the Professional Issues Course, School of Informatics, University of Edinburgh, 24 October 2017

Outline of Lecture

- What is privacy?
- What is security?
- How are they related?
- What is surveillance?
- How does it relate to data science?
- What kinds of regulation?
- Privacy by design and default
- Data science and data
- Internet research
- Ethics, codes, and standards
- Bibliography

Individual Privacy

- Philosophy, social sciences, law: no single definition or conceptualisation
- Seven types (Finn, *et al.,* 2013): privacy of:
    - the person
    - behaviour and action
    - communication
    - data and image
    - thoughts and feelings
    - location and space
    - association
- Other types (Wright and Raab, 2014)
- Context-dependent (Nissenbaum, 2010)
- Conventional privacy paradigm: individualistic, classical liberal, rights-oriented only (Bennett and Raab, 2006)

Individual Privacy's Value

- Deontological (right/wrong action) and consequentialist (right/wrong consequences)
- Privacy is an individual right:
  - fundamental but not absolute (Raab, 2017)
  - 'Everyone has the right to respect for his or her private and family life, home and communications.' (Charter of Fundamental Rights of the EU, Article 7)
  - serves selfhood, autonomy, dignity, but also sociality
- Privacy's importance goes beyond that to the individual; a crucial underpinning of:
  - interpersonal relationships
  - society itself
  - the workings of a democratic political system
- When privacy is protected, the fabric of society, the functioning of political processes and the exercise of important freedoms are protected. When eroded, society and the polity are also harmed; privacy protection is both an individual and a public interest

Privacy and its Social Value (Regan, 1995)

- 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
- Many other writers on how privacy works in society and social relations

  (Goffman, many works; Westin, 1967; Altman, 1975; 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?

- Whatever 'privacy' means, it is not the only important value in policy-making, and not the only public-interest value
- Security is also a fundamental right: 'Everyone has the right to liberty and security of person. (Charter of Fundamental Rights of the EU, Article 6)
- Security (national and other) seems now to be the over-riding value, facing terrorism, crime, many kinds of adverse event
- Does this inevitably lead to (tendentious) 'privacy v. public interest/ security/etc.' construct?
- What else can be said about the relationship between privacy and security? (discussed later)

But what is 'security'?

Some 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’ in Technical Discourse

- ‘Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft and damage to their hardware, software, or information, as well as from disruption or misdirection of the services they provide’ (Wikipedia, quoting Gasser 1988, p. 3)
- This refers only to one meaning of ‘security’
- This refers only to one source of privacy violation
- Data protection (information privacy) principles include this kind of security: ‘[Personal data shall be] (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’ (EU General Data Protection Regulation, Article 5(1)(f))

Computer/cyber/IT security can protect privacy, but is only part of the whole story

Computer scientists (and related specialists) should therefore think outside their box to the wider legal and ethical frame of reference for ‘security’

Security: Types

- **Information** security: to protect information and information systems from unauthorised access, modification or disruption; computer security
- **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
- **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: Dimensions and Dilemmas

- As with privacy, many ways of understanding this
  - **Individual** or **personal** security; security of personal **data**
  - **Collective** security at many levels beyond the individual: international, national, local, neighbourhood, social group; security of **systems**
  - **Objective** security: probabilities of risk
  - **Subjective** security: feelings of (in)security
- Which (if any) of these should prevail, and how can they 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; Raab 2014)

  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

Conflict Between Privacy and Security?

- ‘[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 construction ignore?

Does this construction have any practical effect?

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: (Raab, 2017)

  'privacy'

  'security'

  'national security v. personal privacy' framing

Former UK Foreign Secretary's View

Philip Hammond, Intelligence and Security Speech at the Royal United Services Institute, 10 March 2015

'We are after all, all of us in our private lives, individuals who seek privacy for ourselves and our families, as well as citizens who demand protection by our government from those who would harm us. So we are right to question the powers required by our agencies – and particularly by GCHQ – to monitor private communications in order to do their job. But we should not lose sight of the vital balancing act between the privacy we desire and the security we need.' (emphasis added)

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’?

- Conventional privacy paradigm: ‘balancing’ as policy aim (but thumb on scale)
- Problems with ‘balance’ (e.g., Loader and Walker, 2007; Waldron, 2003; Dworkin, 1977; Zedner, 2009; Raab, 1999; RUSI, 2013; Anderson, 2013; others)
- ‘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))

'(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' is a noun or a verb, and refers to a 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/law enforcement where strategic and operational decisions have to be made, and also brought to bear in their oversight and scrutiny

PRISMS Project: Selected Survey Findings

- *Both* privacy and security important to people
- People do *not* value security and privacy in terms of 'trade-off'
- No significant relationship between people's valuation of privacy and valuation of security
- Significant correlation between valuation of personal and general security

PRISMS

Security and Privacy: Affinities (Raab, 2014, 2012)

- Privacy *itself* is a security value, often promoted as such
  - protective, defensive, precautionary, risk-aversion value
  - 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 or systems in interest of privacy (e.g., encryption)
- Both privacy and security of society or state can therefore be seen as two 'takes' on public interest, changing nature of argument

Surveillance: Types

- watching (eyes and cameras)
- listening (ears and electronic devices)
- locating/tracking
- detecting/sensing
- personal data monitoring (‘dataveillance’)
- data analytics (‘big data’)

All have potential or actual impact on ethical and social values, including privacy; but what’s that? (see earlier)

All used for purposes of security; but what’s that? (see earlier)

All subject to regulation; but how?

From Computer Science to 'Data Science'

- Data science: extracting knowledge or insights from data
- Much of the data are personal data
- Much of the personal data are gathered through surveillance
- Much surveillance uses technologies designed for that purpose
- Much of data science data uses technologies and processes designed for extracting knowledge and insights

Does this require regulation? What and how?

Regulatory Instruments

- Laws and regulatory agencies
- Codes of practice/ethics/standards
- Privacy-enhancing technologies (PETs)
- Privacy by design (and default) (PbD)
- Public awareness
- Training requirements for data users

These instruments relate to the protection of personal data, not to all forms of surveillance if personal data are not 'processed' (collected, stored, etc.)

Privacy/Data Protection by Design and by Default (1)

EU, General Data Protection Regulation (2016)

Article 25 ***Data protection by design and by default***

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Privacy/Data Protection by Design and by Default (2)

EU, General Data Protection Regulation (2016)

Recital 78

The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

Privacy, Security, and (D)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

Ethical Robotics?: BS 8611: 2016

- ‘This British Standard gives guidance on the identification of potential ethical harm and provides guidelines on safe design, protective measures and information for the design and application of robots’
- ‘Ethical hazards are broader than physical hazards. Most physical hazards have associated psychological hazards due to fear and stress. Thus, physical hazards imply ethical hazards and safety design features are part of ethical design. Safety elements are covered by safety standards; this British Standard is concerned with ethical elements’
- ‘Examples of ethical harm include stress, embarrassment, anxiety, addiction, discomfort, deception, humiliation, being disregarded. This might be experienced in relation to a person’s gender, race, religion, age, disability, poverty or many other factors’

‘Facebook reveals news feed experiment to control emotions’

‘Protests over secret study involving 689,000 users in which friends' postings were moved to influence moods’ (Robert Booth, *The Guardian*, Monday, 30 June 2014)

‘In a study with academics from Cornell and the University of California, Facebook filtered users' news feeds – the flow of comments, videos, pictures and web links posted by other people in their social network. One test reduced users' exposure to their friends' "positive emotional content", resulting in fewer positive posts of their own. Another test reduced exposure to "negative emotional content" and the opposite happened.

‘James Grimmelmann, professor of law at Maryland University, said Facebook had failed to gain "informed consent" as defined by the US federal policy for the protection of human subjects, which demands explanation of the purposes of the research and the expected duration of the subject's participation, a description of any reasonably foreseeable risks and a statement that participation is voluntary. "This study is a scandal because it brought Facebook's troubling practices into a realm – academia – where we still have standards of treating people with dignity and serving the common good,” he said.’

Dataveillance: Profiling

Analysis of data on (e.g.) drug use, crime, migrants, asylum-seekers, welfare fraud, consumption history, internet behaviour, credit history, education records, health, etc.

Potentially beneficial, potentially harmful, for individuals or society

Identifies or creates groups, categories, individuals

Predicts behaviour

Decisions based on profiles

False positives, false negatives

'Social sorting': discrimination, social exclusion/inclusion

Used by states/public authorities, law enforcers, businesses; researchers

Internet Research: What is it? (1)

'This document uses the following working definitions:

Internet research encompasses inquiry that:

(a) utilizes the internet to collect data or information, e.g., through online interviews, surveys, archiving, or automated means of data scraping;

(b) studies how people use and access the internet, e.g., through collecting and observing activities or participating on social network sites, listservs, web sites, blogs, games, virtual worlds, or other online environments or contexts;

(c) utilizes or engages in data processing, analysis, or storage of datasets, databanks, and/or repositories available via the [internet]

(d) studies software, code, and internet technologies

(e) examines the design or structures of systems, interfaces, pages, and elements

(f) employs visual and textual analysis, semiotic analysis, content analysis, or other methods of analysis to study the web and/or internet-facilitated images, writings, and media forms.

(g) studies large scale production, use, and regulation of the internet by governments, industries, corporations, and military forces.'

Final Copy: Ethical Decision-Making and Internet Research: Recommendations from the AOIR Ethics Committee. Approved by the Ethics Working Committee, 08/2012. Endorsed by the AOIR Executive Committee, 09/2012. Approved by the AOIR general membership, 12/2012.

Internet Research: What is it ? (2)

'The internet is a social phenomenon, a tool, and also a (field) site for research. Depending on the role the internet plays in the research project or how it is conceptualized by the researcher, different epistemological, logistical and ethical considerations will come into play. The term "Internet" originally described a network of computers that made possible the decentralized transmission of information. Now, the term serves as an umbrella for innumerable technologies, devices, capacities, uses, and social spaces. Within these technologies, many ethical and methodological issues arise and as such, internet research calls for new models of ethical evaluation and consideration. Because the types of interaction and information transmission made possible by the internet vary so widely, researchers find it necessary to define the concept more narrowly within individual studies. This is complicated by the fact that studies of and on the internet cut across all academic disciplines.'

Final Copy: Ethical Decision-Making and Internet Research: Recommendations from the AOIR Ethics Committee. Approved by the Ethics Working Committee, 08/2012. Endorsed by the AOIR Executive Committee, 09/2012. Approved by the AOIR general membership, 12/2012.

Internet Research Ethics (IRE) (1)

'*IRE* is defined as the analysis of ethical issues and application of research ethics principles as they pertain to research conducted on and in the Internet. Internet-based research, broadly defined, is research which utilizes the Internet to collect information through an online tool, such as an online survey; studies about how people use the Internet, e.g., through collecting data and/or examining activities in or on any online environments; and/or, uses of online datasets, databases, or repositories.'

Ess, Charles and the Association of Internet Researchers Ethics Working committee, 2002, "Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee," quoted in 'Internet Research Ethics', *Stanford Encyclopedia of Philosophy*, 2012

Internet Research Ethics (IRE) (2)

'The multiple disciplines already long engaged in human subjects research (medicine, sociology, anthropology, psychology, communication) have established ethical guidelines intended to assist researchers and those charged with ensuring that research on human subjects follows both legal requirements and ethical practices. But with research involving the Internet—where individuals increasingly share personal information on platforms with porous and shifting boundaries, where both the spread and aggregation of data from disparate sources is increasingly the norm, and where web-based services, and their privacy policies and terms of service statements, morph and evolve rapidly—the ethical frameworks and assumptions traditionally used by researchers and REBs are frequently challenged.'

Stanford Encyclopedia of Philosophy, 2012

Article 29 Data Protection Working Party: WP203 (Opinion 03/2013 on Purpose Limitation)

'Under the current framework [EU Data Protection Directive 95/46/EC], it is up to each Member State to specify what safeguards may be considered as appropriate. This specification is typically provided in legislation, which could be precise (e.g. national census or other official statistics) or more general (most other kinds of statistics or research). In the latter case, this leaves room for professional codes of conduct and/or further guidance released by the competent data protection authorities.'

Codes, Statements, Etc.: Mainly General

BSA (British Sociological Association) 2002

ASA (American Sociological Association) 1999/2008

BPS (British Psychological Society) 2013

PSA (Political Studies Association) n.d. (1990s)

SRA (Social Research Association) 2003

AAAS (American Association for the Advancement of Science) 2014

MRS (Market Research Society) 2014

AOIR (Association of Internet Researchers) 2002/2012

UKRIO (UK Research Integrity Office) 2009 [adopted by the University of Edinburgh]

etc.

UKRIO: Code of Practice for Research (2009)

High-level template

No mention of privacy (does mention personal data)

No mention of Internet

No mention of social media

But…

‘3.7.1 Organisations and researchers should make sure that any research involving human participants, human material or personal data complies with all legal and ethical requirements and other applicable guidelines. Appropriate care should be taken when research projects involve: vulnerable groups, such as the very old, children or those with mental illness; and covert studies or other forms of research which do not involve full disclosure to participants. The dignity, rights, safety and well-being of participants must be the primary consideration in any research study. Research should be initiated and continued only if the anticipated benefits justify the risks involved.’

UKRIO: Code of Practice for Research (2009)

‘3.7.3 Organisations and researchers should ensure the confidentiality and security of: personal data relating to human participants in research; and human material involved in research projects.’

‘3.7.10 Researchers on projects involving human subjects must satisfy themselves that participants are enabled, by the provision of adequate accurate information in an

appropriate form through suitable procedures, to give informed consent, having particular regard to the needs and capacities of vulnerable groups, such as the very old, children and those with mental illness.’

University of Edinburgh College of Humanities and Social Science Research Ethics Framework, May 2008

- High-level principles
- Mentions dignity
- Mentions consent
- 'The storage, processing and disposal of information about individuals who are research subjects must meet legal requirements, including the individual's explicit written consent to the proposed holding and use of the data. Individuals' right to access and correct information held about them should also be explained.'

  but 'explicit written consent' is not part of the UK Data Protection Act 1998, Schedule 3, even for processing 'sensitive' personal data; nor is it part of the EU General Data Protection Regulation

However…

‘But as online research takes place in a range of new venues (email, chatrooms, webpages, various forms of “instant messaging,” MUDs and MOOs, USENET newsgroups, audio/video exchanges, etc.) – researchers, research subjects, and those charged with research oversight will often encounter ethical questions and dilemmas that are not directly addressed in extant statements and guidelines. In addition, both the great variety of human inter/actions observable online and the clear need to study these inter/actions in interdisciplinary ways have thus engaged researchers and scholars in disciplines beyond those traditionally involved in human subjects research: for example, researching the multiple uses of texts and graphics images in diverse Internet venues often benefits from approaches drawn from art history, literary studies, etc. This interdisciplinary approach to research leads, however, to a central ethical difficulty: the primary assumptions and guiding metaphors and analogies - and thus the resulting ethical codes - can vary sharply from discipline to discipline, especially as we shift from the social sciences (which tend to rely on medical models and law for human subjects’ protections) to the humanities (which stress the agency and publicity of persons as artists and authors).’

Charles Ess and the AoIR ethics working committee, ‘Ethical decision-making and Internet research: Recommendations from the AoIR ethics working committee’, Approved by AoIR, November 27, 2002, www.aoir.org/reports/ethics.pdf

Therefore…

- Need to review and revise ethical and legal principles, codes and guidance for research using 'big data'/analytics; is this happening?
- Need to recognise that, especially where principles, codes and guidelines leave off, **judgement** must be exercised because conflicting rights and interests are involved; no 'tick-boxes'
- Judgement is needed about the justification of 'big data' research; its limits; its (un)intended consequences; its risks; its legality; its ethics

(How) can researchers be trained to exercise judgement of this kind?

Bibliography (1)

- Altman, I. (1975), *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Monterey, CA: Brooks/Cole Publishing Co.
- Anderson, D. (2015), *A Question of Trust: Report of the Investigatory Powers Review* [Anderson Report], London: The Stationery Office.
- Bauman, Z. (2006), *Liquid Fear*, Cambridge: Polity Press.
- Bennett, C. and Raab, C. (2006), *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge, MA: The MIT Press.
- Bygrave, L. (2002), *Data Protection Law: Approaching its Rationale, Logic and Limits,* The Hague: Kluwer Law International.
- Dworkin, R. (1977), *Taking Rights* Seriously, London: Duckworth.
- Etzioni, A. (1999), *The Limits of Privacy*, New York, NY: Basic Books.
- European Union (2016), *General Data Protection Regulation*
- Finn, R., Wright, D. and Friedewald, M. (2013), 'Seven Types of Privacy', pp. 3-32 in S. Gutwirth, R. Leenes, P. De Hert, et al. (eds.), European Data Protection: Coming of Age?, Springer.

Bibliography (2)

- Gasser, M. (1988) *Building a Secure Computer System*, Van Nostrand Reinhold
- Goffman, E. (many works)
- Goold, B. (2009), 'Surveillance and the Political Value of Privacy'. *Amsterdam Law Forum* 1(4). http://amsterdamlawforum.org.
- Intelligence and Security Committee of Parliament (2015), *Privacy and Security: A Modern and Transparent Legal Framework*, London: The Stationery Office.
- Loader, I. and Walker, N. (2007), *Civilizing Security*, Cambridge: Cambridge University Press.
- Martí Sempere, C. (2010). "The European Security Industry: A Research Agenda". Economics of Security Working Paper 29, Berlin: Economics of Security.
- Nissenbaum, H. (2010), *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.
- Raab, C. (1999),'From Balancing to Steering: New Directions for Data Protection', pp. 68-93 in C. Bennett and R. Grant (eds.), *Visions of Privacy: Policy Approaches for the Digital Age*, Toronto: University of Toronto Press.
- Raab, C. (2012), **'**Privacy, Social Values and the Public Interest', pp. 129-151 in A. Busch and J. Hofmann (eds.) 'Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], *Politische Vierteljahresschrift* Sonderheft 46, Baden-Baden: Nomos Verlagsgesellschaft.

Bibliography (3)

- Raab, C. (2014), 'Privacy as a Security Value', pp. 39-58 in D. W. Schartum, L. Bygrave and A. G. B. Bekken (eds.), *Jon Bing: En Hyllest / A Tribute*, Oslo: Gyldendal; available at: http://bigdataandprivacy.org/wpcontent/uploads/2014/08/Raab_PrivacySecurityValue.pdf
- Raab, C. (2017), 'Security, Privacy and Oversight', pp. 77-102 in Andrew Neal (ed.), *Security in a Small Nation: Scotland, Democracy, Politics*. Cambridge: Open Book Publishers.
- Regan, P. (1995*), Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill, NC: University of North Carolina Press.
  Review Group on Intelligence and Communications (2013) *Technologies, Liberty and Security in a Changing World*, Washington, DC.
- Royal United Service Institute for Defence and Security Studies (2015), *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, London: Royal United Services Institute for Defence and Security Studies.
- Schoeman, F. (1992), *Privacy and Social Freedom* Cambridge: Cambridge University Press.
- Solove, D. (2008), *Understanding Privacy*, Cambridge, MA: Harvard University Press.
- Steeves, V. (2009), 'Reclaiming the Social Value of Privacy', pp. 191-208 in I. Kerr, V. Steeves and C. Lucock (eds.), *Lessons From the Identity Trail: Privacy, Anonymity and Identity in a Networked* Society, Oxford: Oxford University Press

Bibliography (4)

- The President's Review Group on Intelligence and Communications Technologies (2013) *Liberty and Security in a Changing* World – *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, December 12, 2013 (Washington, DC).
- United Nations Development Programme (1994), *Human Development Report 1994*, New York, NY: Oxford University Press.
- Waldron, J. (2003), 'Security and Liberty: The Image of Balance', *The Journal of Political Philosophy*, vol. 11, pp. 191-210.
- Westin, A. (1967), *Privacy and Freedom*. New York, NY: Atheneum.
- Wright, D. and Raab, C. (2014), 'Privacy Principles, Risks and Harms', *International Review of Law, Computers & Technology*, Vol. 28, No. 3, pp. 277-298.
- Zedner, L. (2009), *Security,* London: Routledge.

c.d.raab@ed.ac.uk