Privacy by Design: from research and policy to practice – the challenge of multi-disciplinarity

Pagona Tsormpatzoudi[1], Bettina Berendt[2] and Fanny Coudert[1]

[1]Center for IT and IP Law and [2]Department of Computer Science
KU Leuven, Belgium
firstname.lastname@kuleuven.be

Tsormpatzoudi, P., Berendt, B., & Coudert, F. (2016). Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity. In B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, & S. Schiffner (Eds.), *Privacy Technologies and Policy. Third Annual Privacy Forum, APF 2015. Luxembourg, Luxembourg, October 7-8, 2015. Revised Selected Papers* (pp. 199-212). Berlin etc.: Springer. LNCS 9484.

Abstract. The concept of Privacy by Design (PbD) is a vision for creating data-processing environments in a way that respects privacy and data protection in the design of products and processes from the start. PbD has been inspired by and elaborated in different disciplines (especially law and computer science). Developments have taken place in research and policy, with the General Data Protection Regulation to be adopted by the European Parliament in 2016 and to enter into force in 2018. It is now time to use the results for practical guidance on how to achieve the goals defined by the legislation. In this paper, we summarise lessons learned from the special session on Multidisciplinary Aspects of PbD organised at the Annual Privacy Forum 2015. In particular, we identify important current and future implementation challenges of PbD. These are: terminology, legal compliance, different disciplines' understandings, the role of the data protection officer, the involvement of all stakeholders, and education. We conclude by emphasising the importance of approaching PbD in an interdisciplinary way.

Keywords: Privacy by Design, multi- and interdisciplinary approaches, General Data Protection Regulation, education

1 Introduction

The concept of Privacy by Design (PbD) is a vision for creating data-processing environments in a way that respects privacy and data protection in the design of products and processes from the start, rather than treating these as desiderata that may be treated as additional, ex-post, and lower-priority requirements. PbD has, from the start, been inspired by, and elaborated in, different disciplines (especially law and computer science). Also from the start, PbD was meant to be deployed as a practice in organisations, as something to be codified into actual laws and as a way to enforce law. At the moment it has been codified in the EU, with the new General Data Protection Regulation expected to be adopted by the European Parliament in early 2016 and to come into force in 2018. However, the concept is still not known to large parts of the public and industry.

While developments have taken place in the fields of research and policy, practical guidance on how to achieve the goals defined by the legislation is still lacking. In this context, PbD is becoming a huge multidisciplinary opportunity for "bringing research and policy together", the core theme of the Annual Privacy Forum 2015. At the same time, however, PbD faces many challenges. These include common terms that evoke vastly or subtly different concepts, absence of or uncertainties concerning implementation methods, and disagreement about evaluation criteria.

These observations motivated us to organise a session on the multidisciplinary aspects of PbD at APF 2015. In the present article, we first give an overview of the concept and development of PbD and then summarise lessons learned from the panelists' contributions and the discussions surrounding the panel. This paper does not intend to attribute views and statements to any individual participant but rather identify important challenges for implementing PbD and other take-home messages from the overall debate. The goal is to illustrate current and future implementation challenges of PbD. Amongst them we highlight the importance of teaching PbD concepts and skills, reporting on experiences with students and practitioners. We conclude by emphasising the importance of approaching PbD in an interdisciplinary way.

2 Context: Privacy by Design (PbD)

Privacy by Design (PbD) has in recent years developed as a legal and technological concept that helps enforce data protection obligations and make privacy a priority in an organisation. PbD has developed within experts communities both from the technological side that produced privacy-respecting methods and tools, and from the legal and policy side that reflected on the usefulness and limits of the concept as a new way to enforce the privacy and data protection frameworks.

The idea first emerged in the 1990s with the concept of Privacy Enhancing technologies (PETs), as alternative to the traditional focus on legal and administrative instruments that are exhausted with policy development and monitoring (van Rossem et al., 1995; Koorn et al., 2004). PETs, first, developed in relation to two data

protection principles, data quality and data security[1], thus contribute to the protection of the confidentiality of personal data. However, technologists also started proposing PETs as a solution for the implementation of other data protection principles such as transparency or accountability (Phillips, 2004; Gürses & Berendt, 2010; Diaz & Gürses, 2012). PETs grew as a solution for personal data management in general (Danish Ministry of Science Technology and Innovation, 2005). This wider scope is reflected in the terms under which the concept has been popularised since the 1990s, including "data protection by technology" (ULD, 1996) and "privacy by design" (Cavoukian, 2011). From the start, PETs/PbD have been developed by computer scientists and lawyers, sometimes jointly, sometimes in parallel. Thus, bringing the different perspectives on PbD together remains an ongoing challenge. Technical, legal and other stakeholders should work together and have a role to play in delivering products and services that take privacy into account from the start. In the remainder of this section, we will briefly sketch important elements of today's views from these two disciplines, and identify implementation as a key challenge.

2.1 PbD as a computer-science concept

The increasing use of the term PbD in computer science reflects the concept's increasingly generalised scope: from the focus on *tools* or *instruments* in PETs to a focus on more comprehensive *design* guidelines, processes and practices (see also Gürses, Troncoso, & Diaz, 2011; Hansen, 2015). Computer scientists now consider PbD from a variety of perspectives (many of these are described in the overview in Danezis et al., 2014). These perspectives range in granularity from desirable properties of data (e.g. degrees of anonymity or type of encryption) and constraints on algorithms (Monreale et al., 2014) to methodologies for requirements engineering and the whole process of software development (Gürses 2010; Wuyts 2015). The perspectives range in formalisation from mathematical proofs of datasets and algorithms having certain properties to investigations of human privacy-related behaviour and recommendations for the design of human-computer interfaces (Jameson et al., 2014).

This multitude of approaches also implies that the notion of privacy itself as the goal of PbD is not uniform: it ranges from IT Security's data confidentiality to psychologically and sociologically informed notions of privacy. A matching to legal notions of privacy and data protection is also not always straightforward. A computer-science method that promises to deliver, protect, enhance, etc. "privacy" or "data" therefore has to be investigated closely for the degree to which it can implement legal notions and possibly also the degree to which it does something else.

[1] The principle of data quality (Article 6 Directive 95/46/EC) includes the principles of fairness (data must be processed fairly), lawfulness (data must be processed according to a legitimate legal ground), purpose limitation, data minimisation, and accuracy. PETs are able to ensure confidentiality of personal data as an attribute of information security.

2.2 PbD: the emergence of a legal obligation

From a legal perspective, PbD is an approach to privacy that places technology at the service of the law, i.e. it seeks for technical solutions to address privacy and data protection requirements posed by the legal framework (Tsormpatzoudi & Coudert, 2014).

The emergence of PbD as a legal obligation followed up on a lively policy debate. During the 2000s, the ideas of PETs and PbD gained recognition at EU level, and in 2007 the European Commission published a Communication promoting the use of PETs as complementary mechanism for the enforcement of the data protection framework (European Commission, 2007, p. 6). In this Communication, the EC defines PETs as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing functionality of the information systems". In 2009, under the preparatory works for the reform of the European Data Protection framework, the Article 29 Data Protection Working Party (2009) advocated the introduction of a *principle of privacy by design* that would emphasize the need to implement PETs, "privacy by default" settings and the necessary tools to enable users to better protect their personal data (e.g., access control, encryption). This was seen as a way to move data protection "from theory to practice" and make technology developers responsible for the systems they produce. Like the other data protection principles, this principle would have to be defined "in a technologically neutral way" to keep pace with the fast-changing technological and social environment. Similarly, the wording should be flexible enough to allow stakeholders to translate the principle into concrete measures adapted to each specific case.

After long negotiations, the compromise text for the draft General Data Protection Regulation (GDPR) includes the concepts of data protection by design and by default (Council of the European Union, 2015, Article 23 and Recital 61). The two concepts represent the more comprehensive concept of PbD, which was tailored into these two derivatives for consistency with the scope of the particular legal instrument (GDPR). Data protection by design requires that "the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of the Regulation and protect the rights of data subjects". Data protection by default requires that "the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed".

2.3 Implementation challenges facing PbD

PbD refers to the design process, but it cannot be understood separately from the whole organisational context in which it develops. This is acknowledged in Recital 61

of the Draft GDPR, which points out that the controller should adopt internal policies and measures to comply with the principles to data protection by design and by default (Council of the European Union, 2015). Being related to the general context, PbD is naturally affected by different disciplines. Technical, legal and business stakeholders should work together and have a role to play to deliver products and services that take privacy into account from the start.

The concept of PbD has developed within experts communities both from the technological side that produced privacy-respecting methods and tools, and from the legal and policy side that reflected on the usefulness and limits of the concept as a new way to enforce the privacy and data protection frameworks. However, PbD has so far not reached companies. One rationale for turning the principle into a legal obligation was to drive companies to implement it in practice. Yet, companies lack practical guidance on how to achieve the goals defined by the legislation. Conceptual and terminological challenges are exacerbated when legal provisions get translated into descriptions and instructions for stakeholders from other disciplines, such as engineers or business actors.

3 Overview of the APF 2015 Session on Multidisciplinary Aspects of Privacy by Design

The Computer Science Department and the Center for IT and IP Law of KU Leuven co-organised a session on 7th October 2015 at the Annual Privacy Forum in order to discuss the challenges faced by companies when deciding to integrate Privacy by Design into the development of products and services. The objective of the Annual Privacy Forum, supported by DG Connect and ENISA, is to provide a forum to academia, industry and policy makers, and among other things discuss the uptake of PbD in industry. Although privacy technologies are widely discussed in various research communities, their mere existence is often unknown to the general public. Hence PETs need the support of policy to find their way into IT products. The session received funding by the EU FP7 project PARIS, which aims at defining and demonstrating a methodological approach for PbD in the development of surveillance systems.

The session consisted of a keynote given by Marit Hansen, Privacy & Information Commissioner of the State of Schleswig-Holstein, Germany, who introduced the need of a motivated interdisciplinary approach to privacy and data protection by design. This was followed by a panel that included three more participants who brought different viewpoints to the table. Dan Bogdanov, Product manager for Sharemind at Cybernetica (Estonia), focused on the challenges raised for product development. David Stevens, Data Protection Officer at Telenet (Belgium), related his experience in interacting with other departments from a same organisation (such as marketing or engineering) in order to look for a solution that takes into account all requirements. Matthias Pocs, representing the European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC) (Germany), stressed the importance of involving consumers in the PbD process. The

session was moderated by Antonio Kung, CTO, Trialog, France and coordinator of the PARIS and PRIPARE EU projects.

4 Current challenges for PbD

In this section, we describe four main areas in which clarification and guidance are needed. The first challenge is related to the way the concept is described in the GDPR. The second is the challenge of the interpretation of the concept: we argue how even from a legal standpoint, focussing only on legal compliance can threaten the success of PbD. From an engineering standpoint, viewing privacy only in terms of *risks* (to be guarded against by trying to comply with a law) is even more restrictive; a positive view as a *goal* is more likely to help PbD succeed. The third challenge is the different understandings of PbD across disciplinary boundaries. The fourth challenge is the role of the data protection officer in an organisation – a person who needs to integrate multiple interests and who needs to be loyal to the law as much as to his or her organisation and its (e.g. business) goals. Throughout all challenges, we can see how applying a certain disciplinary lens can enable PbD practitioners to zoom in on and pan around new questions, which in turn require the lens of yet other disciplines.

4.1. Challenges arising from the wording in the GDPR

A factor contributing to the lack of understanding of the principle of PbD and how to implement it in practice, is the way it has been worded in the Draft GDPR. The Communication of the Commission that launched the discussion for the data protection reform initially referred to 'Privacy by Design', as the discussion at the beginning of the reform permitted a general and broad view on the matter (European Commission, 2010). In the first draft of the GDPR the choice was made to introduce the concepts of data protection by design and by default due to the scope of such instrument, which intends to protect the fundamental rights and freedom of individuals, and in particular the right to the protection of personal data, in relation to the processing of such data (Article 1) (Tsormpatzoudi & Coudert, 2015a).

In the compromise text of the GDPR, the principle of *data protection by design* mandates data controllers both at the time of determination of the means for processing and during the processing itself, to take technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing (Article 23). *Data protection by default*, which is introduced in addition to data protection by design in Article 23 (2) and Recital 61, requires privacy settings on services and products that by default comply with the general principles of data protection, such as data minimisation and purpose limitation (Council of the European Union, 2015).

Furthermore, Recital 61 provides a non-exhaustive list of examples of data protection by design measures such as minimising the processing of personal data,

pseudonymising personal data as soon as possible, enhancing transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, and enabling the controller to create and improve security features. These concrete examples enhance the clarity of the provision. However, Article 23 then provides an extensive list of factors related to data processing to be taken into account when deciding about the implementation of data protection by design measures, and these factors blur the picture. Besides the available technology and the cost of implementation, the factors also include 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. Balancing these factors is expected to be a challenging task, given that there is no further explanation on how to interpret and prioritise them in relation to one another. This may eventually be a difficulty for implementing data protection by design in practice (Tsormpatzoudi & Coudert, 2015b).

4.2 Legal compliance for implementing PbD

When developing technologies, system requirements come to fulfil different considerations. This is a challenge to be addressed in complex ecosystems of private organisations, where different departments function with different assumptions of privacy deriving from political, economic, business, legal, or technical interests.

For instance, in a given system, a privacy expert may argue for data minimisation, which will imply that the minimum amount of information should be stored in the system. This may also be a legal requirement. At the same time, a security expert may propose data integrity from a security point of view, which may require a considerable amount of data that is accurate, consistent and reliable. This would be in principle contradictory to data minimisation but also very essential for the system.

Gathering such interests, including compliance with the law, often represents risks to be taken into account in product development. Legal compliance as a risk often results in legal workarounds which may take place for the sake of compliance only. In the above example, an organisation may take a series of data minimisation measures and this may seem to comply with the law, but may not be the case if storage is not really needed at all (see also Schaar, 2010).

The inclusion of the principle of data protection by design in Recital 61 and Article 23 of the draft GDPR creates a legal obligation for data controllers. However, this obligation should be detached from the goal of addressing it only because it may create a compliance risk. Preserving privacy should rather become a goal in itself in product development. Rather than just taking measures to demonstrate that the PbD has been taken into account, data protection by design and by default should penetrate the actual working culture and the decisions taken in an organisation.

4.3 Difficulties of understanding between disciplines

PbD does not provide fixed solutions. It rather suggests that IT solutions alone cannot ensure sufficient respect of privacy in an organisation. In several cases PbD requires a running system with clear responsibilities and tasks that may be process-oriented, taking into account the full lifecycle of system evolution. PbD is therefore a means of involving all relevant stakeholders active in engineering, law, organisational processes, business models, user interaction, or organisational culture. The purpose of the system is the common starting point that allows all stakeholders to discuss about the requirements the system should comply from the perspective of each discipline and further justifies the necessary data processing, the appropriate protection levels and measures to implement privacy.

Involving the relevant stakeholders in this process is not an easy task given that each comes with different systems of beliefs and values even with different vocabulary. This leads to lack of cross-disciplinary understanding. For example, when talking about "erasure" as a good PbD practice, one needs to clarify what exactly is necessary to erase. For instance, a stakeholder who operates on the assumption of storage by default, may exclude logfiles and temporary files from a privacy assessment, even though such files may contain significant amounts of personal data. Thus for a developer of a particular component this may be an acceptable – or even altogether harmless – practice, however, a privacy manager or a compliance officer who may look into the system more holistically will identify the pitfall. The added value of the joint interdisciplinary work would help bring these views together and define solutions that satisfy all involved experts.

4.4 The Data Protection Officer (DPO): a key actor to communicate about privacy internally and to coordinate the different needs

The introduction of the function of a DPO may be a cornerstone in the implementation of PbD as an interdisciplinary concept (Article 34 GDPR). DPOs will have to monitor compliance with data protection law and engage in several activities to promote data protection in their organisation. DPOs may link between different functions of an organszation and as such promote the interdisciplinary aspects of the principle Privacy/Data Protection by Design. DPOs as employees of the data controller have a quite sensitive but pivotal role. They will be the ones to promote the dialogue between different departments and eventually strike the balance between different interests under the common goal of implementing privacy/data protection by design. Their skillset should include the ability to compromise –but without losing sight of the obligation to comply with the law-, be part of a negotiation process, and be ready to accept other views reflecting different system of beliefs and values coming from different stakeholders.

The sensitivity of the role of the DPO has been recognised in the discussions of the draft GDPR, which takes steps to promote their independence. It thus states in its report that Data Protection Officers should be protected from being penalised or dismissed for reasons other than not performing well their data protection compliance

tasks (Article 36 para 3, Article 35 para 7). Nevertheless, even though the Regulation obviously tries to avoid situations of conflict of interest (Article 36 para 4), it should be noted that DPOs will always have as agenda to defend the best interests of the company. Yet, their freedom within the organisation to talk equal-to-equal with other departments will contribute to a higher level of privacy protection.

5 Challenges ahead: Involvement of stakeholders outside the data controllers' organisation, and education

Implementation of PbD has so far been understood mainly in relation to obligations of an organisation as the data controller. This section elaborates on challenges ahead in the implementation of PbD. First, organisations will have to re-assess their focus on the data processing lifecycle. New technologies will illustrate that PbD is a responsibility not only of data controllers but also of data subjects and technology providers. The next steps will be to broaden the scope of application of PbD and find ways of involving end users and technology providers. Second, limited understanding or experience with the concept as illustrated in the sections above will create a significant need to invest in awareness, knowledge and skills. Education will thus be an important future implementation challenge.

5.1 End users

PbD as a negotiation process amongst all stakeholders should not only focus on data controllers but also involve end users, who are meant to ultimately profit from PbD. This idea has been reflected in the GDPR Article 33 para 4, which introduces the obligation of the data controller to perform a Privacy/Data Protection Impact Assessment. Specifically, "the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations". However, the involvement of end users in privacy negotiation is far from trivial. It presupposes awareness and understanding of the core issues that happen in the value chain.

Being the last part in the value chain, end users are often less aware or interested in PbD implementation. This may explain why despite the policy efforts to foster implementation of PbD, the take-up of PETs remains low. As a result, privacy as competitive advantage is still not a mature idea on the market. Some users perceive usability and privacy as a trade-off. Others will only accept any change (e.g. an increase in privacy-friendliness) if it is also accompanied by a usability improvement. Yet others find it hard to accept any change "because they have always worked in this way" – even if, for example, the change consists of storing or processing data that these users never used in the first place. These examples illustrate why also a challenge that sounds relatively specific ("involve end users") calls for contributions from several disciplines, such as usability design and process change.

Education and additional ways to involve end users in PbD implementation will help overcome such challenges. Recently, standardisation initiatives have been

emphasised as a means to furthering PbD implementation. In January 2015, the European Commission issued an Implementing Decision including a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management in the field of security industrial policy (European Commission, 2015). Standardisation may function as an enabling method for involving end users in PbD. However, as consumers (end users) represent only one voice and are in a minority, it may be difficult to be heard in a community established to defend the interests of industry.

5.2 Technology providers

In the compromise text adopted on December 15, 2015, the Regulation introduces the obligation for data controllers to adopt technical and organisational measures appropriate to comply with the requirements of the Regulation and protect the rights of data subjects ("data protection by design") (Article 23) (Council of the European Union, 2015). Yet in several cases, the data controller only operates at the very end of the supply chain and this may be too late for the obligation to be effective.

Because of the scope of data protection law, the obligation to data protection by design is only applicable for the data controller from the moment that personal data are collected and processed. In a case of a drone or remotely piloted aircraft, this would be once the drone is ready to use by the drone operator. However, the drone operator (data controller) comes very late and has no influence in the choice of the components or of the apps chosen to operate the drone. Such decisions that take place during the development phase of the drone, such as whether to integrate automated deletion or to insert a visible sign that its camera is "on" are taken by providers of drones or of its components (sensors, cameras etc.) who act earlier in the supply chain and are excluded from the scope of the data protection framework. "Even though their technologies can (and will) be used to process personal data and even if they can reasonably expect that their technology may severely impact individuals' rights to privacy and data protection, they are not bound to respect the principles of data protection" (Tsormpatzoudi & Coudert, 2015b).

This issue has been identified has been extensively discussed in the GDPR. Eventually the compromise text (Recital 61) requires that technology providers, when developing, designing, selecting and using applications, services and products, shall "be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations". Even though it is not worded as a clear obligation, these actors, in addition to the data controllers, should be responsible for PbD implementation.

Standardisation may be a way to clarify and implement PbD in the supply chain. The standardisation request in the Commission's Implementing Decision M530/2015 explicitly refers to a standard for privacy management in the design, development, production, and service provision processes of security technologies (European

Commission, 2012). Standardisation, followed by relevant certification, is expected to become increasingly important, as the compromise text of the GDPR specifically refers to an approved certification mechanism as an element to demonstrate compliance with data protection by design and by default (Article 23 (2a) Council of the European Union, 2015).

5.3 Education: PbD teaching and training

As the previous sections have shown, the implementation of PbD by all relevant stakeholders (companies, technology or component providers, the public at large) requires an *awareness* of the relevance of the issue and of the challenges posed by a multi-discipline, multi-stakeholder concept. It also requires *knowledge* of concepts and methods: for example, which legal rights and values are to be protected (and what counts as protection), which methods and technologies are currently available to process data while ensuring these protections, how available, usable and economical these are, how to deal with the tradeoffs necessitated by conflicting interests, etc. Last but not least, PbD requires *skills* for transforming this knowledge into action.

Books and other materials alone are ill-suited to creating complex meshes of awareness, knowledge and skills, the more so for concept under continuous development such as PbD. We therefore argue that the development, testing and improvement of teaching and training methods is vital for transporting lessons learned about PbD – such as those described above – into practice. As an outlook, we therefore want to illustrate what we consider key elements of such teaching/training, using two case studies from our own work.

The first case study was a lesson series given to computer science Masters students (Berendt & Coudert, 2015). It involved a collaboration between two courses at KU Leuven during the last third of the semester. In the first course, student teams had developed and begun to carry out a project in which they started from a research question, gathered data from the Web, and analysed it with statistical and data-mining methods. In the second course, students had been instructed on privacy from various disciplinary perspectives, including an introduction to the legal view of privacy and data protection. The students grouped themselves into "developer teams" and "consultancy teams", respectively. For the assignment, each consultancy team specified a possible app that could be built based on one developer team's data-analysis project. The consultants then worked out an "initial privacy impact assessment (PIA) and design advice" based on guidelines that (a) helped them draw on their computational and legal knowledge and (b) were inspired by existing PIA guidelines (Coudert & Berendt, 2014).

This resulted in good presentations and discussions and some excellent written reports. Of course, the analysis was not perfect, but we were surprised to find that the description of data flows by the consultants was often incomplete or faulty, although this should be a basic skill of computer-science students. We also discovered that even though all developer teams reflected the PIA/design advice input in their final projects, early (privacy-unfriendly) modelling choices could be sticky. Both challenges indicated that learning could profit from either more time or a simpler

assignment. After the successful first run, the second route was chosen: In the current (2015) run of the course, the privacy course students' semester project is to develop a PIA/design advice for an existing online/mobile application in the outside world (rather than a fictitious one that is being developed by their peers).

The second case study was a two-day workshop for IT practitioners, organised in the context of the EU FP7 PRIPARE project. The day started with a Welcome and Introduction, followed by two lectures on Privacy Motivation and Introduction (given by Claudia Roda and Susan Perry) and Data Protection and Privacy Principles (given by Pagona Tsormpatzoudi) and ended with a practical session. The exercise was an assignment covering aspects that were discussed mainly during the session 'Data Protection and Privacy Principles'. Its design was based on the assignment of the first case study.

The exercise was designed in a way that allowed follow-up of the use case presented during the Welcome and Introduction of the Participants. The intention was to use the same case in order to perform the exercises of the workshop. The use case was based on the facts of the Patras pilot on anonymous course evaluation from the EU FP7 Project ABC4Trust (Bcheri et al., 2012). It presented a roughly specified flawed IT solution adjusted as follows: "A university hired an IT professional to provide an online course evaluation solution in order to allow professors receive feedback for their classes. The professional provided a typical IT solution, as presented during the introductory session." The assignment was: "Could you help him specify the solution in a privacy preserving manner? The questions below represent the basic steps of a privacy impact assessment. Please use them to complete the task."

A feedback questionnaire that participants filled out at the end of the workshop illustrated that IT practitioners recognised the topic of the lecture (privacy and data protection law) as very important. On specific aspects, participants considered it useful to learn about data protection principles in a logical order determined by the time of the processing they become relevant. In contrast to the Master students of the first case study, the practitioners were able to identify technical aspects (data flows, who has access to what data). However, they tended to have a narrow perspective when they called upon to identify expectations of the different actors regarding the goals of the system.

Furthermore, the discussions and comments showed that the practitioners had difficulties in working on the basis of a use case that was presented to them with no technical details. The reason for this was that in the PRIPARE methodology the legal assessment takes place only before the technical design and assessment of the solution. As an illustration of the methodology, the 2-days workshop started with the legal training; the technical part followed. Therefore, even though we managed to make legal reasoning more explicit and to improve the way we teach PIA, we think that in order to make this use case more successful, we need interdisciplinary assignments, where law and technology are merged together throughout the design process. These assignments will go beyond the principle that was already applied in this workshop: presenting the data protection principles in a logical order determined by the time of the processing. By this extension, we will be able to guide participants to think of legal aspects at the different stages of the actual design (when they become relevant) and not only on the basis of fictitious examples. Whereas education and

training should be adapted to the needs of each stakeholder group, such an approach may be useful to bring law and technology together.

6 Conclusions

The challenges that we identified in the sections above illustrate that implementation of PbD will play a significant role in organisations' efforts to respect privacy. In the years to come we will come across initiatives to specify and apply the concept of PbD during the design process. PbD specification and implementation will go much beyond systems design and will have an impact at different levels. First, it will affect the whole organisational context including stakeholders with diverse interests from different disciplines; and second, the whole supply chain, starting from the component/technology provider and ending at end users. This is the reason why interdisciplinary work may be useful.

Interdisciplinary work is sometimes difficult and time-consuming. But it is reasonable for research (even if not valued in the respective disciplines' metrics) and to some extent necessary for workable solutions. As "the whole is more than the sum of its parts", interdisciplinary approaches will be useful in order to bring to the market products/services that fulfil the common good and serve end users' needs. Yet, it remains a challenge to inform and educate all stakeholders and engage them in a dialogue that will clarify what their goals behind their stated interests are in each case. Openness to understand the underlying incentives of other disciplines will be the first step to move away from (biased) discipline-specific beliefs and values and embrace truly interdisciplinary methods for research and implementation of PbD in practice.

Acknowledgements

This paper was made possible by the funding of the PARIS project (PrivAcy pReserving Infrastructure for Surveillance), EU FP7, under Grant Agreement n° No: 312504, andof ENISA. We thank Marit Hansen, Dan Bogdanov, Matthias Pocs, David Stevens and Antonio Kung for their inspiring keynote, panel contributions, and discussions during the planning of the session, and the APF 2015 participants for their valuable arguments during the session.

References[2]

Article 29 Data Protection Working Party (2009). *The future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP168,*

[2] All online sources were last accessed on January 6th, 2016.

2009). Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Bcheri , S., Goetze N., Liagkou, V., Pyrgelis, A., Raptopoulos, C., Stamatiou, G., Storf, K., Waengmark, P. & Zwingelberg, H. (2012). *D5.1 Scenario Definition for both Pilots.* ABC4Trust Deliverable

Berendt, B. & Coudert, F. (2015). Privatsphäre und Datenschutz lehren - Ein interdisziplinärer Ansatz. Konzept, Umsetzung, Schlussfolgerungen und Perspektiven. [Teaching privacy and data protection - an interdisciplinary approach. Concept, implementation, conclusions and perspectives.] In *Neues Handbuch Hochschullehre. [New Handbook of Teaching in Higher Education]* (EG 71, 2015, E1.9) (pp. 7-40). Berlin: Raabe Verlag.

Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles.* Toronto, Ontario, Canada: Information and Privacy Commissioner of Ontario. (Revised version, originally published 2009). Available at https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf

Coudert, F. & Berendt, B. (2014). *Guidelines for initial privacy impact assessment and related design advice.* http://people.cs.kuleuven.be/~bettina.berendt/teaching/kaw/guidelines.pdf

Council of the European Union (2015). *Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data - Analysis of the final compromise text with a view to agreement.* Presidency to Permanent Representatives Committee, 15 December 2015. Available at http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., & Schiffner, S. (2014). *Privacy and Data Protection by Design – from policy to engineering.* ENISA Report. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

Danish Ministry of Science Technology and Innovation (2005). *Privacy Enhancing Technologies, META Group Report v1.1.* https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf

Diaz, C. & Gürses, S. (2012). Understanding the landscape of privacy technologies. Extended abstract of invited talk in *Proceedings of the Information Security Summit* (pp. 58-63). https://www.cosic.esat.kuleuven.be/publications/article-2215.pdf

European Commission (2007). *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) COM/2007/0228 final (2007).* Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0228

European Commission (2010). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union COM(2010) 609 final.* Available at

http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

European Commission (2012). *Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Security Industrial Policy Action Plan for an innovative and competitive Security Industry Brussels. COM(2012) 417 final.* Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2013.076.01.0037.01.ENG

European Commission (2015). *Implementing Decision of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy, M530 102 final.* Available at http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548

Gürses, F.S. (2010). *Multilateral Privacy Requirements Analysis in Online Social Network Services.* KU Leuven, Dept. of Computer Science: PhD dissertation. https://www.cosic.esat.kuleuven.be/publications/thesis-177.pdf

Gürses, S. & Berendt, B. (2010). PETs in the Surveillance Society: A critical review of the potentials and limitations of the privacy as confidentiality paradigm. In S. Gutwirth, Y. Poullet, & P. De Hert (Eds.), *Data Protection in a Profiled World*. Dordrecht etc., S. 301-321.

Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering Privacy by Design. In *Conference on Computers, Privacy & Data Protection (CPDP 2011)*.

Hansen, M. (2015). *Verabschiedung von Dr. Thilo Weichert und Amtsantritt von Marit Hansen als Landesbeauftragte für Datenschutz Schleswig-Holstein. [Presentation on the occasion of Dr. Thilo Weichert taking leave and Marit Hansen taking office as the Data Protection Commissioner of the German Land Schleswig-Holstein]* Available at https://www.datenschutzzentrum.de/uploads/uld/verabschiedung-weichert/20150903_Hansen_Uebergang-LD_Langtag-Kiel.pdf

Jameson, A., Berendt, B., Gabrielli, S., Cena, F., Gena, C., Vernero, F., & Reinecke, K. (2014). Choice architecture for human-computer interaction. *Foundations and Trends in Human-Computer Interaction, 7(1-2),* 1–235.

Koorn, R., van Gils, H., ter Hart, J., Overbook, P., Tellegen, R., & Borking, J. (2004). *Privacy Enhancing Technologies: White Paper for Decision-Makers.* Ministry of Interior and Kingdom Relations, Directorate of Public Sector Innovation and Information Policy 2004. https://is.muni.cz/el/1433/podzim2005/PV080/um/PrivacyEnhancingTechnologies_KPMGstudy.pdf

Monreale, A., Rinzivillo, S., Pratesi, F., Giannotti, F., & Pedreschi, D. (2014). Privacy-by-design in big data analytics and social mining. *EPJ Data Science, 10.*

Phillips, D.J. (2004). Privacy policy and PETs. *New Media and Society, 6(6),* 691-706.

Schaar, P. (2010). Privacy by Design. *Identity in the Information Society, 3(2),* 267-274.

Tsormpatzoudi P. & Coudert F. (2014). Legal perspective on Privacy by Design. Chapter 3 In C. Troncoso (Ed.): *PRIPARE Deliverable D.5.1 State-of-play: Current practices and solutions* (pp. 22-27). http://pripareproject.eu/wp-content/uploads/2013/11/D5.1.pdf

Tsormpatzoudi P. & Coudert F. (2015a). Gaps in the Legal Frameworks and Lack of Awareness. Chapter 3 In D. Le Métayer (Ed.), *PRIPARE Deliverable D.5.2 Multilateral Gap Analysis: Identification of Research Gaps* (pp. 23-36).

Tsormpatzoudi P. & Coudert F. (2015b). Technology providers' responsibility in protection privacy…dropped from the sky? Paper presented at the *Amsterdam Privacy Conference*, Amsterdam, October 2015..

ULD (1996). *Sommerakademie Datenschutz durch Technik – Technik im Dienste der Grundrechte. [Summer Academy Data Protection by Technology – Technology at the Service of Fundamental Rights.]* https://www.datenschutzzentrum.de/sommerakademie/1996/sa96prog.htm; Summarised in a report available at https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/52DSK-KurzberichtZum_DatenschutzDurchTechnik_.pdf?__blob=publicationFile

van Rossem, H., Gardeniers, H., Borking, J., Cavoukian, A., Brans, J., Muttupulle, N., & Magistrale, N. (1995). *Privacy-Enhancing Technologies, the Path to Anonymity. Volumes I and II.* Registratiekamer, The Netherlands & Information and Privacy Commissioner, Ontario, Canada. Available at https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329 and https://www.ipc.on.ca/images/Resources/anoni-v2.pdf

Wuyts, K. (2015). *Privacy Threats in Software Architectures.* KU Leuven, Dept. of Computer Science: PhD dissertation. https://lirias.kuleuven.be/bitstream/123456789/472921/1/wuyts2014_thesis_online.pdf