EPSRC NEMODE network +

Designing Privacy In:
Setting the Research Agenda

Centre for Research into Information, Surveillance and Privacy

March 2015
## List of Annexes

<table>
<thead>
<tr>
<th>Annex</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Workshop Proposal - Privacy by Design: The Research Agenda</td>
<td>21</td>
</tr>
<tr>
<td>2.</td>
<td>Agenda for EPSRC NEMODE network + Workshop</td>
<td>23</td>
</tr>
<tr>
<td>3.</td>
<td>EPSRC NEMODE network + Workshop Participants</td>
<td>24</td>
</tr>
<tr>
<td>4.</td>
<td>Richard Adams NEMODE network + Workshop Presentation</td>
<td>29</td>
</tr>
<tr>
<td>5.</td>
<td>John Borking NEMODE network + Workshop Presentation</td>
<td>34</td>
</tr>
<tr>
<td>6.</td>
<td>Adriana Lukas NEMODE network + Workshop Presentation</td>
<td>45</td>
</tr>
<tr>
<td>7.</td>
<td>Vincent Toubiana NEMODE network + Workshop Presentation</td>
<td>53</td>
</tr>
<tr>
<td>8.</td>
<td>Chad Wollen NEMODE network + Workshop Presentation</td>
<td>58</td>
</tr>
<tr>
<td>9.</td>
<td>Chris Pounder NEMODE network + Workshop Presentation</td>
<td>68</td>
</tr>
<tr>
<td>10.</td>
<td>CPDP Panel Description</td>
<td>74</td>
</tr>
<tr>
<td>11.</td>
<td>CPDP CRISP Slide</td>
<td>75</td>
</tr>
<tr>
<td>12.</td>
<td>CPDP Panel Participants</td>
<td>76</td>
</tr>
<tr>
<td>13.</td>
<td>John Borking CPDP Presentation</td>
<td>78</td>
</tr>
<tr>
<td>14.</td>
<td>Jason Pridmore CPDP Presentation</td>
<td>82</td>
</tr>
<tr>
<td>15.</td>
<td>Kasey Chappelle Presentation</td>
<td>86</td>
</tr>
<tr>
<td>16.</td>
<td>Tom Ilube Presentation</td>
<td>93</td>
</tr>
</tbody>
</table>
Centre for Research into Information, Surveillance and Privacy (CRISP)

CRISP is a collaborative initiative between the University of Stirling Management School, the Open University Business School and the University of Edinburgh's School of Social and Political Science and School of Law. It is Europe's leading research and knowledge exchange centre dedicated to studying the many dimensions of the surveillance society and its consequences.

CRISP's core aim is to generate and disseminate new knowledge about ‘information, surveillance and privacy’. Specifically we aim to:

1. Provide a platform for world-class social scientific and legal research and knowledge exchange in CRISP’s subject area;
2. Provide an international focal point for existing and future research activities in this area;
3. Build on existing synergies that exist, in terms of current research projects and interests, between the partner institutions and researchers, and thereby enhance research capacities;
4. Provide a solid foundation for future grant applications and knowledge exchange activities;
5. Provide a vibrant environment for doctoral training and supervision in this subject area;
6. Provide a platform which will allow engagement with policy-makers and practitioners relevant to this subject area;
7. Engage with the public on relevant issues connected with Information processing, surveillance and privacy;
8. Enhance public awareness and understanding of the surveillance and privacy implications arising from the development of new ICTs.

CRISP Directors
Professor Kirstie Ball, Open University
Professor Charles Raab, University of Edinburgh
Professor William Webster, University of Stirling

CRISP Website, URL: http://www.open.ac.uk/researchcentres/crisp/
1. Introduction

This report presents an overview of the development of an emerging research agenda, facilitated by the Centre for Research into Information, Surveillance and Privacy (CRISP) and funded by NEMODE +. The agenda explores the theme of how privacy can be designed into organizational processes and technologies. The report is titled 'Designing Privacy In: Setting the Research Agenda'. It captures the activities initiated by CRISP in order to identify key research issues and sets out a future research agenda. The report is therefore both a record of activity and a statement of research potential.

The report provides a brief summary of two main research activities: (1) a research workshop held in London in November 2014 and including participants from academia, practice and civil society, and (2) an expert panel session of the Computers, Privacy and Data Protection (CPDP) Conference, Europe’s leading conference for data protection experts, held in Brussels in January 2015. Both activities were facilitated and delivered by CRISP. These activities have produced a number of direct outputs, including a series of presentations, engagement and discussion with practitioners, experts and civil society, and two short films. The overall outcome is a recognition and definition of an emergent research agenda around the commercial feasibility of privacy by design, relevant to both academia and practice.

From the outset, it is important to acknowledge the support given to CRISP to help facilitate the activities discussed in this report. The workshop hosted by CRISP Open University in London on 19 November 2014 was supported financially by the RCUK/EPSRC funded NEMODE (New Economic Models in the Digital economy) 'network plus’ research programme¹, and the expert panel session at the 2015 CPDP conference in Brussels was supported financially by CPDP². The CRISP Directors would also like to thank all the experts who gave up their time to participate in this intellectual endeavour.

The report has three main sections. Following the introduction, Section 2 sets out the research objectives. Section 3 presents the research activity associated with the London

¹ http://www.nemode.ac.uk
² http://www.cpdpconferences.org
workshop and Section 4 that associated with the expert CPDP panel in Brussels. Section 5 sets out a series of research outcomes, including the emergent research agenda. Following this are a number of annexes capturing information relevant to the research activities, and in particular copies of slides used during the workshop and expert panel.

2. Research Objectives

The core research objective of the research events discussed in this report was to scope out the potential for further research into the theme of privacy by design, and in particular to examine whether there were commercial opportunities inherent in privacy friendly technologies and the key organizational and institutional configurations necessary for the emergence of such technologies. Embedded within this objective is an explicit recognition that ‘designing privacy in’ is a complex process that requires input from academic, practitioner and civil society communities. With this in mind the two research events organized by CRISP included a mix of participants with a diverse range of institutional affiliations and experiences, including academics (from different disciplines), regulators, and actors from the commercial sector and civil society. The purpose here was to provide different perspectives on the emerging research agenda and to establish the validity of the research issues being explored. The key outcome has been an embryonic research agenda, setting out issues for further exploration.

It should be noted from the outset that ‘Privacy by Design’ (PbD) is a long established concept that typically promotes certain processes in order to establish privacy as a design principle, so that privacy is not an afterthought and only considered at the later stages of the design and implementation process (Koops and Leenes 2014). Articles published on the topic range from polemic Cavoukian (2012), to a plethora of ‘how to do it’ guides (Morradien 2014; Gallindo 2014), case studies (Kroener and Wright 2014) and engineering specifications (Rubinstein and Good 2013). In depth empirical evaluations are rare, although a few exist (e.g. Brown 2014). Issues associated with privacy remain undervalued in the development of new technologies. Many of these narratives place privacy concerns in opposition to business interests, as if privacy by design could not be operationalized as a win-win in business models. With this in mind, this research seeks
to explore whether privacy, however defined, could indeed offer a commercial advantage to companies offering new technological products and services, and if so, what are the institutional, organizational, regulatory and cultural requirements necessary to encourage privacy to be ‘designed in’. In this respect, the emergent research agenda places a ‘value’ on the provision of privacy protection and facilitates economic activity. Privacy protection in this perspective renders privacy as something which is not just a human right but is something which has commercial value and which contributes positively to the digital economy.

Annex 1, the ‘Workshop Proposal - Privacy by Design: The Research Agenda’ presents the initial proposal for a workshop to be hosted by CRISP and funded by NEMODE ‘network plus’. It sets out the PbD approach, the importance of ‘privacy’ as a human right and limitations to date in the application of PbD. The key aims of the workshop were:

1. “to explore how PbD could be operationalized as a commercial interest,
2. to identify the technical, organizational and market barriers to this operationalization, and
3. to scope a research agenda for understanding how these barriers may be overcome”.

A further objective, which was not explicitly stated, was to engage leading academics and practitioners in a dialogue about the proposed research agenda.

Following on from the workshop in London, the aim of the expert panel of the CPDP Conference in Brussels was to expose the emerging research agenda to a broader audience, in this case an audience of data protection experts, and to further the discussion about the commercial feasibility of designed-in privacy protection. Annex 10 presents the remit of the CPDP expert panel. The discussion during this panel session allowed us to reflect upon and refine the research agenda, as well as to test the validly of the approach.
3. The Privacy by Design Workshop

The ‘Privacy by Design: The Research Agenda’ workshop, funded by the NEMODE ‘network plus’ programme, organized by CRISP and hosted by the Open University in London, took place on 19 November 2014. The aims of the workshop were: ‘to explore how PbD could be operationalized as a commercial interest, to identify the technical, organizational and market barriers to this operationalization, to scope a research agenda for understanding how these barriers may be overcome, and to engage leading academics and practitioners in a dialogue about the proposed research agenda (Workshop aims are set out in Annex 1). Participation in the workshop was by invitation, with those invited having experience or a research interest in the topic area. The twenty workshop participants came from a range of backgrounds, including academia, public service, commercial companies and civil society. The mix of experiences and expertise was an intentional design element of the workshop as it allowed for a variety of perspectives to emerge and be considered. Annex 3 presents short biographies of the workshop participants.

The workshop was carefully structured by CRISP to facilitate discussion, group learning and the development of ideas. The workshop was split into five main sessions, each building on the previous session to develop the research agenda cumulatively. The first session considered the purpose of the workshop and the intended learning outcomes, with explicit reference to the NEMODE ‘network plus’ programme and the importance of the privacy by design subject area. The second session set out what was/is already known about privacy by design and how the concept and associated practices had evolved over time. The third session explicitly considered four critical perspectives on the privacy by design process, namely those of: (1) the technical developer, (2) the corporation, (3) the regulator and (4) the campaigner. Following on from these different perspectives, the fourth session addressed directly ‘who’ and ‘what’ was worth investigating if privacy by design was to have commercial value and be cherished within organizational and regulatory settings. Via small group work, the fifth session involved the generation of a research agenda, which was subsequently discussed in an open plenary setting. Embedded in the structure of the workshop was a range of activities designed to facilitate the transfer of knowledge, to generate discussion and to reflect
upon competing and conflicting perspectives. The workshop included six presentations, a short film courtesy of Vodafone, group work, and open discussion. The agenda for the workshop is attached at Annex 2.

Materials used during the workshop were available to participants via a dedicated Dropbox account.

A short film, entitled ‘Designing Privacy In’ was produced following the workshop. The film, based on interviews with the workshops' participants and footage from the day, depicts the workshops proceedings, and suggests some conclusions and next steps. It was produced by Professor Kirstie Ball with film production company Two Cats Can (Tony Coe and Mags Noble). Camerawork was by Andrew Rix. The film has been delivered to the NEMODE + team separately.

3. 1 Workshop Presentations

The London workshop incorporated six presentations:

**Dr Richard Adams ‘Designing Privacy In: Setting the Research Agenda’**
Dr Richard Adams, NEMODE Senior Research Fellow, University of Surrey, in his presentation set out the NEMODE ‘network plus’ research agenda and the contemporary significance of privacy in the digital economy. It included a reflection on emerging technologies and rising awareness of privacy amongst consumers and businesses. Dr Adams presentation is attached at Annex 4.

**Dr John Borking ‘Privacy by Design’ – Historical Overview**
Dr John Borking, of Borking Consultancy, a former Netherlands Data Protection Commissioner, presented an historical overview of ‘Privacy by Design’. His presentation charted the emergence of privacy as a design concept and legal attempts to regulate for privacy design, including legal specifications and privacy principles. Dr Borking’s

---

3 www.twocatscan.co.uk
presentation highlighted the formal complexity embedded in traditional PbD approaches. His presentation is attached at Annex 5.

Adriana Lukas ‘Privacy by Design? Quantified Self: A Technologist Perspective’
Adriana Lukas, a ‘Quantified Self’ activist, presented a citizen or service user view, from the perspective of a society saturated by digital technologies. Her ‘technologist perspective’ was one where individual citizens embraced digital technologies to enhance - and quantify - their lives, but at the same time considered the role and value of privacy. Adriana Lukas’ presentation is attached at Annex 6.

Dr Vincent Toubiana ‘Designing Privacy In’ – The Regulatory Vision
Dr Vincent Toubiana, from the French data protection authority CNIL (Commission Nationale de l’Informatique et des Libertés), presented a regulator’s vision of privacy by design. He set out the current requirements for privacy by design in existing national and supra-national regulation and provided examples of privacy preserving solutions, noting also that such activity has a cost attached to it. Dr Toubiana’s presentation is attached at Annex 7.

Chad Wollen ‘Designing Privacy In: Corporate Vision’
Chad Wollen, from Vodafone, presented the corporate vision of privacy by design and explained how private companies had become more aware of the importance of privacy to their customer base, as well as of the importance of demonstrating to customers how the company valued privacy. Chad Wollen’s presentation is attached at Annex 8.

Dr Chris Pounder ‘Privacy by Design’ – The Campaigner’s Vision
Dr Chris Pounder, from Amberhawk, presented the view of the campaigner, in particular giving views about how limitations in the regulation of data protection have resulted in barriers to encouraging privacy by design. In this perspective, there was very little market or regulatory incentive to implement privacy by design techniques. Dr Pounder’s presentation is attached at Annex 9.
3.2 Generating the Research Agenda: Group Discussion

During the latter stages of the workshop, small groups were asked to formulate a research agenda, taking into account the organizational, regulatory and commercial barriers and challenges. The following research agenda emerged – presented as a series of questions grouped thematically:

**Defining the value of privacy**

1. Is there evidence that businesses value privacy by design, and what is this evidence?
2. How is privacy conceived as a commercial value?
3. How does the value of privacy differ between people, organizations, industries and contexts?
4. Can social or psychological experiments be used to sensitize local communities about the value of privacy? How can common tropes about privacy and surveillance (e.g. nothing to hide/fear; security and privacy can be traded off against each other) be challenged?
5. How can anonymity be understood as a social value?
6. What are the costs to an organization of getting privacy wrong?
7. How does an organization in a supply chain negotiate the appropriate privacy levels for themselves and their business model?
8. Does privacy by design actually protect privacy? Is there evidence to demonstrate this?

**Levels of privacy by design**

1. What is the scalability of privacy by design? Can it be implemented across the whole organization or even between organizations?
2. Can existing technical means of placing users in true control of their data (i.e. collection, processing, dissemination) be made scalable and economically efficient? (this implicates system architecture, regulation, norms and punitive measures).
3. Who in the organization is tasked with privacy by design? Is a champion necessary?
4. Is it possible to have ‘levels’ or ‘grades’ of privacy by design use, from basic to advanced users?

Implementation of PbD

1. What inhibits the adoption of privacy by design by designers and companies (i.e., resources, lack of understanding, perceptions of competitive environment, etc.)
2. What different business models exist that support privacy by design?
3. To what extent can privacy by design improve business practice and corporate performance metrics?
4. How does privacy by design chime with business models, cultures and processes?
   To what extent would a company have to change to accommodate it?
5. How can privacy by design ‘best practice’ be developed, understood and disseminated?
6. How can privacy by design performance be certified, measured and monetised?
7. Can start-ups or innovation communities be developed that emphasize privacy by design and its role in the value chain?
8. To what extent can privacy by design practice be compared (a) between industrial sectors and (b) with other corporate socially responsible (CSR) practices already in train, such as environmentally responsible business practice and regulation?
9. At what stage is privacy by design in its lifecycle i.e. how mature is it as a set of ideas and how can this influence businesses’ propensity to adopt it?
10. What corporate reporting mechanisms and techniques would need to be developed for effective privacy by design practice?
11. Is there a risk that companies will market themselves as privacy ‘friendly’ when they are not, and by doing so seek financial reward from the way they position themselves in relation to privacy?

Interventions and instruments

1. What regulatory instruments and other legal measures would be appropriate to encourage privacy by design?
2. Could privacy by design be seen simply as a way of complying with data protection law?
3. What kind of innovations and incentives can be used to encourage businesses to address and adopt privacy by design?

4. Can companies be favourably incentivized or rewarded by a regulator for ‘doing’ privacy by design?

5. Can privacy by design seals be developed and adopted?

6. Would it be possible to run trials of different privacy by design interventions in different contexts?

7. What role does privacy by design play in building relationships between data controllers and data subjects?

8. How can self-audit be encouraged/how can accountability for privacy by design be engineered?

9. Are voluntary international standards possible in this area and how can they be incentivized?

10. What role can the media, pressure groups, and NGOs play in promoting and monitoring privacy by design?

**Cultural divide**

1. To what extent do cultural differences, either in national or institutional contexts, influence how privacy by design is put into practice?

2. How big is the gap between the rhetoric and the reality of privacy by design?

3. How has the role of civil society organizations changed in relation to privacy by design and what is their trajectory?

**Consumers and the general public**

1. How is privacy experienced, felt and acted upon by service users?

2. Why and how do consumers care about privacy?

3. Do we know what consumers require in terms of their privacy protection and how can this be discovered?

4. How can existing privacy by design research be used to educate the general public about privacy, their rights, and their data management?

5. How can the public understanding of privacy and privacy rights be improved?
**Trust building**

1. Are companies’ reputations really at stake if they do not adopt privacy by design?
2. What are the trust issues in the value/supply chain around privacy by design?
3. How and where are the relevant privacy boundaries and how can they be mutually respected?
4. What part can privacy by design play in building relationships between data controllers and the public?

**Design**

1. What is meant by ‘design’ in ‘privacy by design’?
2. Can privacy by design be easily retrofitted to information infrastructures? What are the difficulties of doing this?
3. What would a privacy friendly internet look like?

**4. CPDP Expert Panel**

The ‘Commercial opportunities for designing privacy in: embedding privacy in organizational practices’ expert panel at the Computers, Privacy and Data Protection (CPDP) conference, organized by CRISP, took place on 21 January 2015 in Brussels. The aim of this session was to expose the emerging research agenda to a broader audience, in this case an audience of international data protection experts, and to further the discussion about the commercial feasibility of privacy protection. Annex 10 presents the remit of the CPDP expert panel.

The panel included six speakers: a chair, a moderator and four presenters. All participants are listed in Annex 11 The panel was structured so that each presentation offered a different perspective on the main topic, including: the regulatory perspective, a corporate perspective, a designer’s perspective, and a perspective about investment in privacy. As with the workshop, the intention was to explore competing and conflicting visions, with a view to facilitating engagement and discussion. Short biographies of the panel presenters are attached at Annex 12.
An audience of approximately 40 conference delegates attended the session. A video recording on the expert panel can be found at, URL: https://www.youtube.com/watch?v=sgHa4QydNlo

4.1 The CPDP Expert Panel Presentations

The CPDP expert panel incorporated four short presentations:

*Dr John Borking ‘Historical Perspective of Privacy-by-Design and Economic Considerations’*

Dr John Borking, of the Borking Consultancy, and former Netherlands Data Protection Commissioner, presented a historical overview of privacy by design and a reflection on a number of economic issues. His presentation sets out the origins of the concept and how it has evolved and been implemented over time. Dr Borking’s presentation considered specifically whether there was a ‘business case’ for privacy by design. A copy of his presentation can be found at Annex 13.

*Dr Jason Pridmore ‘Commercializing Privacy by Design: Potential problems in Configuring Privacy’*

Dr Jason Pridmore, Erasmus University Rotterdam, presented a range of potential problems that might arise when trying to configure privacy into the design process. Dr Pridmore emphasized the importance of privacy’s being a value embedded in organizational life prior to and encompassing the development of new goods and services. In this respect, most privacy by design processes were an afterthought and most organizations did not intrinsically value privacy. Dr Pridmore’s presentation is attached at Annex 14.

*Kasey Chappelle ‘Privacy by Design: Embedding Privacy in Organisational Practices’*

Kasey Chappelle, Global Privacy Counsel at Vodafone, presented a range of products and services that Vodafone were developing to give users more control over privacy settings and ‘their’ data. These examples demonstrated that Vodafone saw commercial value in presenting themselves as a privacy friendly company. Kasey Chappelle’s presentation is attached at Annex 15.
**Tom Ilube ‘Pitching Privacy’**

Tom Ilube, of Crossword Cybersecurity, delivered a presentation explaining how difficult it was to gain investment for privacy friendly technologies and services. He explained how he ‘pitched’ such ventures and how there was a reluctance to invest in the area. Tom Ilube's presentation is attached at Annex 16.

**4.2 CPDP Expert Panel Discussion: New Items for the Research Agenda**

In addition to the research agenda generated in the November workshop, the presentations and discussion in Brussels highlighted additional issues that were not covered:

**Design**

1. How can privacy ontologies be built so that the machines could understand things like consent etc?
2. How can ‘ready to wear’ PbD be built, rather than it being custom made for every system?
3. When do organizations start to bother about privacy?

**Implementation**

1. What factors affect an organization’s decision to adopt PbD?
2. How do we calculate an ROI for PbD investment – how do we account for privacy in accounting methodologies?

**Business models**

1. What kinds of privacy friendly products and services startups attract high level capital investment?
2. What is the PbD requirements innovation diffusion model? Do we start at the margins for those very vulnerable populations and work inwards (much like surveillance diffusion) or does something else happen?
3. What alternative funding models are available for the development of privacy innovations?
Organizational values

1. How are an organization’s staff inculcated with privacy values?
2. How can privacy be promoted as part of an organizational culture?

Trust

1. How can consumer trust be maintained in the context of organizational data use?
2. How can organizations become more transparent in their use of customer data?

5. Research Outcomes and Next Steps

As described above, the ‘Designing privacy in: setting the research agenda’ process has delivered a number of research outputs:

1. A high level workshop with experts from a range of academic, practitioner and civil society backgrounds,
2. A dedicated expert panel session of Europe’s leading conference for data protection practitioners,
3. A series of presentations (attached) on privacy by design and the commercial feasibility of privacy protection,
4. A short film about the emerging research agenda around privacy by design (plus a video of the CPDP conference panel), and
5. Constructive engagement with a range of experts.

It is clear from the research process to date that the commercial value of privacy is undertheorised and that there is a lack of empirical evidence about how organizations go about positioning themselves in relation to privacy and/or developing privacy friendly technologies. It is also clear that privacy, as a human value to be embedded in technological development, is growing in importance and is likely, in the near future, to be both a feature of modern technology and a driver of the digital economy. In this respect, the research process suggested that we were on the brink of a new era, an era in which digital privacy was ever more important (however delivered and realized) and
ultimately critical to organizational success. This point raises the critical question for the emergent research agenda: how do we get from where we are to this new era? Or, in other words, what are the environmental conditions necessary for businesses to design privacy in and what business models are likely to be successful?

5.1 Designing Privacy In: The Research Agenda

The work we have undertaken suggests that there are three pillars to this research agenda which relate to the Antecedents, Interventions and Outcomes of Designing Privacy In (DPI). Antecedents refers to how one might examine the contexts from which DPI arises. Interventions examines the practices which promote DPI and outcomes refers to its identifiable effects.

**Antecedents**

The research agenda would concern:

1. The mapping and exploration of differing privacy values between people, organizations, supply chains, industries and other contexts
2. How privacy operates as a commercial value
3. How common tropes about privacy can be challenged
4. How the different barriers to adoption of DPI and the diffusion of DPI driven innovations could be understood
5. Whether anything can be learned from previously introduced, now widely diffused ethically driven business practices

**Interventions**

The research agenda would examine:

1. The point at which the ‘design’ in DPI takes place. A key question concerns whether DPI could be retrofitted to existing infrastructures, could be bought ‘off the peg’ or be automated
2. The factors which drive an organization to adopt DPI: is there a DPI threshold?
3. The monetization and business improvements associated with DPI
4. How DPI can be made scalable and conducted at different intensities/degrees of sophistication
5. The necessity of a DPI champion in organizations and the promotion of a DPI culture amongst staff
6. The difference between the rhetoric and reality of DPI
7. How DPI can be incentivized, who can incentivize it and how (this may include regulators, shareholders, venture capital funders, alternative funding sources e.g. crowdfunding)
8. The impact of DPI on supply chain partners
9. Whether anything can be learned by comparing similar DPI interventions in different contexts
10. How extra-organizational actors, such as NGOs, the media, regulators and other civil society organizations can exert pressure for DPI to be implemented.

**Outcomes**

The research agenda serves to discover:

1. Whether profitable, privacy friendly business models are possible
2. The ways in which the impact of DPI on user privacy could be measured
3. Whether suitable measures of organizational performance which reflect DPI interventions exist
4. Whether DPI can be accounted for as an intangible asset to organizations, whether it is significant as such and whether it can be measured
5. Whether suitable forms of international standards can be developed for DPI
6. Whether a wider understanding of DPI ‘best practice’ can be pursued and established
7. How consumer involvement, trust and transparency around DPI can be promoted
8. How best to educate the general public about DPI

**5.2 Next Steps**

Based on the work we have undertaken and coupled with the growth in the digital data economy we can see considerable scope for the concept of privacy by design. This scope extends not only to business practices but also to privacy by design as a feature of future research funding calls. These calls would emphasise not only the need for in depth comparative research on the possibilities and practices of privacy by design, but also on
its antecedents and outcomes. CRISP is well placed to produce such research and looks forward to future opportunities in this area.

6. References


Annex 1. Workshop Proposal - Privacy by Design: The Research Agenda

Privacy by Design: The Research Agenda
A workshop proposal for NEMODE Network +
Hosted by the Centre for Research into Information, Surveillance and Privacy (CRISP) at the Open University

‘Privacy by design’ (PbD) is an approach to the protection of information privacy that encourages those who design and build information technologies and systems to incorporate privacy principles throughout the whole of the technology design and use lifecycle. PbD rests on the idea that privacy is an important human right and value that must be preserved, cherished and protected. Privacy is a benefit that accrues to society as a collectivity as well as to the individuals who constitute that society. It can thus be protected in a collective way as well as at the individual level. Protection is typically provided by law, incorporating several principles that are usually embodied in national data protection laws and regulatory codes of practice, as well as in measures that aim to raise public awareness of potential incursions and of their rights (Bennett and Raab, 2006). Technological ‘solutions’ have also been sought through ‘privacy-enhancing technologies’ (PETs), which are a precursor of PbD. Dr. Ann Cavoukian, the Ontario Privacy Commissioner, was instrumental in developing the idea of PETs, and has more recently been a vigorous promoter of PbD.

Advocates of PbD are keen to point out its implications. It has been formulated to combat an all-too-familiar approach that adds privacy features to technology once it has been designed and implemented, rather than earlier in the process. PbD views all-encompassing and maximal privacy protections as a ‘win-win’ situation that promotes both ethical business practices and protections for the user against abuses of their data. It implicates not only technologies and the information they generate but also the information infrastructures and business processes that surround them. PbD has the potential not only to increase consumer awareness of the privacy implications of the technology they purchase and use. It also has the potential to enable businesses to obtain competitive advantage and distinctiveness within the marketplace based on the privacy-protective stance they adopt. In a commercial world where data analytics are being promoted as the key to competitive advantage and customer insight, and with rising consumer awareness of these practices, it is thought that a strong ethical stance on consumer privacy will become another aspect of more enlightened and responsible approaches to doing business. Particularly in the wake of the NSA Prism episode, privacy friendly products and brand values espousing privacy have the potential to offer significant competitive advantage.

The temptation, however, is for businesses to agree with the rhetoric of PbD but not to implement it. Even though it is expected to be embedded within the proposed European Data Protection Regulation, its adoption at Member State level is still not guaranteed. Furthermore, there may be significant barriers to its adoption in numerous instances. For example, in the ubiquitous computing environment of smartphones, large multinational phone service providers and companies that design devices and their operating systems may well work to European level data protection standards. However, application developers are located all over the world and are not necessarily subject to the same level of data protection laws or individual scrutiny of their compliance with whatever laws apply to them.

A significant interstitial space now exists where PbD is the topic of commercial hyperbole, significant regulatory rhetoric, and regulatory change in a market environment in which its future will be arbitrated. PbD is at an important phase in its history, and identifying a reflexive, practice-oriented and

---

4 The OECD’s privacy principles can be found here: http://oecdprivacy.org/ the European Data protection principles can be found here, which are the foundation of data protections laws throughout Europe: http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/74; (accessed 4th July 2013);

5 http://www.privacybydesign.ca/ (accessed 4th July 2013)


theory-aware research agenda is now critical. This proposed one-day workshop will bring together leading representatives from the commercial, regulatory, activist and academic sectors to identify the extent of current knowledge and what remains to be known about this phenomenon. It has a number of aims:

- To explore how PbD could be operationalised as a commercial interest
- To identify the technical, organisational and market barriers to this operationalisation
- To scope a research agenda for understanding how these barriers may be overcome

The workshop will begin with a summary of what is known about PbD with examples of best practice. Discussions will then form around a video vignette of the PbD challenges faced in the smartphone sector. The vignette highlights different stakeholders within the smartphone ecosystem and their varying privacy interests. Using the expertise of workshop participants, discussions will focus on how PbD could be a feature of each of these stakeholders’ activities and the commercial advantages that could be gained. From this discussion a series of generalisable research questions will be formed covering the technical, organisational and market-related aspects of the problem. The workshop will deliver a report which will outline the research agenda for PbD. A short film which documents the day will accompany the report. The film will comprise a dissemination tool for use in future Nemode Network+ meetings and events, as well as providing evidence of impact.

The workshop will take place towards the beginning of 2014 at the Open University in Milton Keynes. Participants will be accommodated in the MK Hilton, which is close to the OU campus. Up to 20 participants will be invited, not including the organizers. The invitees, many of whom are in the existing network of CRISP, will be as follows:

Costs
Costs are estimated as follows:
Note: Costing redacted in this version.

Invitees and timing
The workshop will take place towards the beginning of 2014 at the Open University in Milton Keynes. Attendees will be accommodated in the MK Hilton, which is close to the OU campus. Up to 20 participants will be invited, not including the organizers. The invitees, many of whom are in the existing network of CRISP, will be as follows:

Note: List of potential participants redacted in this version.

Reference

---

9 http://www.vodafone.com/content/index/about/about_us/privacy/privacy_by_design.html accessed 4th July 2013
Annex 2. Agenda for EPSRC NEMODE network + Workshop

Designing Privacy In: Setting the Research Agenda
A workshop for EPSRC NEMODE network +

Hosted by the Centre for Research into Information, Surveillance and Privacy
The Open University in London, 1 – 11 Hawley Crescent, Camden Town,
London, NW1 8NP
Wednesday 19th November 2014

9.30 Registration and coffee
9.50 Introduction and aims: The NEMODE network + view.
CRISP directors and Dr Richard Adams, University of Exeter Business School.
NEMODE network + chair.

10.15 An overview of the topic. John Borking, Borking Consultancy
10.45 Coffee

11.15 What is best practice ‘Privacy by design’? Some visions:
11.15 – 11.35 Adriana Lukas, London Quantified Self Group - The tech developer vision
11.35 – 11.55 Vincent Toubiana, Commission Nationale de l’Informatique et des Libertés (CNIL), France - The regulatory vision
11.55 – 12.15 Kasey Chappelle, Vodafone – The corporate vision.
12.15 – 12.35 Chris Pounder, Amberhawk - The campaigner’s vision

12.45 Lunch and networking

1.30 Scoping the PbD problem: Who or what is worth investigating?
Stimulus material: Vodafone. short film ‘Privacy by design across the mobile phone ecosystem’
Activity: in SMALL GROUPS, discuss who or what is worth investigating in the privacy by design ecosystem? What problem areas are there? At what level of analysis and in what academic disciplinary areas do these problems occur?

2.45 Short break

3.00 Generating the research agenda.
3.00 – 3.30 in SMALL groups, form a list of discussion questions. using post-its
3.30 – 4.00 in PLENARY, group the post-its into areas of interest to generate the research agenda.

4.00 – 4.30 Summary and close.
Annex 3. EPSRC NEMODE network + Workshop Participants

**Designing Privacy In: Setting the Research Agenda**

**Participants and Biographies**

**Dr Richard Adams, University of Surrey.**
Dr Richard Adams is Senior Research Fellow on the NEMODE project. NEMODE is an RCUK-funded ‘Network-Plus’ connecting top-level research with trail-blazing digital technology firms. The project brings together the brightest and most innovative minds to inform academic research and public policy, to give support to innovative businesses in digital technologies.

**Professor Atta Badii, University of Reading**
Atta holds the Chair of Secure Pervasive Technologies at UoR. He has established several research groups and two successful multi-disciplinary research centres and currently he is the director of Intelligent Systems Research Laboratory at UoR; this has led several inter-disciplinary collaborative research programmes. Atta holds the designation of Distinguished Professor of Systems Engineering and Digital Innovation (UCC) and is an International Privacy-by-Design Ambassador as designated by the Canadian Information and Privacy Commission. He is also the Director of the European Virtual Centre of Excellence for Ethically-guided and Privacy-Preserving Video-Analytics (VideoSense), and the Coordinator of the European Observatory for Crowd-Sourcing (SciCafe2.0). The Observatory supports participative social engagement, citizens’ science and knowledge communities based on an eco-system of socio-ethically reflective and privacy-dignity respecting co-design to support socially responsive and accountable innovation and Open Transformative Government.

**Professor Kirstie Ball, The Open University**
Kirstie Ball is Professor of Organization at the Open University Business School. She is also director of the Centre for Research into Information, Surveillance and Privacy (CRISP) and Surveillance Studies Network (SSN). She has held grants from the EPSRC, ESRC, EU Framework 7, SSHRC and the Leverhulme Trust. She publishes her work in a wide range of scholarly formats: from books, edited collections, journal articles to consultancy reports, magazines and films. Her new book ‘The Private Security State?’ is out next year with Copenhagen Business School Press. Kirstie’s research interests focus on surveillance in and around organizations, and surveillance in society at large. In particular she is interested in subjectivity and the experience of surveillance, employee surveillance, consumer surveillance and the blurring of public and private boundaries in government surveillance regimes. She has a theoretical interest in surveillance drawing on organization theory, the sociology of the body, science and technology studies and new media theory.

**Dr John Borking, Borking Consultancy**
Dr. J (John) J. F.M Borking, married, (1945), Director/owner of Borking Consultancy in Wassenaar, Netherlands, Of Counsel and external advisor on Privacy-by-Design issues for the law firm CMS Derks Star Busmann, is the former Privacy Commissioner and Board Member of the Dutch Data Protection Authority (CBP) in The Hague. He is e-Law researcher at the University of Leyden and he is a lecturer
on PETs at TopTech (Delft University). He is a certified privacy law expert for EuroPrise in Bonn (Germany) and member of the advisory board. He is chairman of the Dutch Complaints and Disputes Committee e-Recognition (e-Authentication) in The Hague. Dr. Borking holds a PhD from Leiden University.

**Mr Dave Birch, Consult Hyperion**

Dave Birch is a Director of Consult Hyperion, the IT consultancy that specialises in secure electronic transactions. He is an internationally-recognised thought leader in digital identity and digital money, named one of Wired magazine’s global top 15 favourite sources of business information, in the European “Power 50” for digital financial services, a NextBank “Fintech Titan” and ranked Europe’s most influential commentator on the emerging payments field. His latest book “Identity is the New Money” was published in April 2014.

**Mr Ray Corrigan, The Open University**

Ray Corrigan is a Senior Lecturer in Maths Computing Technology at The Open University. Ray blogs random thoughts on law, the Internet and society at B2fxxx, is a signatory of the Necessary and Proportionate International Principles on the Application of Human Rights to Communications Surveillance and has advised the European Commission and UK government on digital rights. Author of 'Digital Decision Making: Back to the Future', published by Springer-Verlag in 2007, he also wrote the OU’s 'Law, the Internet and Society: Technology and the Future of Ideas' course, now available openly on OpenLearn, as well as a variety of other materials on the environment and information and communications technologies.

**Mrs Sara Degli Esposti, The Open University**

Sara Degli Esposti is Research Assistant for the Surprise project at the Centre for Research into Information Surveillance and Privacy (CRISP) at the Open University (UK). She is also a PhD candidate at the Open University where she has investigated organisational information security strategies and compliance with EU data protection principles in the era of big data (www.bigdataprotection.co.uk). Sara is Privacy-by-Design Ambassador and an active member of the International Association of Privacy Professionals (IAPP). She has a BSc in Sociology and a MSc in Business Economics and Quantitative Methods.

**Ms Gemma Farmer, Information Commissioner’s Office**

Gemma has worked at the ICO for six years. Her current responsibilities include managing the ICO’s privacy seals project; producing and reviewing guidance and codes of practice; leading research projects; contributing to Article 29 Working Party subgroups and to the ICO’s work on the European Commission’s proposals for a new data protection Regulation. Prior to the ICO, Gemma worked at the Department for Communities and Local Government on policy areas including local government restructuring and community cohesion and integration; and as a research assistant on projects focused on marginalised communities, drug and alcohol use by young people and health service provision in deprived areas.

**Dr Mark Hartswood, University of Edinburgh**

Mark Hartswood is Research Fellow at the Institute for Language, Cognition and Computation at the University of Edinburgh. His research interests are computer supported cooperative work (CSCW), workplace studies, participatory design and professional vision. Longitudinal design for the co-realisation of work affording systems, particularly in medical settings.

**Mr Tom Ilube, Crossword Cybersecurity Plc.**

Tom Ilube is CEO of Crossword Cybersecurity plc, a technology transfer company focused on the cyber security sector. He was previously Managing Director of Callcredit Consumer Markets, the UK credit reference agency. As part of Callcredit, he launched a major new consumer initiative,
Noddle.co.uk. Previously, Tom was CEO of Garlik, the online identity protection company acquired by Experian. He was Chief Information Officer of Egg plc, the UK’s most innovative online bank. Tom served the ITU, the Geneva-based UN agency, on the High Level Expert Group on Cybercrime and as Chairman of the UK Technology Strategy Board’s Network Security Innovation Platform. Tom has been a regular media commentator and conference speaker on identity theft and cybersecurity issues.

Professor Gerd Kortuem, The Open University
Gerd Kortuem is Professor of Computing at the Open University where he heads the Ubiquitous Computing and Sustainability Lab. His research focuses on the design of computing systems for addressing sustainability challenges - related for example to energy, transportation and local communities. In terms of technology his main interest is ubiquitous computing and the Internet of Things. However, his approach is human-centric and thus to a large extent technology agnostic. Prior to joining the Open University he was a Senior Lecturer at Lancaster University’s School of Computing and Communications where he directed the MSc in E-Business and Innovation. He holds a PhD in Computer Science from the University of Oregon, USA. While doing his Ph.D. he ran the engineering efforts of web startup LivingNetworks.com (now defunct), worked as software engineer at Apple in Cupertino and developed 3D architectural software at Artifice.

Ms Adriana Lukas, London Quantified Self Group
Adriana Lukas is the founder and organiser of the London Quantified Self group, an informal community that brings together individuals using tools and methods of self-tracking to gain more knowledge about themselves. The Quantified Self movement started in the Bay area in 2008 and has been growing steadily across the world. Previously Adriana worked with companies in Europe and the United States in communication and integration of technology in the enterprise, focusing on increasing individual employees capabilities and autonomy as the foundation of collaboration and creativity. Adriana has been involved in the online development and the user-centric web since 2001, evangelised social media to the UK before disowning it around 2007, moving onto privacy and personal data related projects. She is interested in technologies that empower the individual and Quantified Self seemed to fit the bill.

Mr Kishor Mistry, Surveillance Camera Commissioner’s Office
Kishor Mistry is Head of Policy and Support for the Surveillance Camera Commissioner (SCC). The SCC is a statutory role created by the Protection of Freedoms Act 2012. The role is to encourage, review and advise on the Surveillance Camera Code of Practice as issued by the Home Office. Kishor is a civil servant and has worked in a variety of roles across a number of departments. Most recently he took a sabbatical as the CEO of a charity. In his own time, he chairs the governing body of a local secondary school.

Professor Bashar Nuseibeh, The Open University
Bashar Nuseibeh is Professor of Computing at The Open University (Director of Research, 2002-2008). Previously, he was a Professor of Software Engineering and Chief Scientist at Lero – the Irish Software Engineering Research Centre (2009-2012). He was also an academic member of staff (Reader) in the Department of Computing at Imperial College London and Head of its Software Engineering Laboratory (1990-2001). He continues his association with Imperial College as a Visiting Professor, and maintain strong research links with the Distributed Software Engineering Group. He is also a Visiting Professor at the National Institute of Informatics, Japan. He is currently holder of a Royal Society-Wolfson Merit Award (2013-2018) and a European Research Council (ERC) Advanced Grant on Adaptive Security and Privacy (2012-2017), and serves as Editor-in-Chief of the IEEE Transaction on Software Engineering (2010–). Previously, he held a Senior Research Fellowship from The Royal Academy of Engineering and The Leverhulme Trust (2005-2007) and served as Editor-in-Chief of the Automated Software Engineering Journal (1995-2008).
Ms Fola Ogunsola, Consult Hyperion
Fola Ogunsola works as a Consultant at Consult Hyperion where she specialises in contactless payments using smartcards and mobile devices. She obtained her M.Sc. in Information Security from Royal Holloway, University of London. Her experience cuts across information security, access control, data protection, identity management, payment systems, and the design and deployment of multi-function smartcard solutions. She currently supports a major payment scheme, and other clients, in their ongoing provision of secure retail payments. Her daily work experience and the growing debate on cyber security issues have increased her interest in the fields of privacy and data protection.

Dr Chris Pounder, Amberhawk Training Limited
Dr. Chris Pounder is been a Director in Amberhawk Training Limited since the company was founded in 2008. The company specialises in training staff who are responsible for data protection, Freedom of Information, information security and other aspects of Information Law. Most of Amberhawk’s delegates use the company to obtain the BCS/ISEB qualification in these fields. As well as being involved in consultancy and training work, Chris also writes the “Hawktalk” blog which covers topical privacy related subjects. In 2012, Chris was appointed to two Government Advisory Committees. He is a member of the Identity Assurance, Privacy and Consumer Advisory Group (advising the Cabinet Office on “privacy friendly” use of identity assurance techniques) and the Data Protection Advisory Panel (advising the Ministry of Justice on its approach to the EU’s Data Protection Regulation and Directive in the field of law enforcement). Chris’s career in data protection dates back to 1978 and is well documented (e.g. on Google). He has spoken at numerous conferences on data protection and related matters and also writes the occasional freelance article for the IT-related Press and the academic journals in the field of security and data protection. He has also given oral and written evidence before various Parliamentary Select Committees where issues of privacy, data protection and security have arisen (e.g. ID Cards, Surveillance, Computer Misuse Act, data retention policies, supervision of the national security agencies). Prior to Amberhawk, Chris joined Masons Solicitors in July 1999 as part of its growing Data Protection and Privacy Team; Masons merged with Pinsents to form PinsentMasons in 2006. He is mentioned by name in Chambers 500, where the latter recognised PinsentMasons‘ Data Protection team as being in the “First Tier”. Prior to that, Chris held the Data Protection Officer post at Cap Gemini and the Greater London Council where he advised MPs on the Data Protection Act 1984. Chris’s Ph. D. is in computational quantum chemistry. This required Chris to programme computers in a number of languages as well as dealing with complex mathematical and technical issues at the supervisor/assembler level.

Professor Charles Raab, University of Edinburgh
In 2012, Charles Raab resumed his Chair as Professor of Government, at the University of Edinburgh, which he had held from 1999 to 2007 before retiring as Professor Emeritus and Honorary Professorial Fellow. He has held visiting positions in the Oxford Internet Institute, the Tilburg Institute for Law, Technology, and Society (Tilburg University, The Netherlands), Queen’s University, Kingston, Ontario, and the Victoria University of Wellington (NZ). He was a Fellow at the Hanse-Wissenschaftskolleg (Institute for Advanced Study) in Delmenhorst, Germany. With colleagues at the University of Stirling and the Open University, he is a Director of CRISP (Centre for Research into Information, Surveillance and Privacy. His main general research interests are in public policy, governance and regulation, and more specifically in information policy (privacy protection and public access to information; surveillance and security; identity and anonymity; information technology and systems in democratic politics, government and commerce; and human rights implications of information processes). His research has been funded by the ESRC, the Nuffield Foundation, the National Science Foundation (USA), the European Commission (including 6th and 7th Framework Programmes), and the former Scottish Office. He participates in the Research Groups on Policy and Governance and on International Relations, and is co-convener (with Andrew Neal and Juliet Kaarbo) of the ESRC seminar
series, *Security in Scotland, with or without constitutional change*. He has engaged in advisory and consultancy work for UK and Scottish government departments, the Office of the Information Commissioner, the European Commission, the New Zealand Law Commission, Liberty, the Equality and Human Rights Commission, and the Netherlands Organisation for Scientific Research (NWO), among others. He was the Specialist Adviser to the House of Lords Select Committee on the Constitution for their inquiry, resulting in *Surveillance: Citizens and the State, 2nd Report, Session 2008-09*, HL Paper 18 and HL Paper 114. He is a member of the editorial or advisory boards of nine journals in the fields of information policy and public policy, and on the advisory boards of several research projects. He is a member of the Surveillance Studies Network, participates in the Canadian-funded project on ‘The New Transparency: Surveillance and Social Sorting’, and served on the Management Board of the European Union’s COST Action on ‘Living in Surveillance Societies’ (LiSS). He has given written and oral evidence to Parliamentary Select Committees.

**Dr Vincent Toubiana, Centre Nationale d’Information et des Libertés, France.**

Vincent Toubiana is an IT Expert at CNIL (the French DPA) where his work focuses on the implementation of EU’s cookie guidance, privacy issues related to the “Internet of Things”, and anonymization techniques. He formerly worked as a researcher at Alcatel-Lucent Bell-Labs and New-York University (NYU) where he developed and maintained several browser extensions like “TrackMeNot” and “Context-Aware-DNT” in collaboration with Helen Nissenbaum. He obtained his Ph.D. in computer networks at Telecom ParisTech (French National School of Telecommunications) in 2008.

**Professor William Webster, University of Stirling**

William Webster is Professor of Public Policy and Management at the University of Stirling. He is a Director of the Centre for Research into Information, Surveillance and Privacy (CRISP) and chair of the Department of Management, Work and Organisation, at the University of Stirling. William also led the 4 year multidisciplinary pan-European Living in Surveillance Societies (LiSS) COST Action. His research interests include; everyday surveillance practices, the governance and regulation of surveillance, and governing in the information age. He is a recognised expert on the policy processes, practices and governance of Closed Circuit Television (CCTV) in public places.

**Professor David Wilson, The Open University**

David Wilson is Professor of Organization Theory at the Open University. He was previously at the University of Warwick. He is the author of ten books and over eighty scholarly articles. He was Chairman of the British Academy of Management (1994 – 1997) where he served for over ten years as an Executive member. He is a Fellow of the Academy, elected in 1994. He was also elected as a Fellow of the Academy of the Social Sciences in 2009. He was the elected President of the scholarly society, the European Group for Organization Studies (EGOS) for 3 years (2000-2003) and has been re-elected a Board member on three consecutive occasions (current term of office runs to July 2015). He has had a long association with the scholarly journal *Organization Studies*, beginning as Editorial Assistant (1981-1992), becoming Co-Editor (1992-1996), Deputy Editor (1996-1999) and finally Editor-in-Chief (1999–2003). He has been a member of EGOS for over twenty years. At Warwick Business School he undertook many senior roles including Academic Director of the MBA (Full-Time and Distance Learning), Head of the Strategic Management Subject Group, Deputy Dean of the School (2007 -2009) and Acting Dean (2009 -2010). He was appointed Head of Department, Sociology, Warwick University (2011-2013). His research interests include strategic decision making and performance; comparative studies of public/private/non-profit organizations; he conducted one of the first studies of voluntary labour in non-profit organizations in the UK; how organizations deal with extreme uncertainties and critical approaches to the commodification of management and scholarship.
Designing Privacy In: Setting the Research Agenda

Dr Richard Adams
NEMODE Senior Research Fellow

The good news

Source: https://futurecities.catapult.org.uk/ (10/11/2014)
Old fears refreshed

Every silver lining has a cloud

But, we are complicit and compliant

When do we share your information with others?...When we are fulfilling our mission of being open

Wednesday 29 November, 2014

Source: https://www.aclu.org/ordering-pizza (10/11/2014 with permission)

Wednesday 29 November, 2014
Growing concern about privacy and data security

Source: www.gigya.com (10/11/2014)

NEMODE: an enabler of research in the Digital Economy

Funding available for
• Open call (£3k)
• Workshops (£10k)
• International speakers (T&S)
• Placements and secondment (£12k)
• Start-up support (£20k)
• Pilot studies (£50k)

Business models, data and privacy

**Business model 1: Data supported products and services**
- Servitisation
- Informatised products
- Industrial and domestic


**Business model 2: Monetising customer data**
- Advertise
- Sell
- Aggregate

**Business model 3: User data as the user’s data**
- Privacy as a differentiator

**Please tick appropriate box:**
- I will pay with cash
- I will pay with my data

Ello: Simple, beautiful & ad-free
[http://ello.co/manifesto](http://ello.co/manifesto)

Wednesday 19 November, 2014
Annex 5. John Borking EPSRC NEMODE network + Workshop Presentation

AN OVERVIEW OF PRIVACY-BY-DESIGN

Dr. John J. Borking

THAT' S ME PERSONAL DATA ≠ I AM PERSONAL DATA

Dr. John J. Borking * 1945 - Dutchman
Former Privacy Commissioner & Board Member
Data Protection Dutch Authority
Former Board member Dutch Gaming &
Lotteries Authority
Former Senior Counsel Europe Xerox Corp.
Participating in EU, CEN, Dutch and Norwegian
research projects on privacy protection/PbD
Researcher e-Law University of Leiden
ICT Arbiter/ Mediator SGOA
Expert member Advisory Board EuroPrise

MENU

• What is Privacy-by-Design (PbD)?
• The data protection law as a list of design
  specifications for PbD
• PbD: Haute Couture Or Ready to Wear?
• What If Encryption Isn’t An Option?
• Privacy Management Systems
• Conclusions
WHAT IS PRIVACY BY DESIGN?

- Article 23 of the GDPR (EP12 March 2014) requires “data protection by design” and “data protection by default”
- DPbD is a new Privacy Principle (Whereas #61 GDPR)
- DPbD is applauded as a core innovation of reform (Albrecht Report 2012/011 (COD) (However: Whereas # 46 - 95/46/EC)
- The word: ‘by’ implies that data protection purposely has to be realized by design. Article 23 makes it mandatory. (prerequisite for public procurement tenders)
- Shift within EC from Privacy by Design (2007) to Data Protection by Design (2012)

LEGAL OBLIGATIONS PbD

The Controller / Processor shall:
- Implement appropriate and proportionate technical and organizational measures and procedures ensuring
  1. the processing will meet the requirements of the GDPR
  2. the protection of the rights of the data subject
- Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion
- The results of a Data Protection Impact Assessment is leading for PbD
- Focus on: 1. the state of the art, 2. current technical knowledge, 3. international best practices and 4. the risks
PRIVACY BY DESIGN:
TECHNOLOGY + ORGANIZATION + ENVIRONMENT

INFORMATION TECHNOLOGY:
- PRIVACY SUPPORTING ARCHITECTURES
  - PRIVACY ENHANCING TECHNOLOGIES

ORGANIZATION:
- MANAGEMENT SUPPORT FOR PRIVACY
  - PRIVACY SUPPORTING BUSINESSES & PROCESSES & DPIAs

PHYSICAL ENVIRONMENT:
- PRIVACY SUPPORTING ORGANIZATION OF PHYSICAL SPACES

FEED BACK ON EXPERIENCE OF PRIVACY.
ESSENTIAL FOR PRIVACY, TRUST AND ADOPTION


LEGAL SPECs FOR DESIGNING PbD

- PRINCIPLES CONCERNING THE FUNDAMENTAL DESIGN OF APPLICATIONS
- PRINCIPLES CONCERNING THE LAWFULNESS OF PROCESSING
- PRINCIPLES CONCERNING THE RIGHTS OF THE DATA SUBJECT
- PRINCIPLES CONCERNING PROCESSING BY A PROCESSOR
- PRINCIPLES CONCERNING DATA TRAFFIC WITH THIRD COUNTRIES

HOW TO BUILD SOFT LEGAL NORMS INTO OBJECT CODE?

How far can we go in minimizing the need for the identity of a person?
Two key central research questions:

- What conditions must be kept in mind when engineering an information system in order to guarantee that the system be used effectively and efficiently without revealing the user’s identity?
- What types of architecture & information and communication technologies can contribute towards achieving this goal?

Privacy-Enhancing Technologies (PETs) The Path To Anonymity (1995)
**PETs: 2 Design Principles:**

- **Identity Protector**
  - Sheltering the user's identity (opacity)

- **Identity Domains**
  - separate one's true identity from transaction details through the use of pseudo-identities
  - **Anonymity** - no identifiable data at all
  - **Pseudonymity** - identifiable for authorised users only
  - **Unlinkability** - no common identifier to link systems
  - **Unobservability** - anonymous until required for identification

**FIRST PRINCIPLE OF PbD: HOW DOES IT WORK?**

**USER KNOWN**

**THE IDENTITY PROTECTOR**

**IDENTITY DOMAIN**

**PSUEDO IDENTITY DOMAIN**

- **PID 1**
- **PID 2**
- **PID n**

**THE WORKINGS OF THE IDP**

An identity protector performs the following functions:

- It generates pseudo-identities as needed;
- It converts pseudo-identities into actual identities (as desired);
- It combats fraud and misuse of the system;
- At least two domains are created: an identity domain and a pseudo domain, one in which the user's actual identity is known and accessible, and one in which it is not;
- It permits the designer of a system to minimize the collection of personal data stored in the database.
SECOND PRINCIPLE OF PbD
SEPARATION OF DOMAINS

IDENTITY DOMAIN

IDENTITY PROTECTOR

PSEUDO-IDENTITY DOMAIN(S)

PbD REQUIREMENT QUESTIONS

ANALYSIS:
- Which data is needed
- Which data is collected
- Which data is recorded

DESIGN:
- Which elements are in the pseudo domain
- Which elements are in the identity domain
- Which level of self-determination is required

IMPLEMENTATION:
- Which techniques are available
- Which techniques can be used
- How to prevent the leak of information

ONE PRACTICAL EXAMPLE OF PbD: Hospital Information System

Basic tables with Pseudo Identities & ID Domains

Van Barkum, 1997
Borking, 2010
Dialogue between client and server in Hospital Information System

- login with ‘physician name’ (pn)
- transfer to the server
- check in table ‘physician’
- Transfer seq ‘physician’ to the client
- encrypt to ‘pid_physician’
- transfer the pid ‘physician’ to the server
- search table ‘care relation’
- select ‘sequence primary key of patient’ and search table ‘patient’
- transfer to client
- select the required patient
- encrypt seq ‘patient’ to ‘pid_patient’
- transfer to server
- search table ‘anamnesis’ with pid of physician and of pid patient etc. (Bokking, 2010, p.274)

Emerging Partial Identities
Marit Hansen, EU privacy workshop, October 2001

DEVELOPMENT OF PRIVACY KNOWLEDGE ENGINEERING

- Applying PETs Classic = Common Criteria = ISO 15408
- Translating Privacy Law in machine-readable code (Ontologies)
- Formulate Transfer Rules for personal data
- Applying control and feedback design
IMPLEMENTING PRIVACY PRINCIPLES INTO PbD (PISA 2003)

1. Determine the privacy principles
2. “Chain” selected articles of the DPD (GDPR) that belong to the chosen privacy principles.
3. Split the principles into a sets of tiny elements
4. Find the ontologies and taxonomies leading to a simplified conceptual model of the principle
5. Add knowledge base to enable interpretation of the queries
6. Formulate personal data transfer rules
7. Implement required security.
8. Implement HCI principles for building trust (ergonomics)

Example PbD: Transparency Principle: Elements for Data subject (PISA 2003)

1. Transparency (T)?
2. Be aware of T options
3. Be informed of PII processes
4. Be aware of what happens to PII
5. When expires the use of PII
6. Control how PII is handled
7. Enable to object to processing
8. Give explicit consent to Controller
9. Enable exercising rights
   • etc., etc.

DEVELOPMENT OF PRIVACY ONTOLOGIES FOR PbD 2003 – 2008 - 2011

Definition:
Formal machine understandable description of terms and relations in a particular domain (Bench-Capon 2007)

For privacy protection:
Encapsulation of knowledge about the data protection domain and relationships between concepts in an unambiguous standardization and legal instantiation (Kenny & Borking 2003)
What If Encryption Isn’t An Option?


- Key privacy parameters: 1. actors, 2. data, 3. actions, 4. purpose and 5. conditions. Using these parameters an organization can model and design their privacy practise (policy and data handling processes). For example consent can be modelled with a Condition parameter.

- For example, ABC Bank [actor] may disclose [action] customer phone number [data] to ABC Marketing Department [actor] for offering new services [purpose] if customer has consented to ABC Bank offering new service by telephone [condition].

OPTIONS: FROM PbD HAUT COUTURE TO READY TO WEAR

- Example PbD Haute couture e.g. Obligation Management System (OMS) (Cassassa Mont, 2006) & privacy ontologies
- PbD building principles analogous to Object Oriented Software Design designing PbD ‘ready to wear’ patterns
PbD HAUT COUTURE
PRIVACY OBLIGATIONS MANAGEMENT

PbD BUILDING PRINCIPLES
Object Oriented Software Design

Privacy Risk Management and selection of building patterns for: (not limited to)

- Privacy requirements patterns
- Anonimization and pseudonymization
- Hiding of personal data
- Data minimization
- Transparency
- Auditing and accounting
- Informed consent  (Van Rest, 2012)

PRIVACY BY DESIGN READY TO WEAR PATTERNS 1

Anonimization & pseudonymization patterns

Remove identifying parameters
Replace identifying parameters
Decrease resolution

Aggregation
Pseudonymous email
Blur (part of) image

K-anonymity
Revocable privacy
Decrease time resolution
PRIVACY BY DESIGN READY TO WEAR PATTERNS 2

TERRA INCognita PbD - WHO IS CONTROLLING THE AMBIENT?

- The ambient is a powerful knowledge repository; users do not have immediate control of their identity; scope of profiling is vast.
- Need for transparent information about data protection policy (suggested by the ambient in an intuitive way) and automatic protection

AMBIENT INTELLIGENCE
PbD ideas for Managing Spheres of Influence

- **Privacy Environment:**
  - Privacy negotiated at each moment by spheres of influence (social, employee, contractual, etc.)
  - Privacy is highly contextual: can be more easily compromised
  - User presets the sphere of influence by specifying the permission for each group.
- **PbD Solution:**
  - What kind of PbD architectures and DPIAs are needed?
    - Software agents or e-immunity device that prioritize interactions with different people?
  - DPIA for Aml similar to the CEN standard BS EN 16571:2014:
    - RFID privacy impact assessment process?
PROBLEMS FOR PRIVACY BY DESIGN

- PbD is done mostly without a proper privacy risk analysis up front (D-PIA) (Borking, 2010)
- The translation of PbD (the legal specs) into actual designs of systems is done by example. Therefore, everybody is free to postulate a particular design (process) as "Privacy or Data Protection by Design" Needed: standardized design patterns. [Van Rest, 2012]
- On top of that, actual implementation of PbD is confronted with difficulties such as lack of economic incentives, transparency of systems, legacy systems, and lack of adoption by organizations/end-users and consumers (Borking, 2010)

CONCLUSIONS

- PbD: No one-size-fits-all solution (van Rest 2012)
  - We need a toolbox with PIA, Privacy Design Patterns, PETs, PMS and design processes (Waterfall etc.) (More P&RE research please)
  - Validate (use of) PbD-toolbox via design processes
  - We do need the collection of and publication of concrete examples to learn from and collect and create metrics for the consequences of PbD

- PbD: Should facilitate certification of [product, production process, design], like certificates from EuroPrise & Certification should proof the presence of PbD (a sine qua non) (www.european-privacy.seal.eu/about/europrise)

- (Not a conclusion): Use Adoption factors (promotion by EU & DPA) and maturity gauging of organizations. [Borking, 2010]

A Few References

- Borking J.J.F.M., Privacy Law is Code: About the deployment of privacy enhancing technologies, Leiden 2010 (Privacyrecht is Code; Over het gebruik van PETs)
- Camerinah J., R.Leenes & D.Sommer (eds.) Digital Privacy, Berlin, 2011
- COM (2010) 245, A Digital Agenda for Europe, Brussels 2010
- Fritsch L., State of the art of Privacy Enhancing Technology (PET), Deliverable 2.1, PETWeb Research project, Oslo 2007
- IPC Ontario Toronto 2009, www.ipc.or.ca/images/Resources/7 foundational principles
- Pneeli B., Ikoromou D. (eds), Privacy Technologies and Policy, Springer 2012 & 2014
- Ribbers P.N.A., Privacy Process Requirements, Deliverable PRIME F 1, Brussels 2007
- WP 168 The Future of Privacy , Brussels 2009
Privacy by design?
Quantified Self

a technologist perspective

Open University Camden
November 2014
London
analysis
interpretation
correlations
connections
patterns
machine learning...
privacy is a behaviour not a setting

privacy is essential to identity

if you are not paying for it,
you are the product
Personal Data Infrastructure

Data Sources

Data Aggregation

Data Analysis

User Device

Data Directory manages data flows

Functionality layer (modules, plug-ins, apps)

Analytic Apps

Visualisation Apps

System Management

UI APIs

User Devices

• Mobile
• PC
• Tablets
• etc

(Different capabilities)

Ideally uses Open Standards across stack

Database (historic data)

Individual APIs convert different inputs to standard dataset
So what is to be done?
Designing Privacy In

19/11/2014

Legal background

- Fairly little about « Privacy by Design »
  
  1. Mostly about data minimization Article 6.1 of Directive 95/46/EC : « Member States shall provide that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed»

  2. Indirect references to PbD in parts related to information and consent

- References to « Privacy by Design » explicit in recent WP29 recommendations (IoT)
Why Privacy by Design matters

- Good practices
- Simplified discussions with DPA
- Being a Privacy champion

Good Practices

- Facilitate user acceptance
  - The case of sleep trackers in bedrooms
    - To be effective a sleep tracker has to record sounds and moves in the bedroom,
    - May process very sensitive information, trust is critical.
  - A crowd founded project (Sense) adopts a “Privacy by Design” approach
    - Records only specific sounds,
    - Offers local control over recoded data.
Good Practices

- Recent opinion on the Internet of Things
  - Many references to “Privacy by Design”,
  - Focus on three products of the “Internet of Things”,
  - Details some recommendations:
    - Limit data collection,
    - Process data locally,
    - Only transmit aggregated data,
    - Keep users in control.

Simplified discussions with DPA

- Storing less data limits the risk,
- Most data processing could be done by storing less personal data,
- Examples:
  1. ISP and Mobile phone company wants to find subscribers:
     - The ISP first transmits the addresses of customers,
     - The name is sent only if there is a match.
  2. An advertiser offers an opt-out to its mailing service without storing email addresses:
     - It only keeps a hash (transformation) of the email address,
     - When it receives a suggested email address, it computes hash to check if the user opted-out,
     - Similar to Facebook “Custom Audience”
Prioritizing privacy preserving solutions

- "Privacy by Design" solutions have a cost
  - Need new skills,
  - Collecting less data means less repurposing (no "Big Data"),
  - Few short-term advantages.

- Significant research interest for PbD
  - Behavioral targeting,
  - Geo-location,
  - Proximity testing.

- Increasing number of "Privacy Preserving" solutions
  - Sadly most of them remain papers,
  - DPA starts to provide incentives to adopt these solutions.

Example: Cookie Consent regulation

- Examples
  - Due to the cookie consent regulation most web-analytics solutions require consent,
  - In some countries (including France) there is an exemption under certain conditions (limited retention, anonymization, no secondary use),
  - Piwik is an open-source "privacy-friendly" analytics solution which follows WP29 opinion on "Cookie Consent",
  - As of today, it's the only web-analytics that does not require consent in France,
  - Existence of "privacy-friendly" solution provides an argument to DPAs.

1 Source Google Scholar scholar.google.com/scholar?q="privacy+preserving"&as_ylo=YEAR_X&as_yhi=YEAR_X

1 Source Google Scholar scholar.google.com/scholar?q="privacy+preserving"&as_ylo=YEAR_X&as_yhi=YEAR_X
Conclusion

• Legal ground to support “Privacy by Design” is being developed
  ▪ Regulation had no strong requirement for PbD,
  ▪ Recent recommendations a regulation hint a more formal support.

• Data Protection Authorities provide “Privacy by Design” support on a case by case basis
  ▪ “Privacy by Design” is often specific to the type of processing,
  ▪ Learning from data controller needs.

• There should be more incentive to support “Privacy by Design”
  ▪ Trust only pay in long term,
  ▪ DPA starts to provide incentive to adopt “Privacy Preserving” solutions.

Thank you!
Privacy: “It’s about the next twenty years”

“In the 20’s and 30’s it was the role of government, 50s and 60s it was civil rights, the next two decades are going to be privacy. I’m talking about the Internet, I’m talking about cell phones, I’m talking about health records. Who’s gay and who’s not,”


Written by Aaron Sorkin & Patrick Caddell
We believe in a new “privacy era”: Access to information is driven by brand trust; and its use by relevance and personalisation.

1993
Anonymity & Uncertainty

2007
Surveillance & Cynicism

2014
Transparency & Empowerment

We know customer information belongs to the customer.

It sums up everything we do to empower our customers. It tells them that we want them to be in the driving seat, in control, at their best.

POWER TO YOU
Two discussion points

1. Mental models for managing “your information”
2. Cognitive load and 21st Century “data access”

Customers don’t know what it is to “manage their information”

Customers want control….. but don’t want to spent time and energy controlling

Especially, on something they don’t understand
The importance of metaphors

“Metaphor is not a harmless exercise in naming. It is one of the principle means by which we understand or experience…. To the extent that we act on our reason, metaphor plays a role in the creation of reality”
Data is the New Oil
By Michael Palmer

“Data is the new oil” Clive Humby, ABB Senior marketer’s summit, Kellogg School.

Data is just like crude. It’s valuable, but if unrefined it cannot really be used. It has to be changed into oil, gas, plastic, chemicals, etc to create a valuable entity that drives profitable activity. It must be broken down, analyzed for it to have value.

Your Data is Black Gold, So Don’t Give Away the Drilling Rights
October 31, 2011 @ Big Data, Business Markets
But, where is the customer?

Transparency
& Empowerment

Control Reassurance Relevance

Bringing the human (data subject) back in?

Digital Shadow
Data Exhaust
Digital Footprint

BIG BROTHER IS WATCHING YOU
Consumers user language relates to wars and battles

Bombardment  Invasion

What is the right metaphor for “managing MY information”? 
Two discussion points

1. Mental models for managing “your information”
2. Cognitive load and 21st Century “data access”

A Goldilocks problem

Really? Too cold.....
Really? Too hot....

Presentation..... Just right?

Participation.... Just right?
How do we present Meaningful information Alongside Meaningful choices?

It sums up everything we do to empower our customers. It tells them that we want them to be in the driving seat, in control, at their best.

POWER TO YOU
Privacy by Design

Dr. C. N. M. Pounder
chris.pounder@amberhawk.com

CRISP: London, 19 November, 2014

BASIC POINTS

• There is little market incentive in the private sector to use or implement Privacy by Design techniques.

• Privacy by Design will not be implemented successfully unless the legislative environment surrounding the processing of personal data also provides an adequate level of privacy protection.

• The Snowden revelations have shown that the legislative environment is inadequate and that the Government is reluctant to change it.
REGULATION WON’T HELP MEMBER STATE EXEMPTION

- Article 2: This Regulation does not apply to the processing of personal data: … in particular concerning national security… by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

- Article 21: Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided …(in A.5, A.11-A.20 and A.32)…, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard: (a) public security; (b) the prevention, investigation, detection and prosecution of criminal offences etc etc and (c) other public interests of the Union or of a Member State, in particular … taxation matters …

DAPIX A.23 WEAKENS FURTHER

*Data protection by design and by default*

Original from Commission

Having regard to the state of the art and the cost of implementation, 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 and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

Major change (DAPIX)

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, [including minimisation and pseudonymisation], in such a way that the processing will meet the requirements of this Regulation and protect the rights of (…) data subjects.
THE NINE IDA PRINCIPLES

1. **User Control**: Identity assurance activities can only take place if I consent or approve them
2. **Transparency**: Identity assurance can only take place in ways I understand and when I am fully informed
3. **Multiplicity**: I can use and choose as many different identifiers or identity providers as I want to
4. **Data Minimisation**: My request or transaction only uses the minimum data that is necessary to meet my needs
5. **Data Quality**: I choose when to update my records
6. **Service-User Access and Portability**: I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want
7. **Governance/Certification**: I can have confidence in any Identity Assurance System because all the participants have to be accredited
8. **Problem Resolution**: If there is a problem I know there is an independent arbiter who can find a solution


THE NINTH IDA PRINCIPLE (Exceptional Circumstances)

9. **Exceptional Circumstances**: Any exception has to be approved by Parliament and is subject to independent scrutiny

We recognise that special interests (e.g. law enforcement) may need exemptions and this is the purpose of the Ninth Principle.

Such special interests should be subject to a simple rule: exemptions have to be explicitly defined and publicly reported.

We do not think it advisable to allow existing legislation to define access to any data from the Identity Assurance Service since such legislation, when it was originally enacted, could not have been scrutinised in the context of an Identity Assurance Service.

Any exemption from these Principles needs public scrutiny in order to gain credibility and maintain trust.

“Dispute Resolution” Principle still applies (“If there is a problem I know there is an independent arbiter who can find a solution”)
Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and despite attempts to hack into this with an incorrect key, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.

https://www.youtube.com/watch?v=5Px1WjVWIb0
CCTV CONCERNS

• Have you reduced the “benefits” of CCTV (especially unsupervised CCTV)?

• Have you moved the problem from data collection to data retention and subsequent access by the authorities (in the absence of a proper legislative framework)?

• Do you have the potential for more CCTV cameras on the grounds that camera’s protect privacy on data collection?

• Is this variant of Privacy by Design a Trojan Horse?

QUESTIONS?

©Chris Slane

chris.pounder@amberhawk.com

Amberhawk Training Limited
and
Hawktalk’s balanced blog.
THE END
Privacy by Design

Dr. C. N. M. Pounder
chris.pounder@amberhawk.com

CRISP: London, 19 November, 2014
Annex 10. CPDP Panel Description

Wednesday 21 January

CPDP 2015 will stage more than 60 panels and workshops with a stimulating mix of academics, practitioners, regulators and advocates, as well as multiple side events such as open debates, PechaKucha performances and artistic interventions.

Please note that this is a preliminary version of the program which is still in its early stages. Accordingly, some panels may change or be rescheduled.

08.15 - Welcome coffee in Le Village

CPDP 2015 Panels at Maison des Arts

8.45 - COMMERCIAL OPPORTUNITIES FOR DESIGNING PRIVACY IN: EMBEDDING PRIVACY IN ORGANISATIONAL PRACTICES

organised by CRISP

Chair William Webster, University of Stirling (UK)
Moderator Geoffrey Donker, University of California Irvine (US)
Panel John Borking, Borking Consultancy (NL), Casey Chapelle, Vodafone (UK), Tom Ilube, Call Credit Group (UK), Jason Pridmore, Erasmus University (NL)

The need to design privacy into technological development and deployment is well understood and has resulted in concepts and approaches like 'Privacy by Design' and 'Privacy Enhancing Technologies'. Although these approaches are well established, they are arguably hampered by being too prescriptive and relatively unsympathetic to complex organizational settings and processes. Recently, these approaches have been complemented by a drive to commercialise privacy, to place a monetary value on privacy and to demonstrate how privacy can represent a commercial opportunity. Whilst this perspective places added value on the concept of privacy it does little to ensure privacy is a value embedded in organizational processes and practices – and privacy friendly technologies are only likely to emerge from environments where privacy is a cherished value. This panel takes the strengthening of privacy a step further by exploring how it can be deeply embedded into organizational settings and the interrelated regulatory environment.

- How can the value of privacy be commercialised?
- How can the value of privacy be embedded into organizational processes and practices?
- What is the role of regulation in commercialising privacy?
Commercial opportunities for designing privacy in: embedding privacy in organizational practices

Chair:
Professor William Webster, CRISP Director, University of Stirling (UK)

Moderator:
Professor Geoffrey Bowker, University of California Irvine (US)

Speakers:
Dr John Borking, Borking Consultancy (NL)
Dr Jason Pridmore, Eurasmus University, (NL)
Kasey Chappelle, Vodaphone Privacy Group (UK)
Tom Ilube, Call Credit Group (UK)
Annex 12. CPDP Panel Participants

Commercial opportunities for designing privacy in:

Embedding privacy in organizational practices

**John BORKIN**
Dr. J (John) J. F.M Borking, married, (1945), Director/owner of Borking Consultancy in Wassenaar, Netherlands, Of Counsel and external advisor on Privacy-by-Design issues for the law firm CMS Derks Star Busmann, is the former Privacy Commissioner and Board Member of the Dutch Data Protection Authority (CBP) in The Hague. He is e-Law researcher at the University of Leyden and he is a lecturer on PETs at TopTech (Delft University). He is a certified privacy law expert for EuroPrise in Bonn (Germany) and expert member of the advisory board. He is chairman of the Dutch Complaints and Disputes Committee e-Recognition (e-Authentication) in The Hague. Dr. Borking holds a PhD from Leiden University.

**Geoffrey BOWKER**, University of California Irvine (US)

**Kasey CHAPELLE**
Kasey Chappelle is Vodafone Group’s Global Privacy Counsel, guiding the company’s privacy and data protection strategy, policy and compliance. She leads a group of privacy legal, regulatory and public policy experts across the Vodafone corporate family, to form strategy around privacy risks, create best practices, respond to external developments and share Vodafone’s position with policy makers and opinion formers. Her background is in consumer privacy and regulatory law, with experience as eBay’s global privacy director, handling consumer privacy issues for eBay’s e-commerce, financial and online services around the world. She started her legal career as an associate in telecommunications, technology and privacy law at Willkie Farr and Gallagher in Washington, DC. Before that, she studied and worked in advertising and graphic arts - skills that come in handy when advising on privacy by design, user interfaces and product development.

**Tom ILUBE**
Tom Ilube is CEO of Crossword Cybersecurity plc, a technology transfer company focused on the cyber security sector. He was previously Managing Director of Callcredit Consumer Markets, the UK credit reference agency. As part of Callcredit, he launched a major new consumer initiative, Noddle.co.uk. Previously, Tom was CEO of Garlik, the online identity protection company acquired by Experian. He was Chief Information Officer of Egg plc, the UK’s most innovative online bank. Tom served the ITU, the Geneva-based UN agency, on the High Level Expert Group on Cybercrime and as Chairman of the UK Technology Strategy Board’s Network Security Innovation Platform Tom has been a regular media commentator and conference speaker on identity theft and cybersecurity issues.
Jason PRIDMORE, Erasmus University (NL)

William WEBSTER
William Webster is Professor of Public Management and Policy at the University of Stirling. He is a Director of CRISP - the Centre for Research into Information, Surveillance and Privacy. He is an international expert on the governance of CCTV, privacy and everyday surveillance. Between 2009 and 2013 he led the Living in Surveillance Societies (LiSS) research programme and he is a project partner in the IRISS and ASSERT European Commission funded research projects.
HISTORICAL PERSPECTIVE OF PRIVACY-BY-DESIGN AND ECONOMIC CONSIDERATIONS

Dr. John J. Borking

Session: Commercial Opportunities for Designing Privacy in: Embedding Privacy in Organisational Practices.

MENU

• WHAT IS PRIVACY-BY-DESIGN (PbD)?
• TIMELINE PRIVACY-ENHANCING TECHNOLOGIES (PETs) / PRIVACY-by-DESIGN / PRIVACY MANAGEMENT SYSTEMS (PMS)
• ECONOMIC CONSIDERATIONS
WHAT IS PRIVACY-BY-DESIGN?

- The word ‘by’ implies that data protection purposely has to be realized by design.
- First in the history of Mankind: Building Ethical principles into machines.
- The application of such principle would emphasize the need to implement privacy enhancing technologies (PETs), privacy by default settings and the necessary tools to enable users to better protect their personal data (e.g. access controls, encryption).

WP 168 The Future of Privacy p.13
ECONOMICS PbD
CENTRAL QUESTIONS

- When starts an organization bothering about privacy?
- What factors affect an organization’s decision to introduce PbD/PETs?
- Is there a business case for PbD?

ROGER’S THEORIE ON THE DIFFUSION OF INNOVATIONS, i.e PbD/PETs

Rogers, 2003, p.11
THE ROI-PI EQUATION
Return on Privacy Investments

- INVESTMENT IN PBD/PETs REQUIRE A CERTAIN LEVEL MATURITY (IAM PARAMETER) & INSIGHT IN COSTS AND QUANTITATIVE AND QUALITATIVE BENEFITS.

- ROI = FINANCIAL TOOL THAT MEASURES THE ECONOMIC RETURN OF A PROJECT OR INVESTMENT

\[ \text{ROI-PI} = \frac{\text{Total Cost} - (\text{Intangible Benefits} + \text{Tangible Benefits} + \text{Value Of Risk Mitigated})}{\text{Total Costs}} \]

Value of Risk mitigated based on data leakage figures USA
Example: IXQUICK.com case
Borking, J.J, Assessing Investments mitigating Privacy risks, Leiden 2010

References

- Borking J.J.F.M., Privacy Law is Code: About the deployment of privacy enhancing technologies, Leiden/Deventer 2010 (Privacyrecht is Code: Over het gebruik van PET)
- Fritschi L., State of the art of Privacy Enhancing Technology (PET), Deliverable 2.1, PETWeb Research project, Oslo 2007
- IPC Ontario Toronto 2009. www.ipc.on.ca /images/Resources/7 foundational principles
- Preneel B., Ikonomou D. (eds), Privacy Technologies and Policy, Springer 2012 & 2014
- Ribbers P.M.A., Privacy Process Requirements, Deliverable PRIME F 1, Brussels 2007
- WP 168 The Future of Privacy, Brussels 2009
Commercializing Privacy by Design

Potentials and problems in configuring privacy

Jason Pridmore, PhD
Department of Media and Communication

Value and definition of privacy

Corporate motivations  Human behaviour
End user expectations and demands  Technological artefacts
Regulatory desires and requirements  Technological processes
Systems and patterns of work
Privacy configurations

• Cannot easily separate privacy
  – Exponential set of arrangements
• Privacy is too often an afterthought
  – Attempts with Privacy policies, data protection frameworks, and PETs
  – Where we end up with PbyD

Which Privacy by Design?

• Pre-emptive Privacy by Design
  – Focus: data confidentiality and the security of data transfer
  – Systems engineering perspective
  – Reliance on significantly reduced data capture or cryptographic practices and other security mechanisms to achieve properties like anonymity, unlinkability, unobservability, and communications content confidentiality.
  – Not often initially identified as Privacy by Design
Which Privacy by Design?

- Compliance and Beyond PbyD
  - Regulatory/legal approach
  - Focus on ‘data protection’
  - Ensuring compliance in the fair use and analysis of data
  - Limitations in enforcement result in collaborative approach

Which Privacy by Design?

- User-centric PbyD
  - Selling privacy to the consumer directly
  - Problem of privacy translated to inability of users to be responsible for their own data
  - Provide simplified solutions that empower consumers to reveal and conceal the information they want to in the context of their choice
Privacy by Design Choices

- Definition of the problem is determinative of how the problem can be or will be resolved
- Privacy as a differentiator for commercial success remains limited
- Transparency is a double edged sword
- Success is based on changing and transforming the role of how these pieces are configured

Success factors?

- Consider the whole configuration
  - Shaping of people and technology in relation to each other
- Recognise the limitations of consumers
  - Context matters in the success or not of Privacy by Design
- There are no one size fits all solutions
  - Privacy by Design can only really be done on a case by case basis
Annex 15. Kasey Chappelle Presentation
Information Manager

What is My Information Manager?
With My Information Manager, you can see what personal information we hold about you, and control how it's used.
And you make sure your services and apps are relevant to you by sharing your likes and dislikes.

Why use My Information Manager?
Giving us permission to use your information means that we can tailor our services to you.
And it helps us make sure you only receive marketing messages that match your interests.

How do I use My Information Manager?
Use it to see the different kinds of information we currently hold about you.
Then choose which of our services can use which bits of information.
“both viciously complex and floatingly abstract”
Creating a culture of privacy across Vodafone
Our commitments guide how we will conduct ourselves and treat our customers and employees

Comprehensive operational privacy processes
Standard global risk control processes to ensure that how we handle information meets our Commitments, complies with law and lives up to customer privacy expectations while meeting business needs

Managing critical privacy concerns
Formal assessment and global policy governance of the most critical privacy risks facing our company and industry

Respect
We value privacy because of its value to people. It's about more than legal compliance - it's about building a culture that respects privacy and justifies the trust placed in us

Privacy by Design
Respect for privacy is a key component in the design, development and delivery of our products and services

Openness and Honesty
We communicate clearly about actions we take that may impact privacy, we ensure our actions reflect our words, and we are open to feedback about our actions

Accountability
We are accountable for living up to these principles throughout our corporate family, including when working with our partners and suppliers

Choice
We give people the ability to make simple and meaningful choices about their privacy

Balance
When we are required to balance the right to privacy against other obligations necessary to a free and secure society, we work to minimise privacy impacts

Laws and Standards
We comply with privacy laws, and we will work with governments, regulators, policymakers and opinion formers for better and more meaningful privacy laws and standards
Introduction
Welcome to this module on Privacy by Design. At Vodafone we are committed to building privacy considerations into our products and services from the outset, and using our influence to shape the technologies of our partners and peers. This module introduces you to our commitments to Openness and Honesty, Choice and Privacy by Design and uses a fictional example to illustrate their application.

In this module you’ll learn:
- Who is accountable for meeting this commitment
- How our policy standards apply through the design process
- Where to find advice from privacy specialists
- Which high risk categories need particular attention.

Features of the app
The mCommerce team are deciding which basic features should be included in the app. Can you see any features which may impact on users’ privacy? Select those features you think need consideration.

1. Targeted advertising
2. Voucher for children’s services
3. Map showing nearby suppliers
4. Share on Facebook, Twitter, other social features
5. Analytics reports
The regulation must strike a **balance**: We believe **strong privacy** protections are the key to a **sustainable data economy**. We can't operate or grow as a business unless our customers trust us with their personal information. But the current regime has created process, not protection.
Annex 16. Tom Ilube Presentation

Tom Ilube

@crosswordcyber
www.crosswordcybersecurity.com
tom.ilube@crosswordcybersecurity.com