2

An Introduction to Privacy

As privacy is a broad concept, the following sections scope the privacy landscape and set out the context in which our work is established.

2.1 Introduction to Privacy

The concept of privacy differs among different communities. This section provides a summary of the definitions and vocabulary that are used as background for our work. Furthermore, this section presents a set of taxonomies that aim to structure the field.

2.1.1 Privacy Definitions

Solove [Sol06] accurately summarized the problem of privacy: "Privacy is a concept in disarray. Nobody can articulate what it means. As one commentator has observed, privacy suffers from an embarrassment of meanings."

Indeed, there exists an abundance of definitions trying to scope the concept of 'privacy.' As there still is no single widely accepted definition, this section summarizes the most referenced definitions.

Warren and Brandeis are considered the first authors of a publication detailing the right to privacy. They define privacy as *"the right to be let alone"* [WB90]. Although the definition originally aimed at the protection of individuals against gossip and slander, through time it has gained a wider meaning. Digital privacy researchers have been interpreting the definition as "an autonomous (digital) sphere in which the data about persons are protected so that unauthorized others cannot access it, also known as data confidentiality" [Gür10]. In this interpretation of privacy, it is hence important to avoid making personal data (i.e. data relating to an identifiable person) available to a larger audience.

Westin, on the other hand, defines privacy as "*the right of the individual to decide what information about himself should be communicated to others and under what circumstances*" [Wes70]. This definition relates privacy to the right to control the information that is revealed to others. This concept is often referred to as information self-determination [Gür10, RP09], as the user himself is able to determine which information he is sharing when and how.

Related to this idea of self-determination is the concept of identity construction. A third definition therefore states that privacy is "*freedom from unreasonable constraints on the construction of one's own identity*" [Agr99]. In the offline world, people will share different information with different people. One will, for example, share different stories with friends, parents, or acquaintances. In the online world, this phenomenon is similar: individuals will want to reveal different information in different contexts.

Nissenbaum [Nis04] introduced '*contextual integrity*' as an alternative benchmark for privacy. This approach requires adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it.

2.1.2 Privacy Vocabulary

This section highlights the privacy-related vocabulary that is used throughout the thesis. We do not intend to propose any definitions ourselves, but we summarize the terms as they are described by the European Data Protection Directive (DPD)[Eur95]. The Directive regulates the protection of individuals with regard to the processing of personal data.

First of all, it is important to note that data protection legislation in particular, but also privacy research in general, is mainly concerned about protecting *personal data* (sometimes also referred to as personal identifiable information or PII). General facts (e.g. the sky is blue) do not require special privacy preservation as they are considered general knowledge. Privacy is person-bound and concerns the protection of data that can be linked to a certain individual (or set of individuals). Personal identifiable information has been defined as "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" [Eur95]. Thus, according to legislation, information does not require privacy protection when it has been anonymized. Note however that in this era of big data, full anonymity is hard, if not impossible [Tuc13]. De-identification (removing pseudo-identifiers) will simply not suffice to anonymize information, and even more advanced anonymity techniques cannot guarantee full anonymity when data are linkable. A more extensive privacy protection will hence be essential.

Another privacy concept related to data processing is '*data subject*.' This refers to the individual that is linked to the personal identifiable information. This is not necessarily the creator of the information. In e-health applications, for example, patient data are created and managed by physicians while the data actually involve a particular patient (i.e. data subject).

2.1.3 Privacy Properties

To have a solid base for the types of privacy threats handled by the proposed LINDDUN framework, we have elaborately studied definitions of privacy properties. In this section, we discuss the set of properties that sets the scope of the privacy domain in this thesis. Most privacy properties in the LINDDUN framework comply with the terminology proposed by Pfitzmann and Hansen [PH10], as it is widely recognized in the privacy research community.

Privacy is sometimes distinguished as *hard privacy* and *soft privacy* [Dan12]. Hard privacy relates to *data minimization*, and is based on the assumption that personal data is not divulged to third parties. The system model of hard privacy is that a data subject provides as little data as possible in order to reduce the need to "trust" other entities. The data subject himself will be the active security party (i.e. is responsible for hiding information).

Soft privacy, on the other hand, is based on the assumption that the data subject has already lost control of his personal data and has to trust the honesty and competence of the data controllers. Soft privacy is mainly achieved by data security (e.g. access control) and regulatory implementations (e.g. policies, consents, purpose-based access and processing, audit, etc.). It will be up to the data controller (i.e. receiver of the information, in general this will be the back-end system) to ensure data protection. Unfortunately, this implies that it will be difficult for the data subject to verify how his data are collected and processed.

The following paragraphs enlist a number of privacy properties that are implemented by LINDDUN and thus are used throughout this thesis.

Unlinkability. Unlinkability refers to hiding the link between two or more actions, identities, and pieces of information. Examples of unlinkability include hiding links between two anonymous messages sent by the same person, two web page visits by the same user, entries in two databases related to the same person, or two people related by a friendship link in a social network.

Unlinkability is defined by Pfitzmann and Hansen. as [PH10]: *"Unlinkability of two or more items of interest (IOIs, e.g. , subjects, messages, actions, etc.) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not."*

Anonymity and Pseudonymity. Anonymity refers to hiding the link between an identity and an action or a piece of information. Examples are the anonymous sender of an email, writer of a text, person accessing a service, person to whom an entry in a database relates, and so on.

Anonymity is defined as: *"Anonymity of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set"* [PH10]. Anonymity can also be described in terms of unlinkability. If one considers sending and receiving of messages as attributes; the items of interest (IOIs) are who has sent or received which message. Then, *"anonymity of a subject with respect to an attribute may be*

defined as unlinkability of this subject and this attribute." For instance, *sender anonymity* of a subject means that to this potentially sending subject, each message is unlinkable. Correspondingly, *recipient anonymity* of a subject means that to this potentially receiving subject, each message is unlinkable.

Pseudonymity suggests that it is possible to build a reputation on a pseudonym and use multiple pseudonyms for different purposes. Examples include a person publishing comments on social network sites under different pseudonyms and a person using a pseudonym to subscribe to a service.

Pfitzmann et al. [PH10] defines pseudonymity as: *"A pseudonym is an identifier of a subject other than one of the subject's real names. Pseudonymity is the use of pseudonyms as identifiers. A subject is pseudonymous if a pseudonym is used as identifier instead of one of its real names."* Pseudonymity can also be perceived with respect to linkability. Whereas anonymity and identifiability (or accountability) are the extremes with respect to linkability to subjects, pseudonymity is the entire field between and including these extremes. Thus, pseudonymity comprises all degrees of linkability to a subject.

Plausible Deniability. Plausible deniability refers to the ability to deny having performed an action that other parties can neither confirm nor contradict. Plausible deniability from an attacker's perspective means that an attacker cannot prove a user knows, has done or has said something. Sometimes, depending on the application, plausible deniability is desirable over non-repudiation (i.e. a security property to ensure accountability). For instance, in an application used by whistleblowers, users will want to deny having ever sent a certain message to protect their safety. Other examples include off-the-record conversations, the possibility to deny the existence of an encrypted file, deny that a file is transmitted from a data source, or deny that a database record belongs to a person.

The relation between non-repudiation and plausible deniability is described by Roe in [Roe97]: *"The goal of the non-repudiation service is to provide irrefutable evidence concerning the occurrence or non-occurrence of an event or action. If we believe that there is a need for this as a security service [...] we must also concede that some participants desire the opposite effect: that there be no irrefutable evidence concerning a disputed event or action."* This "complementary service" is plausible deniability.

In particular, it ensures that "an instance of communication between computer systems leaves behind no unequivocal evidence of its having taken place. Features of communications protocols that were seen as defects from the standpoint of non-repudiation can be seen as benefits from the standpoint of this converse

problem, which is called plausible deniability."

The security property 'non-repudiation' and the privacy property 'plausible deniability' are mutually exclusive. This should however not cause any conflicts, as systems will either require strong non-repudiation properties to ensure accountability, while others will require plausible deniability. For e-commerce applications, non-repudiation is an important security property. Imagine a situation where a buyer signs for a purchased item upon receipt, the vendor can later use the signed receipt as evidence that the user received the item. For other applications, such as off-the-record conversations or online voting, participants may desire plausible deniability for privacy protection such that there will be no record to demonstrate the communication event, the participants and the content. In this scenario, non-repudiation is a privacy threat.

Undetectability and Unobservability. Undetectability and unobservability refer to hiding the user's activities. It is, for example, impossible to know whether an entry in a database corresponds to a real person, or to distinguish whether someone or no one is in a given location.

Undetectability is defined as: "*Undetectability of an item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not. If we consider messages as IOIs, this means that messages are not sufficiently discernible from, e.g. , random noise"* [PH10]. For anonymity and unlinkability, not the IOI, but only its relationship to the subject or other IOIs is protected. For undetectability, the IOIs are protected as such.

Unobservability is defined as: "*Unobservability of an item of interest (IOI) means undetectability of the IOI against all subjects uninvolved in it and anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI*" [PH10]. The definition suggests that unobservability is undetectability by uninvolved subjects combined with anonymity even if IOIs can be detected. Consequently, unobservability implies anonymity, and unobservability implies undetectability. It means, with respect to the same attacker, unobservability reveals always only a subset of the information anonymity reveals. In later sections, we focus on undetectability, since unobservability is in fact a combination of undetectability and anonymity.

Confidentiality. Confidentiality refers to hiding the data content or controlled release of data content. Examples include transferring encrypted email, applying access control to a classified document or a database containing sensitive information.

NIST [MGK09] describes confidentiality as follows: *Confidentiality means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.* Although confidentiality is a security property, as the definition above states, it is also important for preserving privacy properties, such as anonymity and unlinkability. Therefore, confidentiality is also considered an important privacy objective.

Awareness. Although the aforementioned privacy properties are often considered as the core properties, we also consider the following two properties, namely content awareness, and policy and consent compliance, important privacy objectives due to their significance to privacy and data protection. With the emerging of Web 2.0 technologies, users tend to provide excessive information to service providers and lose control of their personal information. Therefore, the awareness property is proposed to make sure that users are aware of their personal data and that only the minimum necessary information should be sought and used to allow for the performance of the function to which it relates.

Awareness is a rather broad concept. Endsley [End95] defined situation awareness as "*the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.*" Awareness in computer-supported cooperative work has been defined as "*an understanding of the activities of others, which provides a context for your own activities*" [DB92]. Sohlenkamp [Soh98] defined awareness as "*an understanding of the state of a system, including past activities, present status and future options.*" In this thesis, awareness refers to an understanding of the consequences of sharing personal information in the past, present and future.

The more personal identifiable information a data subject discloses, the higher the risk is for privacy violation. To ensure awareness, a number of technical enforcement tools have been developed. For instance, the concept of personal information feedback tools has been promoted [LHDL04, PK09] to help users gain privacy awareness and determine themselves which personal data to disclose.

The Platform for Privacy Preferences Project (P3P) [W3C] has been designed to allow websites (as data controllers) to declare their intended use of the information that they collected about the browsing users (as data subjects). P3P addresses the awareness property by making users aware of how personal data are processed by the data controller (i.e. the individual or group who determines the purposes and means of the processing of personal data).

Although not necessarily privacy-oriented, another responsibility of the user, within the realm of content awareness, is to keep user's data up-to-date to prevent

wrong decisions based on incorrect data. This means that the data subject or the data controller (depending on the applications) is responsible for deleting and updating inaccurate information. For example, it is crucial to maintain the patient's data in an e-health application. Imagine a doctor forgetting to mention that the patient is a diabetic, the absence of information could cause fatal consequences for patients taking medication without considering negative side effects on diabetics. Note that the definition of awareness is altered in the improved version of LINDDUN (see Chapter 6). As awareness in the current definition puts quite some responsibility on the user, this will be shifted towards the system side.

Compliance The policy and consent compliance property requires the whole system as data controller to inform the data subject about the system's privacy policy, and allow the data subject to specify consents in compliance with legislation, before users accessing the system. According to the definitions from the EU Directive 95/46/EC [Eur95]: *"Controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."* *"The data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."*

A policy specifies one or more rules with respect to data protection. These are general rules determined by the stakeholders of the system. A consent specifies one or more data protection rules as well, however, these rules are determined by the user and only relate to the data regarding this specific user. The policy and consent compliance property essentially ensures that the system's policy and the user's consent (usually specified in textual form) are indeed implemented and enforced.

This property is also related to legislation. There are a number of legal frameworks addressing the raised concerns of data protection, such as the Health issued the Insurance Portability and Accountability Act (HIPAA) [HIP06] in the United States, the Data Protection Directive 95/46/EC [Eur95] in Europe, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [OEC80].

One example of consent compliance can be found in an e-health context. In some countries, healthcare professionals are only allowed to access medical information if the data subject has given informed consent (or in case of emergency).

There are initiatives to protect data subjects and create openness. It is clearly important to ensure that internal rules actually comply with those promised in

Table 2.1: Summary of privacy vocabulary

Privacy Concept	Description
Personal Identifiable Information (PII)	Information which can be linked back to an individual
Data Subject	Individual that is linked to the PII
Item of Interest (IOI)	information related to an individual (e.g. subjects, messages, actions, etc.)
Unlinkability	Not being able to distinguish whether 2 IOIs are related
Anonymity	Not being able to identify the subject within a set of subjects
Plausible deniability	Being able to repudiate having performed an action
Undetectability	Not being able to distinguish whether an IOI exists
Unobservability	Undetectability against all subjects involved
Confidentiality	Authorized restrictions on information access and disclosure
Awareness	Being conscious about consequences of sharing (PI) information
Compliance	Following regulations and internal business policies

policies and consents. Unfortunately, few technical solutions exist to guarantee compliance. A possible non-technical solution is to use employee contracts to enforce penalties (e.g. , get fired or pay fines) to ensure compliance. Another solution is to hire an auditor to check policies compliance. Eventually, necessary legal actions can be taken by data subjects in the case of non-compliance.

To conclude, we revisit these privacy properties together with the legal vocabulary described in the previous section by summarizing their definitions in Table 2.1 for easy reference.

2.1.4 Privacy Taxonomies

Similar to the myriad of available privacy definitions, there have been several attempts to structure and classify privacy concepts. First we discuss taxonomies that address privacy from a legal perspective. Second, we summarize the privacy classifications that are specifically targeted to software engineering.

Note that we have also created our own privacy taxonomy to classify privacy solutions. It is described in Chapter 6 where it is linked to LINDDUN.

Solove's Taxonomy Solove presents a taxonomy of privacy violations from a legal perspective [Sol06]. Even though the taxonomy does not discuss digital privacy, but describes privacy in general, it provides some useful insights in the matter. Solove makes a distinction between 4 basic groups of harmful activities: information collection, information processing, information dissemination, and invasion.

In the first group, information collection, he included two types of privacy violations: surveillance, which he defines as "the watching, listening to, or recording of an individual's activities", and, interrogation which consists of various forms of probing for information.

The second group of harmful activities, information processing, considers the use, storage, and manipulation of data that have already been collected. It consists of 5 types of violations: aggregation (i.e. combining data related to an individual), identification (i.e. linking data to individuals), insecurity (i.e. carelessness in protecting stored data), secondary use (i.e. using data for a different purpose than it was collected for), and exclusion (i.e. when the data subject is unaware about the data others have about her).

The third group concerns information dissemination and contains 7 violation categories: breach of confidentiality (i.e. not keeping a person's information confidential although promised), disclosure (i.e. revealing truthful 'sensitive' information about a person), exposure (i.e. revealing someone's nudity, grief, or bodily functions), increased accessibility (i.e. amplifying information accessibility), appropriation (i.e. use of one's identity to serve another one's purpose), and distortion (i.e. dissemination of false information).

The final group concerns invasion, and unlike the previous groups, does not necessarily involve personal information. It consists of invasion violations (i.e. invasive acts that violate a person's tranquility) and decisional interference violations (i.e. governmental incursion into a person's private decisions).

FIPPs. The Fair Information Practice Principles (FIPPs) [fip73] are a set of guidelines proposed by the United States Federal Trade Commission. They can be considered the foundation of all current data protection legislation. They, for example, served as basis for the guidelines of the Organisation for Economic Cooperation and Development (OECD) [OEC80], and the European Data Protection Directive [Eur95], among other influences. There are 5 core FIPP categories which can be described as follows:

- Notice/Awareness: Consumers should be properly informed before collecting personal information.
- Choice/Consent: Consumers must be able to choose how their personal information will be used. This holds in particular to secondary use (e.g. registration to a mailing list or transfer of information to third parties).
- Access/Participation: An individual should be able to access data about himself and to contest that data's accuracy and completeness.
- Integrity/Security: Data should be accurate and secure.
- Enforcement/Redress: There should be enforcement measures in place to ensure the FIPPs are being followed. Three alternative approaches have been suggested: self-regulation, private remedies, or government enforcement.

The FIPPs are also used as basis for other privacy taxonomies. Microsoft's Privacy Guidelines [mic08], for example, are based on the core concepts of the FIPPs.

Also, the privacy taxonomy defined by Anton et al. [AER02], which was created to classify and analyze privacy goals and requirements, is based on the FIPPs. However, their framework does not only contain the 5 FIPPs as privacy protection goals, but also includes a set of privacy vulnerability goals that are related to existing threats. These vulnerability goals include information monitoring, information aggregation, information storage, information transfer, information collection, information personalization, and contact.

European Data Protection Legislation. Legislation is a complex matter. It is often vague and formulated in an ambiguous way which makes it very hard to implement. Note that data protection and privacy legislation should not be used interchangeably. De Hert and Gutwirth [DHG06] define privacy as a tool of opacity to limit power by setting normative rules. Data protection, on the other hand, is defined as a tool of transparency to channel and allow power. Data protection legislation is however more in line with the privacy requirements for software systems that are covered in this thesis.

Many claim that trying to hard-code all legislative rules should be avoided, as a techno-regulation only moves the bureaucratic overhead to system developers [KL14]. Privacy does not only require technological measures, but needs organizational measures as well. In addition, it is hard to foresee all potential domains and contexts (and their corresponding regulations) in which a software product will be used. And even if all regulations are properly identified, they

often have a fuzzy, open-ended description. Nevertheless, some of the data protection legislation will impact system requirements, or can, with some minor effort, be incorporated into the system's design.

Guarda and Zannone [GZ09] summarize the *European Data Protection Directive* [Eur95] in the following 9 principles:

1. Fair and Lawful Processing: the collection and processing of personal data shall neither unreasonably intrude upon the data subjects' privacy nor unreasonably interfere with their autonomy and integrity, and shall be compliant with the overall legal framework.
2. Consent: personal data shall be collected and processed only if the data subject has given his explicit consent to their processing.
3. Purpose Specification: personal data shall be collected for specified, lawful and legitimate purposes and not processed in ways that are incompatible with the purposes for which data have been collected.
4. Minimality: the collection and processing of personal data shall be limited to the minimum necessary for achieving the specific purpose. This includes that personal data shall be retained only for the time necessary to achieve the specific purpose.
5. Minimal Disclosure: the disclosure of personal data to third parties shall be restricted and only occur upon certain conditions.
6. Information Quality: personal data shall be accurate, relevant, and complete with respect to the purposes for which they are collected and processed.
7. Data Subject Control: the data subject shall be able to check and influence the processing of his personal data.
8. Sensitivity: the processing of personal data, which are particularly sensitive for the data subject, shall be subject to more stringent protection measures than other personal data.
9. Information Security: personal data shall be processed in a way that guarantees a level of security appropriate to the risks presented by the processing and the nature of the data.

As the DPD was created in a time where the Internet was still in its infancy, a proposal has been drafted in 2012 that proposes a reform of the current legislation to strengthen online privacy rights [Eur12]. Key changes include the

'right to be forgotten' and the requirement that consents necessary for data processing are given explicitly. The 'right of data portability' allows easier access to one's own data and more transparency about how data are handled is required as well. Also the responsibility and accountability for those processing personal data is increased by applying principles like 'Privacy by Design.'

The *E-Privacy Directive* [Eur02] was enacted in 2002 and supplements the DPD as it focuses on data protection in the digital age. It regulates the electronic communications sector and was amended in 2009 [Eur09]. It is mainly known for requiring the user's consent before storing cookies, and is therefore often referred to as the 'Cookie Directive.' In addition, the directive regulates online spam by imposing an opt-in regime, where unsolicited emails can only be sent with prior agreement of the recipient. Also the storage and processing of both traffic data and location data are included in the Directive. Traffic data should be erased or made anonymous as soon as they are no longer needed for the purpose of the transmission. Processing of these data can only occur when the data are anonymized or when the subscriber has given his consent.

Although data protection legislation is complex and often ambiguous, some rules can be automated in software systems. In recent years, research has emerged that aims at abstracting rights and obligations from legal documents and that provides traceability between (written) privacy policies and their implemented software counterparts [AER02, BA08, SBSCB06, CHCGE10, YA10, AGR14].

Privacy Paradigms. Gürses [Gür10] has classified the privacy technology landscape according to three privacy paradigms: privacy as control, privacy as confidentiality, and privacy as practice.

Privacy as control aims at providing data subjects with a means to control disclosure to their own data. Also organizational means to define and enforce data security policies and prevent abuse of unauthorized access fall into this category. Examples of related technologies include privacy settings, access control and auditing to facilitate appropriate data usage.

Privacy as confidentiality puts less trust into the organizations. This paradigm prevents disclosure of information or at least minimizes the disclosure as much as possible to avoid linkability to the data subject. Example technologies are anonymous authentication protocols and anonymous communication networks.

Privacy as practice focuses more on the social aspect of privacy and aims at make information flows more transparent through feedback and awareness tools. Note that these three paradigms are not mutually exclusive.

Privacy by Design. Privacy by Design [vRGB+95, Cav09, GGTD11] is a concept that was developed in the late 90's by Ontario's Information and Privacy Commissioner Ann Cavoukian. It is an engineering approach that focuses on the entire process starting from privacy and data protection principles.

Privacy should not merely be assured by compliance and regulatory frameworks, as there is no use in hard-coding legal rules if the system itself does not have a solid security and privacy foundation.

Privacy by Design can be accomplished by applying the 7 Foundation Principles:

1. *Proactive not reactive; Preventative not remedial*: Privacy threats should be anticipated and prevented, rather than remedied after they have occurred.
2. *Privacy as default setting*: Privacy should be the standard. Personal data should be automatically protected, even without any actions from the individual himself.
3. *Privacy embedded into design*: Privacy should not be considered as an add-on, but should be embedded in the design and architecture of software systems and business activities in general.
4. *Full functionality - positive sum, not zero-sum*: Privacy should coexist with other business interests. Unnecessary trade-offs should however be avoided (e.g. privacy vs. security or privacy vs. performance). One should strive for a positive sum.
5. *End-to-end security - full lifecycle protection*: Privacy requires security throughout the entire lifecycle of the personal data, ensure secure cradle to grave management of all data.
6. *Visibility and transparency - keep it open*: Privacy objectives and promises stated by the business should be followed and systems should be operating accordingly. These system objectives should also be brought to the users' attention.
7. *Respect for user privacy - keep it user-centric*: Privacy interests of the user are most important, thus measures to empower the user should be applied.

Privacy by Design has been heavily promoted in the privacy community. Indeed, providers have to enable users to better protect their personal data. The approach has already obtained positive results. For example, the roll-out of a smart grid system in Ontario was successful as it included Privacy by Design

principles early on in the development process [Kre13]. The approach does however not always result in a positive outcome. The ELENA project in Germany, which was designed to collect income information for employees, was discontinued even though data protection authorities were already involved in the early stages of the project [Kre13, Sch10]. Despite the privacy requirements that were included, the project was heavily criticized by privacy activists. One of the critiques concerned the inclusion of all data of the conventional paper forms, although the need for some of these data fields was doubtful. This experience illustrates that Privacy by Design cannot be successful when it is reduced to merely an endorsement of security and data protection functionality, without acknowledging evolvable requirements.