WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

The RFID PIA – developed by industry, agreed by regulators

Spiekermann-Hoff, Sarah

Published in:
rivacy Impact Assessment: Engaging Stakeholders in Protecting Privacy

Published: 01/01/2020

Document Version:
Publisher's PDF, also known as Version of record

Document License:
Other

Link to publication

Citation for published version (APA):
Spiekermann-Hoff, S. (2020). The RFID PIA – developed by industry, agreed by regulators. In Springer (Ed.), *rivacy Impact Assessment: Engaging Stakeholders in Protecting Privacy* Springer.

Download date: 20. Apr 2025

1 The RFID PIA – developed by industry, agreed by regulators

Sarah Spiekermann, Professor for Business Information Systems Engineering, Vienna University of Economics and Business (WU Wien)[1]

Abstract - This chapter discusses the privacy impact assessment (PIA) framework endorsed by the European Commission on February 11th, 2011.[2] This PIA, the first to receive the Commission's endorsement, was developed to deal with privacy challenges associated with the deployment of radio frequency identification (RFID) technology, a key building block of the Internet of Things. The goal of this chapter is to present the methodology and key constructs of the RFID PIA Framework in more detail than was possible in the official text. RFID operators can use this article as a support document when they conduct PIAs and need to interpret the PIA Framework. The chapter begins with a history of why and how the PIA Framework for RFID came about. It then proceeds with a description of the endorsed PIA process for RFID applications and explains in detail how this process is supposed to function. It provides examples discussed during the development of the PIA Framework. These examples reflect the rationale behind and evolution of the text's methods and definitions. The chapter also provides insight into the stakeholder debates and compromises that have important implications for PIAs in general.

1.1 Introduction – The history of the RFID PIA

With more technologies penetrating our everyday lives, maintaining the privacy of personal information has become an issue of growing concern. A recent global survey showed that, when prompted, 88% of consumers say that they are worried about who has access to their data; 84% worry about where their data is stored. Most importantly, such concerns are on the rise: 89% state in the same survey that they are becoming more security conscious with their data.[3]

---

[1] I particularly want to thank Wolf-Rüdiger Hansen and Frithjof Walk (Association of Automatic Identification and Mobility, AIM Global), Heinz-Paul Bonn (Federal Association for Information Technology, Telecommunications and New Media, BITKOM), Harald Kelter (Federal Office for Information Security, BSI), Christian von Grone (Gerry Weber), Markus Sprafke (Volkswagen), Gerald Santucci (Directorate General Information Society, European Commission), Johannes Landvogt (Federal Office for Data Protection and Freedom of Information), Barbara Daskala and Udo Helmbrecht (European Network and Information Security Agency, ENISA) as well as Andreas Krisch (European Digital Rights Association, EDRI) and Marie Ötzel (Vienna University of Economics and Business, WU Wien) for their support in the PIA Framework development process. I also want to thank Elizabeth Board (GS1 US) and Marisa Jimenez (formerly GS1) for their co-authorship of the PIA Framework and Paul Skehan (European Round Table, ERRT), Pierre Blanc (Carrefour), Joseph Alhadeff (Oracle, US), Veronique Corduant (Deutsche Post) and Daniel Caprio Jr. (McKenna Long & Aldridge, US) for their active stakeholder involvement.

[2] Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data. Protection Impact Assessment Framework for RFID Applications ; URL: ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

[3] Fujitsu Research Institute,"Personal data in the cloud: the importance of trust", Tokyo, 2010, pp. 8, 13. Fujitsu gathered its data from 500 consumers from each of Australia, Brazil, Canada, China, Finland, Germany, India, Japan, Singapore, Switzerland, the UK and US, for a total of 6,000. The data was gathered between June and September 2010. http://ts.fujitsu.com/rl/visit2010/downloads/Fujitsu_Consumer_Data_Privacy_Report_part2.pdf

Despite these growing concerns, privacy is not holistically regulated or even legally addressed in some countries. Instead, privacy regulation is an international patchwork that fails to establish a common trust framework for people while often forcing companies to incur a high transaction cost for compliance. In times of constant technical evolution, regulation often comes too late, lacks practical enforcement mechanisms and finds itself charged with crippling innovation. In response to this legal dilemma, regulators seek new ways to regulate privacy. Globally integrated, timely and effective privacy protection would be more feasible if global industry players, associations or whole sectors committed to institute common privacy procedures and integrate privacy-friendly architectures and defaults into their systems ("privacy by design").

One promising way to achieve this goal is to avoid regulating the dos and don'ts of specific technologies at a national level; instead, global industry players and sectors could embrace privacy impact assessments (PIA). "A PIA is a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects."[4] If PIAs were mandatory, companies would be forced to proactively investigate and prepare for potentially disadvantageous social implications of the technologies they build and deploy.

PIAs are seen as a particularly promising way to confront the privacy challenges inherent in ambient computer services. PIAs enforce creative thinking about how the ethical challenges of ubiquitous, "always-on" technologies could be addressed; as a result, they stimulate innovation around socially attractive technologies instead of stifling their launch. One ambient technology that has stirred up particularly strong privacy debates and, as a result, became one of the first to be regulated with the help of a PIA, is radio frequency identification (RFID). With other wireless technologies such as Bluetooth or wireless LAN, RFID is a major building block of the "Internet of Things" or "ubiquitous computing environment", envisioned by computer science (CS) researchers[5]. RFID tags embed "smart" chips that communicate with readers and transfer their information to a back-end infrastructure for processing and analysis. The wireless transfer of item information or object-to-object communication is vital for many current services and products, new home and after-sales services, real-time logistics, intelligent manufacturing, and more. In the next decade, it has been estimated that some 87 billion passive tags and 6 million readers will be deployed in Europe.[6]

The reason why RFID has caused particularly strong privacy debates is the combination of three of its technological traits that raise consumer fears: First, humans have always been afraid of the invisible. And this invisibility is manifest in many kinds of RFID that use chips too tiny to be recognised by the human eye, communicating information through fabrics and at long distances (6-8 meters for UHF frequencies) without a line of sight. Second, and unlike many other forms of IT, RFID cannot be "switched off". For mobile phones and PCs, users can opt out of participation, go offline or switch off the device. For RFID – at least for the time being – this is not the case. And last but not least, RFID technology is expected to be

---

[4] Wright, David, "Should privacy impact assessments be mandatory?", *Communications of ACM*, Vol. 54, No. 8, August 2011.

[5] Weiser, Marc, "The Computer for the 21st Century", *Scientific American*, Vol. 265, No. 3, Sept 1991, pp. 94-104.

[6] GS1 and Logica CMG, European passive RFID Market Sizing 2007-2022, Report of the BRIDGE Project, February 2007, p. 8. BRIDGE (Building Radio frequency Identification solutions for the Global Environment) was an Integrated Project funded by the European Commission.
http://www.bridge-project.eu/data/File/BRIDGE%20WP13%20European%20passive%20RFID%20Market%20Sizing%202007-2022.pdf

ubiquitously deployed and present on or embedded in all products and product components carrying barcodes today, which means that the technology will be very pervasive very soon.[7]

Because RFID is a highly promising building block of innovative service delivery, regulators at the EU level have avoided passing the kind of technology-specific "RFID Law" that was considered in the US.[8] The risk of strangling RFID-related innovations was too great. Therefore, calling for PIAs for RFID has been regarded as the ideal political route. In May 2009, the European Commission issued a Recommendation in which it established a requirement for endorsement by the Article 29 Data Protection Working Party of a framework for personal data and privacy impact assessments of RFID applications.[9] This framework was to be developed by industry, but "in collaboration with relevant civil society", according to Article 4 of the Recommendation. The resulting process framework (or "process reference model") "is designed to help RFID Application Operators uncover the privacy risks associated with an RFID Application, assess their likelihood, and document the steps taken to address those risks".[10]

The road to agreement on this PIA framework, finally endorsed by the Art. 29 Working Party in February 2011[11], was a rocky one. The 18 months of political battle can be characterised by two PIA construction phases: Phase 1 led to the submission of an initial PIA Framework draft (PIA I) written under the auspices of GS1.[12] It introduced a distinction between a *PIA framework* as a general outline for RFID PIA and *PIA templates* as concrete implementation guidelines.[13] The draft fell victim to many of the typical pitfalls a PIA design can have: It focused on the general reporting of privacy issues only, avoided any kind of risk identification process, failed to link to any legal system already governing privacy in Europe and was written as a barely structured pamphlet in a language that Norbert Wiener would probably recognise as "forensic discourse".[14] Unsurprisingly, the Article 29 Data Protection Working Party (Art. 29 WP hereafter) rejected the piece as unacceptable.[15]

---

[7] Another "political" reason why RFID has led to such intense privacy debates is the industry's strong push for RFID roll-out and perfection. In particular, the intent to make it the carrier medium of the future barcode has caused privacy rights organisations to become more alert to RFID than other technologies that penetrate markets slowly.

[8] Schmid, Viola, "Radio Frequency Identification Law Beyond 2007" in Christian Floerkemeier, Marc Langheinrich, Elgar Fleisch, Friedemann Mattern and Sanjay E. Sarma (eds.), *The Internet of Things*, Proceedings of IOT 2008, LNCS 4952, Springer-Verlag, Berlin, 2008, pp. 196-212.

[9] European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009) 3200 final, Brussels, 12 May 2009. http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

[10] Privacy and Data Protection Impact Assessment Framework for RFID Applications [the "PIA Framework" hereafter], 11 February 2011, p. 3. http://cordis.europa.eu/fp7/ict/enet/policy_en.html

[11] Art. 29 Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

[12] GS1 is an international association dedicated to the development of global barcode numbering standards and the electronic management of these. It was formed by a merger of the European Article Number (EAN) Association and the Unified Code Council (UCC). GS1 chose RFID as the carrier medium for the barcode system and contributes strongly to the development of the technology. It wrote and edited the initially submitted PIA Framework (called "PIA I" by PIA Framework stakeholders and authors) in co-operation with the European retail industry (represented by the European Retail Round Table Association), a German association called "RFID Informationsforum" (later re-named 'GS1') and a group of other companies.

[13] The Recommendation called for a "framework" and not concrete PIA guidelines. The PIA "Framework identifies the objectives of RFID Application PIAs, the components of RFID Applications to be considered during PIAs, and the common structure and content of RFID Application PIA Reports" (PIA Framework, p. 4). The Framework "could be used as a basis for the development of industry-based, sector-based, and/or application-based PIA templates" (p. 3).

[14] In his influential work on cybernetics, Norbert Wiener distinguishes between two types of language: "one of which is intended primarily to convey information and the other to primarily impose a point of view against a

In Phase 2 of the PIA Framework development, a European group from a variety of industries and academic backgrounds forced the initial authors to outline a methodology that identified privacy risks and mitigation strategies. This group also insisted that the PIA report provide enough details about an RFID application and its back-end infrastructure to allow for a comprehensible identification and judgement of such risks.

As one of the co-authors of the RFID PIA Framework, I describe in this chapter the details of the methodology that was finally endorsed as well as means to apply it. I comment on the purpose and scope of RFID PIAs, the most important procedures, the reasoning behind them, and the meaning of details, definitions, formulations and structure. I also report on the stakeholder challenges overcome, the compromises reached and the lessons learned about PIA construction, at both a technical and political level.

The structure of this article is based on four phases of a privacy impact assessment process for RFID (see figure 1). Some preliminary considerations lead to two main PIA process phases: initial analysis and privacy risk assessment. The initial analysis and privacy risk assessment are accompanied by documentation and reporting.

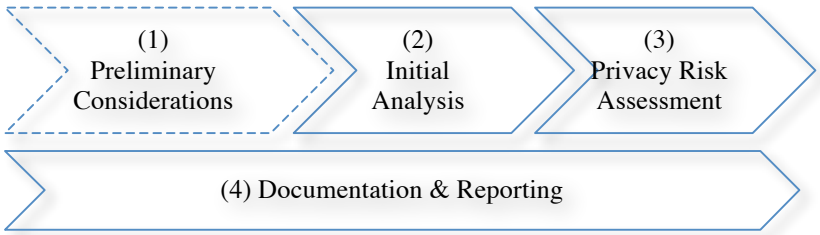

Fig. 1 Process phases of a privacy impact assessment (PIA) for RFID

In this chapter, I define and explain the terms and concepts of the RFID PIA Framework as I understand them as a co-author.[16] Stakeholder discussions are tricky in that conflicting interests can result in "language" (usage of terms) in the final documents that leave room for interpretation. Any material that might be regarded as personal opinion or backroom information is included in the footnotes so it is not confused with the more factual frame of the main text. When I use the term "PIA Framework" in this chapter, I refer to the specific RFID PIA Framework endorsed on 11 February 2011. Official terminology from the RFID PIA Framework appears in *italics* the first time it is used in the text; the spelling of terms also matches the official document. If I excerpt a definition from the Framework, I provide the exact wording and details of the Framework's text in the footnote section. For further information, the reader should refer to the official RFID PIA Framework published by the European Commission[17].

---

wilful opposition". See Wiener, Norbert, *The Human Use of Human Beings: Cybernetics and Society*, Houghton Mifflin, New York, 1950.

[15] Readers interested in the concrete criticisms of PIA I can also consult the collection of documents published by the European Digital Rights Association (EDRI): http://www.edri.org/edrigram/number8.15/article-29-no-to-rfid-pia

[16] My role in this negotiation was that of rapporteur for the European Commission in the first phase of the PIA Framework development. I then led the negotiations for a German industry group in the second phase of the PIA Framework development and co-authored the PIA III Framework.

[17] The European Commission has posted the PIA Framework document as well as key documents that led to the final version on the Web. See http://cordis.europa.eu/fp7/ict/enet/policy_en.html as well as http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm

1.2 Preliminary considerations before engaging in a PIA

Before engaging in the PIA core processes (initial analysis, privacy risk assessment), one must consider a few key points. These include the status of a company deploying RFID as an "RFID operator" in the sense of the PIA Framework (who), the scope of the relevant RFID application (what) and the timing of the PIA (when).

The Commission's Recommendation indicates that *all* RFID operators should assess the impact of their operations on privacy and data protection. It defines an RFID application operator as a "natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an application, including controllers of personal data using an RFID application"[18]. Yet, RFID is a widely used technology that is already embedded in many of today's products and service architectures. Automobiles, for example, contain various RFID applications. RFID gates regularly support manufacturing processes. Ski resorts, public transport companies, toll collectors and event organisers use RFID infrastructures to efficiently manage access controls. As a result, the question is whether all of these RFID operators now and in the future need to immediately consider the privacy implications of their operations. What about tiny retailers or kiosks that may soon use RFID readers only to check out customers, replacing traditional barcode scanners with an RFID system? Are they all equally in need of a PIA? Will every car leaving the factory require a PIA prior to sale, just because it uses RFID for anti-theft protection? The *scope* of the PIA roll-out was a prominent issue in the preparation of the PIA Framework.

The compromise embedded in the PIA Framework is that its procedures will have **no retrospective effect** and **only apply if "significant changes in the RFID application" are made.** The most significant changes are those that "expand beyond the original purposes" of the application, or lead to new "types of information processed; uses of the information that weaken the controls employed".[19] For example, if a fitness club uses lockers with RFID keys and later personalises the keys so that premium members can benefit from the use of their preferred lockers, then the upgrade of the RFID functionality would justify the need for a PIA. The PIA would be needed because the upgrade supplements the original locking function of the system with a customer-relationship function.

In the context of this fitness club example, another aspect of scope becomes apparent: whether the fitness club is the RFID operator responsible for conducting the PIA. After all, fitness clubs are not technology providers; the function and technical architecture of the systems they use are often pre-determined by system vendors. As the goal of a PIA is not only to identify privacy risks, but also to mitigate them technically, can customers implementing an "out-of-the-box" RFID system be held responsible for privacy controls because they are the ones "operating" it? At this point, the definition of the RFID operator becomes important. **The RFID operator is the entity determining the purposes and means of operation.**[20] This is indeed primarily the entity running the RFID application in its premises. However, seen that in many cases these commercial entities are not technically

[18] Recommendation, op. cit., Art. 3(e).

[19] The factors that would require a new or revised PIA include "significant changes in the RFID Application, such as material changes that expand beyond the original purposes (e.g., secondary purposes); types of information processed; uses of the information that weaken the controls employed; unexpected personal data breach with determinant impact and which wasn't part of the residual risks of the application identified by the first PIA; defining of a period of regular review; responding to substantive or significant internal or external stakeholder feedback or inquiry; or significant changes in technology with privacy and data protection implications for the RFID Application at stake" (PIA Framework, p. 5).

[20] See the glossary at Appendix B of the PIA Framework.

prone, it would often need to be the system vendor or system implementer and not necessarily the customer (such as the fitness club owner) who would carry the bulk of responsibility for conducting a PIA. The responsibility of *system* vendors also becomes important when they offer turnkey RFID systems. In this case, system vendors need to conduct PIAs, because they are the ones who determine the purposes and means of those applications. The authors also thought that in cases where RFID systems are tailored to customer needs, then system vendors would have the prime responsibility to inform their customers of the privacy implications of the RFID application and to use (potentially standardised) PIA templates to check for the privacy risks together with them.

Another important issue to consider is *when* a PIA needs to be conducted. What constitutes a significant change of an RFID application? Here the definition of an RFID application becomes important because it outlines the breadth of the system landscape to be watched. An RFID application is "An Application that processes data through the use of tags and readers, and which is supported by a back-end system and a networked communication infrastructure" [PIA Framework, p. 23]. **The consideration of RFID back-end systems' links and sharing networks is important for a PIA kick-off**. It is important because privacy problems often result from the "secondary" processing of data somewhere at the back-end of a system and outside of the particular application that initially collects and uses the data for a specific purpose. For example, a retailer may initially collect, store and process uniquely identified purchase item data for his RFID-enhanced inventory control application. These activities do not cause any privacy concerns. However, when the retailer decides that purchase data items should be forwarded to a back-end loyalty-card system containing customer identities, a privacy problem is created and a PIA or PIA upgrade is warranted. Thus, **the RFID application borders considered for the PIA analysis and kick-off should be understood as the initial application collecting the RFID data <u>plus</u> all those networked communication infrastructures that receive the RFID-based data for additional purposes.**

Finally, a strong concern among stakeholders was whether a PIA would need to be conducted for *every* system and thus potentially *every* product that embeds an RFID application supported by a back-end infrastructure. For example, the automotive industry questioned whether each car containing an RFID-enabled anti-theft functionality supported by dealers' car-owner databases would need a PIA. This would create an unjustifiable cost load to complete manufacturing. The PIA Framework therefore specifies that PIAs need to be done only once for a product series: "If RFID Application Operators reuse one RFID Application in the same way for multiple products, services or processes, they may create one PIA Report for all products, services or processes that are similar" (PIA Framework, p. 6).

1.3 Initial analysis to determine the scope of PIA

Some companies *are* RFID operators in the sense of the Framework but still don't need to conduct a PIA because they simply don't have a privacy problem. These RFID operators have RFID data that is never used for personal data processing or profiling. One only needs to think of a farmer using RFID for tagging his cattle. Furthermore, RFID applications differ in the *degree* to which they entail a privacy risk. For these reasons, an initial analysis can be used by RFID operators to assess whether and at what level of detail they need to conduct a PIA. The decision tree in figure 2 depicts the principal questions an RFID operator needs to consider in documented form for initial analysis.

The key question at the outset of the initial analysis is whether the RFID application actually processes personal data or whether the RFID application links RFID data to personal

data. The issue of linking must be understood in the context of the RFID application definition outlined above: Because the RFID application in the RFID PIA Framework is a broad system infrastructure that includes a data-sharing network at the back-end, one must ask whether that level contains links between RFID data and personal data. For example, a manufacturer may use RFID in manufacturing and for employees' access control. The question is whether these two data sources could be linked at some point to investigate who had access to the manufacturing unit at a specific point in time.

For those who are not privacy experts, it is crucial to note that in the initial analysis phase, "personal data" is understood in a legal sense. A layman would think of personal data as being information about an identified individual – a known person. In the legal sense, however, the definition of personal data is much broader. According to the EU Data Protection Directive, personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[21]

If a company does not handle personal data (right side of the decision tree), it may not need to conduct a PIA (Level 0, no PIA). Companies that do not handle personal data must conduct a PIA only if individuals will carry RFID tags that the companies process. This consideration (Q2b) was developed with a view to retailers who may process tags in their retail outlets that are passed on to their customers. The thinking here is that **the process of using and passing on tags alone creates a responsibility for RFID operators** to check whether they create privacy problems outside their own premises.

If a company does handle personal data (left side of the decision tree) in conjunction with its RFID application (i.e., a retailer using unique purchase identifiers in conjunction with identifiable loyalty card data or a health care system involving patient data in a hospital), it must answer a second question (Q2a) about the personal data on the tags. If personal data is stored in tags, the privacy analysis requires more detail. In fact, **the terminology of "levels" was introduced as an indicator for the level of detail expected for privacy analysis**. The threat environment for privacy breach is enlarged in situations where personal data is not only stored at the back-end of an RFID application, but also directly on the tag. PIAs for these situations need to look at both domains: the back-end and the front-end. **The level terminology does <u>not</u> refer to the level of risk inherent in an RFID application.** In fact, future smart card applications may even benefit from storing more of an individual's information directly on the tag and thus potentially under user control. Even though this kind of RFID application would require a careful a priori privacy analysis (level 3, full-scale PIA), it could be the more privacy-friendly system. After all, privacy scholars agree that decentralised data-processing architectures (ideally under user control) are more privacy friendly than centralised ones.[22]

[21] European Parliament and the Council, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, Art. 2(a).

[22] Spiekermann, Sarah, and Lorrie Faith Cranor, "Engineering Privacy", *IEEE Transactions on Software Engineering*, Vol. 35, No. 1, January/February 2009, pp. 67-82.

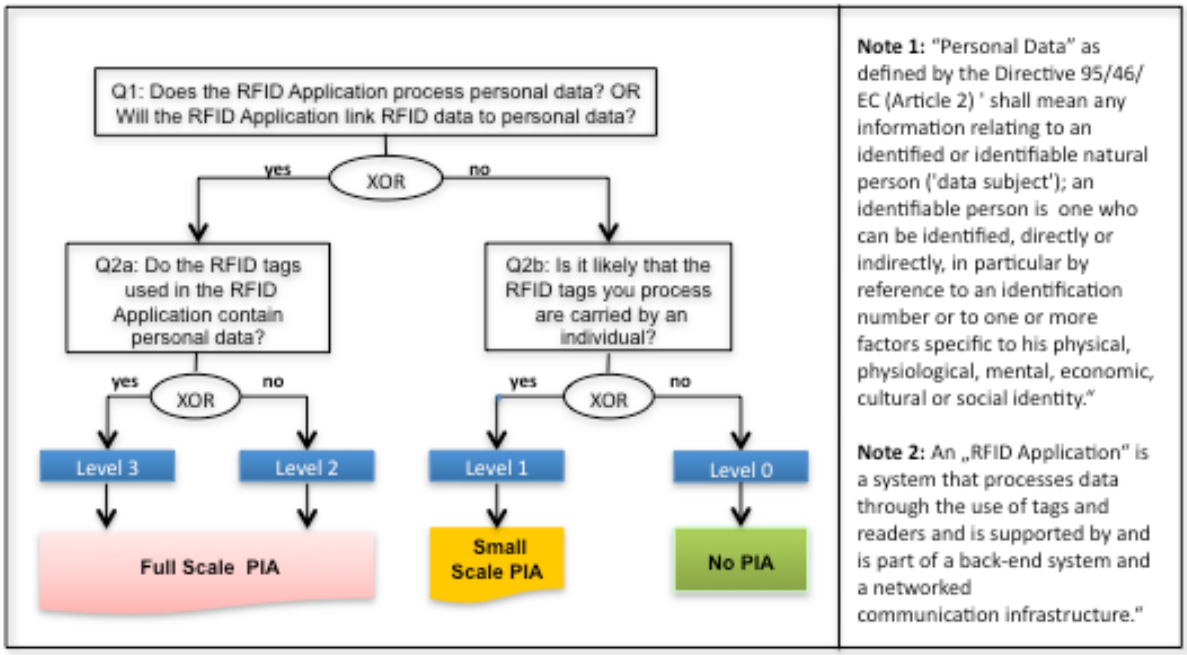

Fig. 2: Initial decision tree on PIA necessity and scope

A recurring question on the initial decision tree is how a full-scale PIA differs from a small-scale PIA. The UK and Canada make a distinction between small scale and full scale for PIAs.[23] This distinction has been made because companies (in particular, small and medium enterprises) that do not process personal data in relation to RFID data should not be overburdened with a privacy analysis, even if they have to take some responsibility for passing tags that are then carried by individuals. An earlier version of the PIA Framework (dubbed "PIA II"[24]) actually contained separate process charts for small-scale and full-scale PIAs. Wright comments: "The phases in a small-scale PIA mirror those in a full-scale PIA, but a small-scale PIA is less formalized and does not warrant as great an investment of time and resources in analysis and information-gathering."[25] During the Framework development discussion, stakeholders suggested that responsibility for conducting a small-scale PIA could probably remain with the person or team who introduced the RFID application; furthermore, a small-scale PIA could dispense with the stakeholder process recommended for a full-scale PIA. Stakeholders also argued that entities developing PIA templates for whole sectors or product- and services lines should certainly run through a full-scale PIA.

Ultimately, the initial analysis must be reported. One pitfall involved in the negotiation of PIA reports with industry is the difficulty of establishing consensus on what needs to be reported in the different phases of analysis. Companies often want to avoid a description of data flows, push for the publication of just a summary about the results of a PIA (as is the case in Canada), or both. Indeed, a major achievement for the RFID PIA Framework is that all of these common pitfalls were avoided. Europe's PIA for RFID now states that the "initial

[23] See respectively [UK] Information Commissioners Office (ICO), *Privacy Impact Assessment Handbook*, Version 2.0, Wilmslow, Cheshire, June 2009, and Office of the Privacy Commissioner of Canada, *Assessing the Privacy Impacts of Programs, Plans, and Policies*, Audit Report of the Privacy Commissioner of Canada, Ottawa, 2007.

[24] Spiekermann, S., *PIA II - A Proposal for a Privacy Impact Assessment Framework for RFID Applications*, Vienna University of Economics and Business, 2011, http://cordis.europa.eu/fp7/ict/enet/policy_en.html, published there under the title: German Industry Alternative Proposal on the RFID Privacy and Data Protection Impact Assessment Framework [21 Oct 2010].

[25] Wright, op. cit.

analysis must be documented and made available to data protection authorities upon request" (PIA Framework, p. 6) and that this documentation not only describes the RFID application at a superficial level, but contains all information needed to judge the potential privacy impact of the system. This requirement implies that the RFID application description must contain detailed information about the method and purpose of data storage, processing and transfer. Table 1 shows what reporting elements must be contained in for an RFID application description according to Annex 1 of the RFID PIA Framework. Most of these information elements are not specific to RFID and may be used in other system contexts.

RFID Application Operator	• Legal entity name and location • Person or office responsible for PIA timeliness • Point(s) of contact and inquiry method to reach the Operator
RFID Application Overview	• RFID Application name • Purpose(s) of RFID Application(s) • Basic use case scenarios of the RFID Application • RFID Application components and technology used (i.e., frequencies, etc.) • Geographical scope of the RFID Application • Types of users/individuals impacted by the RFID Application • Individual access and control
PIA Report Number	• Version Number of PIA Report (distinguishing new PIA or just minor changes) • Date of last change made to PIA Report
RFID Data Processing	• List of types of data elements processed • Presence of sensitive information in the data being processed (health, for instance)?
RFID Data Storage	• List of types of data elements stored • Storage duration
Internal RFID Data Transfer (if applicable)	• Description or diagrams of data flows of internal operations involving RFID data • Purpose(s) of transferring the personal data
External RFID Data Transfer (if applicable)	• Type of data recipient(s) • Purpose(s) for transfer or access in general • Identified and/or identifiable (level of) personal data involved in transfer • Transfers outside the European Economic Area (EEA)

Table 1 – Reporting elements of the initial analysis of an RFID application according to Annex I of the RFID PIA Framework

1.4 PIA risk assessment process

One of the biggest challenges for the PIA stakeholder process was to gain industry consent to a *process* for privacy risk assessment. Running through a proper process and reporting on its individual steps is more time-intensive and costly for companies than writing a report with less stringent requirements. Scholars agree that if PIAs "are conducted in a mechanical fashion for the purpose of satisfying a legislative or bureaucratic requirement, they are often

regarded as exercises in legitimization rather than risk assessment".[26] Coming up with the *right* process for PIAs was difficult because few publicly available, proven examples exist. The difficulty in developing the PIA risk assessment process was that it needed to be concrete enough to help uncover *all* (or at least most) privacy risks while being generic enough to cover all of the ways that RFID technology can be deployed. As with many modern quality management or business continuity activities, "completeness" for this process could only be achieved through a process reference model that enforced the identification of privacy risks and mitigation strategies with its *procedure*.

If the initial analysis concludes that a PIA is necessary and the RFID application description is completed (as described in table 1), the first step of the risk analysis is also completed. The relevant material is gathered and status quo information is available (see figure 2). The next step (step 2) is to identify the privacy risks associated with the RFID application.

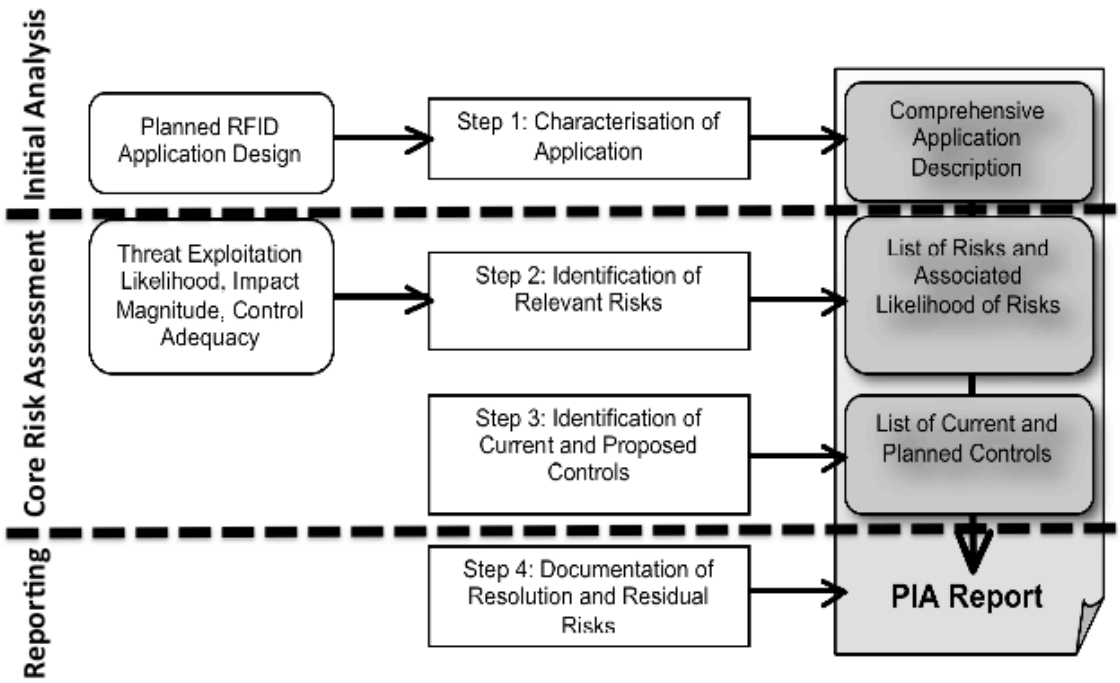

Fig. 3: PIA risk assessment process [PIA Framework, p. 8]

Laymen associate many meanings with the term "risk". But for professional risk assessments, it is vital to embrace a precise and established definition. Most security risk assessments and respective ISO standards used as references[27] for the PIA Framework agree on the following definition of risk: "a function of the likelihood of a given threat-source exercising a particular potential vulnerability and the resulting impact of that adverse event

[26] Wright, op. cit.

[27] These included: International Organization for Standardization (ISO), ISO/IEC 27005 Information technology – Security techniques – Information Security Risk Management, Geneva, 2008; Bartels, C., H. Kelter, R. Oberweis and B. Rosenberg, "Technische Richtlinie für den sicheren RFID-Einsatz", in TR 03126, B.f.S.i.d. Informationstechnik, Bundesamt für Sicherheit in der Informationstechnik, Germany, 2009; European Network and Information Security Agency (ENISA), Emerging and Future Risks Framework – Introductory Manual, Heraklion, 2010; Stoneburner, Gary, Alice Goguen and Alexis Feringa, National Institute for Standards and Technology (NIST), Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30, July 2002.

on the organization".[28] This definition sees the *extent* of risk as a result of three main factors: (1) threats, (2) the likelihood of these threats and (3) their impact magnitude (see left side of figure 2). It is therefore vital to understand whether RFID applications actually *threaten* privacy and with what effects. When risks are assessed, the next step (step 3) in the risk assessment procedure calls for the RFID operators to identify controls that mitigate these risks. The final step (step 4) results in documentation and reflection on what has been done to reduce privacy risks and what remains to be done later (residual privacy risk).

1.4.1 How is the risk assessment done step-by-step?

Even though figure 3 suggests a relatively easy way to conduct the PIA risk assessment, putting this process into practice is not a trivial task. In fact, in order to reach consensus among the negotiating parties of the PIA Framework, a relatively high level of abstraction was chosen in the official document depicting the risk assessment process (Figure 3). That said, there are existing international risk assessment standards that can now be used to translate this overview process (Figure 3) into a practical step-by-step methodology (for example, the method proposed by the National Institute for Standards and Technology (NIST) 2010) can be helpful, even if this process relates exclusively to security assessments).[27] One of the most usable and recognized methodologies to handle the details of the RFID risk assessment has been proposed by the German Federal Office for Information Security (BSI) [BSI2007]. By adhering to the BSI PIA standards outlined hereafter, a company signals its commitment to optimise its security and privacy operations according to timely standards in security management and EU data protection regulation. The step-by-step process that a company would need to run through is depicted in Figure 4. Here it becomes clear that an organisation needs to first understand its *privacy targets*, then analyse how these targets are threatened and finally judge risks based on the situation and existing control landscape (Figure 4). Each step is supported by an explicit keying scheme as well as tables which ensure the rigour of the methodology The next section will outline how to conduct a PIA according to this standard.

[28] Stoneburner, Goguen and Feringa, NIST, op. cit., July 2002, p. 8.

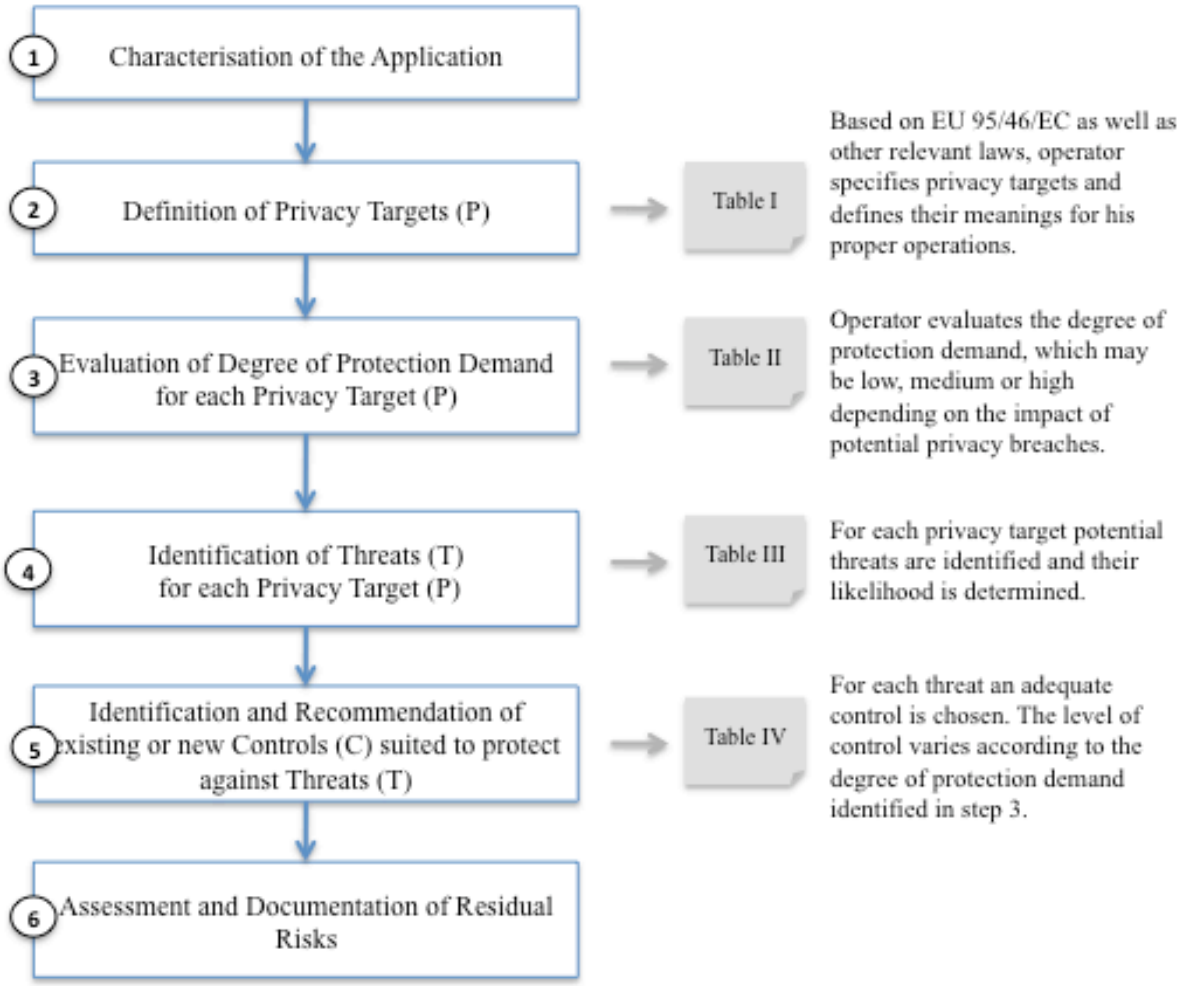

Fig. 4: Full-scale PIA process in detail

Defining privacy targets

The purpose of the risk analysis is to understand what is at risk. What is the privacy protection target? The UK's Privacy Impact Assessment Handbook regards the following aspects of privacy as being at risk and worth protecting: (1) privacy of personal information, (2) privacy of the person, (3) privacy of personal behaviour, and (4) privacy of personal communications.[29] Yet, instead of putting these four privacy targets at the centre of the risk assessment, the PIA Framework consortium opted to take legislation as the starting point of risk analysis. Framed in a legal way, the Data Protection Directive formulates the nine privacy targets summarised in table 2 (and included in Annex II of the RFID PIA Framework). Note that every privacy target can have a key associated with it (P1, P2, … P_N). These keys can later be linked to threats and controls (see Figure 5).[30] The use of a key

[29] ICO, op. cit.
[30] The keys were part of PIA II, but omitted from the official and final PIA Framework document to avoid giving the impression that the Annex tables represent the complete methodology.

structure facilitates systematic risk assessment and is often employed by both privacy and security assessments.[31]

Description of privacy target (taken and updated from the respective EU Privacy Directive(s); here Directive 95/46/EC)	
Safeguarding quality of personal data	Data avoidance and minimisation, purpose specification and limitation, quality of data and transparency are the key targets that need to be ensured.
Legitimacy of processing personal data	Legitimacy of processing personal data must be ensured either by basing data processing on consent, contract, legal obligation, etc.
Legitimacy of processing *sensitive* personal data	Legitimacy of processing sensitive personal data must be ensured either by basing data processing on explicit consent, a special legal basis, etc.
Compliance with the data subject's right to be informed	It must be ensured that the data subject is informed about the collection of his data in a timely manner.
Compliance with the data subject's right of access to data, correct and erase data	It must be ensured that the data subject's wish to access, correct, erase and block his data is fulfilled in a timely manner.
Compliance with the data subject's right to object	It must be ensured that the data subject's data is no longer processed if he or she objects. Transparency of automated decisions vis-à-vis individuals must be ensured especially.
Safeguarding confidentiality and security of processing	Preventing unauthorised access, logging of data processing, network and transport security and preventing accidental loss of data are the key targets that need to be ensured.
Compliance with notification requirements	Notification about data processing, prior compliance checking and documentation are the key targets that need to be ensured.
Compliance with data retention requirements	Retention of data should be for the minimum period of time consistent with the purpose of the retention or other legal requirements.

Table 2: Privacy targets identified in Annex II of the PIA Framework

The PIA Framework consortium took the articles of the Data Protection Directive as its privacy targets for several reasons. Most importantly, it is very useful and sensible to draw privacy threats from existing legal frameworks and thereby combine a PIA with a legal compliance check. While scholars tend to distinguish PIAs from compliance checks and privacy audits[32], the stakeholder negotiation over RFID PIAs cast doubt on the value of this distinction: taking privacy legislation as a starting point for privacy threat analysis saves companies cost and time.[33] **If a company commits to invest in a (potentially cost intensive)**

[31] Bartels, Cord, Harald Kelter, Rainer Oberweis and Birger Rosenberg, TR 03126 – Technische Richtlinie für den sicheren RFID-Einsatz, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2009; ENISA, Emerging and Future Risks Framework – Introductory Manual, op. cit.; ENISA, Flying 2.0 – Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology, Heraklion, 2010.

[32] Wright, op. cit.

[33] In fact, combining the RFID PIA process with a legal privacy compliance check was an important reason why major industry bodies got involved in the RFID PIA Framework definition in its second phase. The argument was that, especially for small and medium enterprises, investing in privacy issues twice – once for PIA and again for legal compliance – was unjustifiable.

PIA, the minimum outcome it expects is the legal compliance of its operations. It should be noted that the PIA Framework stakeholder group did not view the EU's Data Protection Directive as the only valid privacy target; the group also considered that its RFID PIA approach was sufficiently flexible to take into account other relevant jurisdictions, depending on where PIA will be used (e.g., in the US). An alternative set of rules could, for example, be the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[34] Taking current privacy laws as privacy targets makes the risk assessment process timely and adaptable for various regions.

Making legal privacy rights the targets of privacy analysis also has practical benefits: Many PIA processes start with a difficult discussion of what privacy actually is in order to define what needs protection. Yet, as Lillian R. BeVier notes, "Privacy is a chameleon-like word, used denotatively to designate a range of wildly disparate interests – from confidentiality of personal information to reproductive autonomy – and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name."[35] As a result, stakeholder discussions about privacy targets can be lengthy and frustrating. Such discussions also risk producing an incomplete list of privacy issues that is more compromised than complete. The law, in contrast, is an undisputable common denominator that leads to acceptance of the resulting risk assessment.

Taking legislation as a central starting point to define privacy targets also produced some valuable insight on how a PIA is different from a security risk assessment. In fact, security agencies such as the German BSI have been among the first organisations to look into the security of RFID systems and means to identify security risks.[36] They tend to confine privacy targets to those data protection issues that are found in the security domain. Here privacy is typically manifest in four targets: The guarantee of anonymity, pseudonymity, unlinkability and unobservability.[37] Yet, are these privacy targets suited to embrace the privacy rights manifest in European privacy law, such as the *legitimacy* of processing personal data or *data subjects' right* to be informed and have access to her data? No. **Security and data protection targets as found in security risk assessments often do not constitute viable privacy targets as such. However, they may offer the technical means to ensure the safeguarding of confidentiality and security of processing** (as outlined in Articles 16-17 of the EU Data Protection Directive 95/46/EC) **or of the quality of personal data** (Article 6). Consequently, for the purpose of PIAs, security targets can be described as nested within privacy targets. Many privacy targets can be met only if security targets are met.

As mentioned above, legislation was used to constitute the privacy targets in the RFID PIA Framework. Yet taking legislation as the privacy target for PIA also has drawbacks. One is that data protection laws may not cover all of the privacy issues inherent in RFID. Laws often lag behind current technological developments and have varying foci and strengths. For

---

[34] Organization for Economic Co-operation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD, Paris, 23 Sept 1980. http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[35] BeVier, Lillian R., "Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection", *William & Mary Bill of Rights Journal*, Vol. 4, Issue 2, 1995, pp. 455-506 [p. 458]. Cited also in Solove, Daniel J., "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, Vol. 154, No. 3, January 2006, pp. 477- 560.

[36] Bartels, Cord, Harald Kelter, Rainer Oberweis and Birger Rosenberg, TR 03126 - Technische Richtlinie für den sicheren RFID-Einsatz, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2009. As previously mentioned, the German BSI published PIA templates that provide a detailed description of how PIAs for RFID can be conducted for e-ticketing applications in public transport and for events, as well as how they can be used for retail logistics and employee cards. These templates can be accessed for initial guidance at: https://www.bsi.bund.de/cln_165/EN/Topics/ElectrIDDocuments/RadioFrequencyIdentification/TR_RFID/trfid_node.html

[37] See p. 51 in Bartels et al., supra.

example, focus group studies on privacy concerns around RFID revealed that people are afraid of being restricted, criticised or exposed through automatic object reactions.[38] This concern relates to the possibility that RFID technology could be used to "paternalistically" regulate behaviour by observing and correctively influencing interactions with objects. This practice might breach the *physical* right to be let alone[39] as a form of privacy. However, this law is not explicitly regulated by the EU Directive (although it is recognised in US common law); as a result, PIAs using the EU's legal framework as the sole privacy target would probably fail to identify this risk. Some PIA experts therefore advise using the legal framework as a starting point to define PIA targets[40] before questioning whether the list is really complete.

Defining protection demand and importance categories

Even though all privacy targets are equally important vis-à-vis the regulator, some of them will have different degrees of urgency from a company perspective. In security assessments, it is common practice that security targets (i.e., the confidentiality of data) are ranked according to the loss or damage that would result from their potential breach. Such a ranking of targets or formation of protection demand categories is important, because companies or regulators need to be aware of their most important points of system failure and they need to be able to prioritise security investments in those areas.

However, the judgement of the relative priority of security targets is a challenge. The extent of damage can often not be evaluated solely in financial terms. In those cases, "soft" factors must be considered, such as the potential loss of a company's reputation or the social implications for people in their roles as citizens or customers. An informed qualitative judgement of experts is therefore often used to estimate the amount of damage resulting from a security breach. According to this judgement, protection demand categories are formed (for a similar approach, see also BSI2008).

When protection demand categories are formed for ***privacy*** targets, a challenge is that even fewer of them can be represented in monetary terms. For example, it is hard to judge how customers or citizens will react in cases where companies or regulators are not transparent enough, don't describe data processing practices to an adequate extent, etc. Nevertheless, the extent of consequences of privacy breaches should be anticipated for RFID operators as well as for customers of the RFID operator (the "data subjects") in order to get a feeling for the importance and priority of different privacy measures. Customers could lose their social standing, money or even their personal freedom as a result of a privacy breach. But regardless of whether this actually happens or not, companies can also damage their reputation and brand when privacy breaches become known to their customers or the public at large through negative press coverage. RFID operators should, therefore, carefully consider how the breach of different privacy targets could differentially impact their market reputation or lead to financial compensation payments. Based on this judgement, they can prioritise the different privacy targets for their operations. For example, they can form protection demand categories "low – 1", "medium – 2" or "high – 3". In a later state of the risk assessment, such a categorisation can help to choose privacy controls that correspond in strength and vigour.

[38] Spiekermann, S., *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*, Shaker Verlag, Aachen, 2008.
[39] Warren, Samuel, and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. IV, No. 5, 15 Dec 1890.
[40] ICO, op. cit.

Deducing privacy threats from privacy targets

Once privacy targets are identified and prioritized as to their protection demand, they can be used to systematically deduce threats. The core question is how a privacy target is threatened. For example, compliance with a person's right to be informed (P4) may be threatened by secret data collection (T10) or incomplete information about the data collection's purpose (T11). Again, keys (P_4, T_{10}) can be used to systematically link privacy targets to privacy threats. Annex III of the PIA Framework contains a relatively extensive but incomplete list of potential threats with RFID-specific examples. Depending on the industry and the RFID application at hand, RFID operators can pick and comment on the potential threats from this list that are relevant to their operations. Alternatively, RFID operators may also need to add other threats that are more meaningful to them. Sector-specific PIA templates, which will be developed from this framework and for use in different industries, may inform threat identification in greater detail. Figure 5 visualises the link between privacy targets and threats with the help of keys.

Table I

Privacy target code and name	
P1	Safeguarding quality of personal data
P2	Legitimacy of processing personal data
P3	Legitimacy of processing *sensitive* personal data
P4	Compliance with the data subject's right to be infor
P5	...

Table II

T7	Threat codes and names	P2	....
T8	Invalidation of consent	P2	Consent has been obtained under threat of disadvantage. Example: Cannot return/exchange/use warranties for products when RFID tag is deactivated.
T9	Invalidation of explicit consent	P3	Consent has not been given explicitly. Example: Must accept an RFID based access control system to sensitive locations such as labor union offices, toilets, smoking areas, etc.
T10	Secret data collection	P4	Some data is secretly recorded and thus unknown to the data subject, e.g. movement profiles. Example: Consumer is read out while walking in front of stores or in mall and no Logo or Emblem is warning him or her about RFID readouts.
T11	Incomplete information	P4, P8	The information provided to the data subject on the purpose and use of data is not con Example: RFID Information posters t clear information on how RFID data i processed and used.

Fig. 5: Deriving privacy threats from privacy targets systematically

Not all threats given as examples in the PIA Framework Annex III may be equally probable. Many of them will not materialise at all from a specific operator's perspective. An RFID operator must therefore identify those threats that are *likely* to occur in the respective organisation. Threats can occur from within and outside of the particular system at hand and

derive from likely uses and possible misuses of the information. A full-scale PIA would typically involve a stakeholder group identifying threats and determining their likelihood. This group should include the technical staff responsible for the RFID roll-out, managers who will benefit from RFID data, those responsible for data protection of the respective RFID operator (if there is one) and end users of the RFID service. Potentially, additional external stakeholders, such as privacy rights groups, may be consulted. But obviously many companies will be reluctant to do so.

In security risk assessments, threats and their likelihood are identified and judged based on the vulnerability of a system.[41] Vulnerability analysis identifies the technical weaknesses of a system that may be exploited by an attacker. Yet, can this methodology be transferred to a PIA? How does a vulnerability relate to a privacy threat? In preparing the PIA Framework, the authors found that RFID operators may fail to meet the privacy targets of the legal environment due to two kinds of threats: (1) threats caused by neglect of privacy-friendly practices and (2) threats caused by the exploitation of a RFID system's technical vulnerability. Consequently, in the privacy context, threats can originate in the technology or stem from poor privacy management. The threat analysis of a PIA can benefit by systematically distinguishing between these two kinds of threats.

One threat of particular concern in the RFID context is the potential *secrecy of data collection* that may undermine a data subject's right to be informed that an RFID is being used. The rating of privacy threats should therefore consider the read-range difference, which depends on the type of RFID technology used. Different frequencies make it more or less likely that secret tracking of RFID tags can take place and therefore cause a greater or lesser number of privacy threats. For example, the UHF frequency entails a potentially higher privacy threat than HF or LF. Proximity technology (ISO/IEC 14443) causes fewer privacy threats than vicinity technology (ISO/IEC 15693). Nevertheless, independent of the technology, it is also necessary to consider how easy it is to get the reader in the vicinity of the tag without drawing attention to it.

Finally, a prime subject of debate is the threat that RFID tags could be used to profile or track individuals.[42] The RFID tag's information – in particular its identifier(s) – would be used as a sort of "cookie" to re-recognise, profile and track an individual. Retailers who pass RFID tags to customers without automatically deactivating them at check-out *may* unintentionally enable this threat. For this reason, the EC's Recommendation contains a special retail section that is repeated in the RFID PIA Framework. It states:

> A risk that has caused a prime subject of debate is that RFID Tags could be used for the profiling and/or tracking of individuals. In this case the RFID Tag's information – in particular its identifier(s) – would be used to re-identify a particular individual. Retailers who pass RFID Tags on to customers without automatically deactivating or removing them at the checkout *may* unintentionally enable this risk. A key question, though, is whether this risk is likely and actually materialises into an *undismissable* risk or not. According to point 11 of the RFID Recommendation, retailers should deactivate or remove at the point of sale tags used in their application unless consumers, after being informed of the policy in accordance with this Framework, give their consent to keep the tags operational. Retailers are not required to deactivate or remove tags if the PIA report concludes that tags that are used in a retail application and would remain operational after the point of sale do not represent a likely threat to privacy or the protection of personal data as stated in point 12 of the same Recommendation. Deactivation of the tags should be understood as any process that stops

[41] Stoneburner, Goguen and Feringa, NIST, op. cit.

[42] Guenther, Oliver, and Sarah Spiekermann, "RFID and the perception of control: the consumer's view", *Communications of the ACM*, Vol. 48, Issue 9, 2005, pp. 73-76.

> those interactions of a tag with its environment which do not require the active involvement of the consumer [PIA Framework, p. 9].

The PIA Framework authors and stakeholders debated at length about whether and how the PIA Framework should contain clear guidance for the retail sector on when to deactivate. All agreed that the "likelihood" of this profiling and tracking risk depends on three main factors: (1) the volume of RFID readers that RFID operators use officially outside a retailer's premises that gather RFID tags' data in a way the individual cannot control, (2) the volume of RFID tags passed on to customers that are "left on" and (3) the number of malicious attackers that will regularly and personally spy on consumers' assets. Furthermore, all retail stakeholders involved in the negotiations agreed to abstain from the reading of "foreign" tags as part of their PIA controls. If foreign tags were processed, they agreed that they would need to use privacy-by-design methods to mitigate the creation of personally identifiable data from tag information. They argued that either of these two control methods would sufficiently mitigate the threat of uncontrollable profiling or tracking, making the risk "dismissible" (not likely enough to require deactivation). This agreement was supposed to be included in a separate "Deactivation Annex" in the PIA Framework.

What retail stakeholders could not agree on, unfortunately, was a threshold level at which the volume of left-on RFID tags is so high that deactivation becomes a necessity. One retailer suggested that the threshold level would be reached when retailers use RFID tags for anti-theft purposes and thus embed dual-functionality RFID tags in all products that they seek to protect. At this point, (most) retailers will heavily invest in the RFID infrastructure at their checkout systems; it must be assumed that they would do so only for a reasonably large volume of tags. However, not all retail stakeholders could agree to this "anti-theft" threshold suggestion. Consequently, it was not included in the Annex, leaving this Annex with relatively little material that addresses the "deactivation dilemma". As a result, informal feedback from the WP 29 Technical Subgroup viewed the Annex as an attempt by retailers to get around the deactivation provision. As a further result, the "deactivation decision" was postponed and no information on it was included in the PIA Framework except for a repetition of what was already agreed in the May 2009 EC Recommendation (see above).

Identifying and implementing controls to mitigate privacy risks

The crucial step in the privacy risk assessment process is to identify controls that can help to "minimise, mitigate or eliminate the identified privacy risks" [PIA Framework, p. 10]. First, controls are considered that are implemented already or available for implementation. This helps operators judge real threats and their likelihood. Then, the identified threats as well as the protection demand level of the respective privacy target should guide the decision on which of the identified controls are relevant and thus need to be implemented. Figure 6 visualises this relationship.

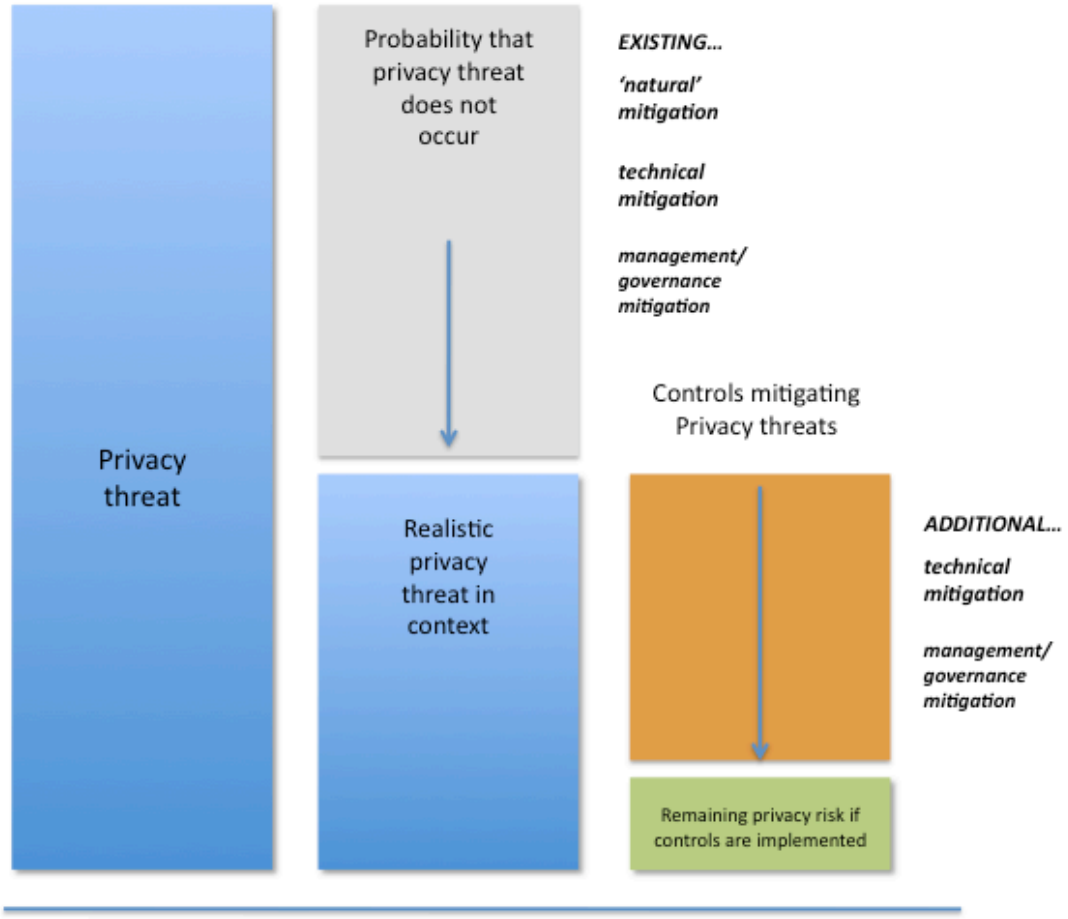

Fig. 6: Assessing and controlling privacy risks

Controls are either of a technical or non-technical nature. Technical controls are incorporated into an application, e.g., access control mechanisms, authentication mechanisms and encryption methods. Non-technical controls, on the other hand, are management and operational controls, e.g., policies or operational procedures. Controls can be categorised as being preventive or detective. Preventive controls inhibit violation attempts, while detective controls warn operators about violations or attempted violations. In the privacy context specifically, it is important to note a category of "natural" privacy controls created by the environment. Natural privacy controls are physical or social artefacts in the environment that enforce privacy-sensitive behaviour simply through the force of their existence. For example, if no readers that can conduct a tracking of items or individuals are physically installed (i.e., because there is no business case for it), then "naturally" there is also no (likely) threat to privacy. Similarly, a social rule to avoid staring at people also acts as a natural privacy control. A list of control examples for RFID is included in Annex IV of the PIA Framework. Many of them were drawn from the catalogue of EuroPrise[43], an entity that helps companies understand how privacy friendly their systems are.

[43] https://www.european-privacy-seal.eu/ See also Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, EuroPrise Criteria, Version 1.0, Kiel, Germany, 2009.

1.5 PIA reporting

To save companies' time, the RFID application description, as outlined in Annex I of the PIA Framework, always constitutes the first part of a more complete PIA report. If this first part reveals that the RFID application under scrutiny processes personal data in relation to RFID or allows for personal profiling with the help of RFID, then a privacy risk analysis must be completed; furthermore, every step of this analysis must be fully documented and included in the PIA report. From an organisational perspective, it is sensible to report conclusions made at each step outlined above in figure 3. Just publishing a summary of the risk analysis is not acceptable under the RFID PIA Framework.

That said, a major point of debate in the PIA negotiation process was the question of who would receive the privacy analysis and to what extent such detailed reports would need to be public. In Canada, for example, government institutions have to post PIA summaries on their website. Companies involved in the RFID PIA negotiations were strongly opposed to the idea that internal data flows and processing operations might leak outside the company or even be exposed to competitors. This issue is of particular concern where RFID is used to enable product functionality through the technology's object-object recognition capability (e.g., in-car communication). Here company-internal innovation processes and legitimate competitive secrecy conflict with the ambitions of privacy reporting.

The compromise reached for RFID PIAs is that **PIA reports will not be public, but must be made available to competent authorities** in line with section IX of the Directive 95/46/EC. This requirement means that, in most cases, a company's data protection official or the department responsible for the RFID deployment will prepare the PIA report for authorities.

The PIA Framework contains an important distinction between reporting and scheduling the PIA process: "Scheduling of the PIA process [shall be] so that there is sufficient time to make any needed adjustments to the RFID Application" [PIA Framework, p. 4]. In contrast, the "PIA Report [shall be made] available to the competent authorities at least six weeks before deployment" [PIA Framework, p. 4]. This distinction is made because the whole purpose and goal of PIAs is "to run through (a) risk assessment phase well before final decisions on an RFID Application's architecture are taken so that technical privacy mitigation strategies can be embedded into the system's design, and do not need to be 'bolted on' later" [PIA Framework, p. 8]. This implies that PIAs need to be kicked off in the early requirements definition phase of an application design or upgrade; the need is also recognised for security engineering (as the above-cited NIST guide makes clear).

1.6 Conclusion

The development and endorsement of the RFID PIA Framework is a great achievement for the European privacy landscape on many grounds. First, one of the technologies that has the most potential to intrude on personal privacy can be controlled through a procedure that promises a relatively complete, holistic and proactive tackling of the problem. The methodology will help RFID operators assess whether, why and to what extent their RFID applications entail a privacy risk; it will also help them identify viable strategies for minimising these risks. Second, the methodology outlined in the Framework leaves companies enough room to adapt it to their industry or their specific conditions. This adaptability, along with the ability to ensure legal compliance by using privacy legislation as the target of analysis, promises a wide acceptance of the PIA Framework methodology. Third, the RFID PIA guide is, to my knowledge, the first PIA guide developed by industry

instead of data protection authorities. It is a result of a true and difficult stakeholder process. It may therefore find wider backing from the industry than a top-down PIA or regulation would receive. Most importantly, it was a true international effort. The Framework was motivated and edited mostly in the EU, but US technology policy-makers influenced it heavily. For this reason, the Framework contains no terminology in the main text that would limit it to European borders. Consequently, some US companies and industry bodies will probably promote its use as well. Finally, the RFID PIA is generic enough to be adaptable to other technologies of the Internet of Things. It can be taken as a starting point or even a blueprint for how to do privacy impact assessments generally.

Despite these promising facts, some challenges lie ahead. The PIA Framework will enter a proof-of-concept phase. All industries using RFID will need to develop PIA templates. Tools are needed to support the methodology. Industry associations will need to set standards for how to go about PIAs in their respective domains. All of this will take time and effort on the part of companies. At this point, the question becomes: to what extent are companies really willing to comply with the rules that they have set for themselves? So far, it is unclear where in an organisation a PIA would be kicked off. Who would typically have the responsibility? And at what points in time do specific criteria require a PIA upgrade?

An open question is also what will happen if companies do not comply with the PIA Framework methodology. Will there be any sanctions? Or could this PIA Framework become mandatory for RFID operators? If not, how can companies be rewarded for their willingness to embrace PIA? Will established privacy seals or auditing companies incorporate the PIA Framework methodology into their controlling operations?

The trade associations who have developed and, most importantly, signed the RFID PIA Framework – GS1, the German Association for IT, Telecommunications and New Media (Bitkom), the Association of Automatic Identification and Mobility (AIM), the European Retailers Round Table (ERRT) and the European-American Business Council (EABC) – will undoubtedly come back with some answers in due course.