Proceedings Paper:
Porcedda, MG orcid.org/0000-0002-9271-3512 (2019) 'Privacy by Design' in EU Law. Matching Privacy Protection Goals with the Essence of the Rights to Private life and Data Protection. In: Lecture Notes in Computer Science. Annual Privacy Forum, 13-14 Jun 2018, Barcelona, Spain. Springer Nature , pp. 183-204. ISBN 9783030025465

https://doi.org/10.1007/978-3-030-02547-2_11

'Privacy by Design' in EU Law.

Matching Privacy Protection Goals with the Essence of the Rights to Private life and Data Protection

Maria Grazia Porcedda[1][0000-0002-9271-3512]

[1] Centre for Criminal Justice Studies, School of Law, University of Leeds, UK
m.g.porcedda@leeds.ac.uk

Abstract. In this paper I tackle the question, currently unaddressed in the literature, of how to reconcile the technical understanding of 'privacy by design' with the nature of 'privacy' in EU law. There, 'privacy' splits into two constitutionally protected rights– respect for private and family life, and protection of personal data– whose essence cannot be violated. After illustrating the technical notion of privacy protection goals and design strategies, developed in the privacy threat modelling literature, I propose a method to identify the essence of the two rights, which rests on identifying first the rights' 'attributes'. I answer the research question by linking the technical notion of privacy protection goals and strategies with the attributes and related 'essence' of the rights to private life and to the protection of personal data. The analysis unveils the need to adjust and further develop privacy protection goals. It also unveils that establishing equivalences between technical and legal approaches to the two rights bears positive effects beyond PbD.

Keywords: Data protection by design; privacy by design; information security canons; protection goals; essence; privacy; data protection; Charter of Fundamental Rights.

1 Introduction

Privacy by design (hereafter PbD), which stems from PETs but has almost supplanted them [1], aims to embed 'privacy' in information technologies, network and information systems and business practice (Cavoukian as in [2]), and possibly also processes and physical design [3].

The PbD challenge launched by Cavoukian [4] has been keenly taken by computer scientists, legal scholars, or a combination of both. Computer scientists have focused on developing technical ‘protection goals’ that embed legal requirements into software and hardware development. This was the case of the authors of the LINDDUN project [5], and of the ENISA Paper on engineering PbD [6].

Legal scholars have highlighted the limitations of PbD requirements stemming from the applicable law. Pagallo [7], Leenes and Koops [1], as well as Schartum [2], argue that it is not possible to hard–wire legal rules in computer systems, notably because legal rules require flexible application [1], [7]. Furthermore, PbD approaches would need to be harmonized with the principle of technology neutrality inherent in the applicable law [1]. Importantly, PbD, whether in its form of a legal provision [1], or a standard [8], should not be seen like a shortcut to ensure automated compliance with data protection principles. Rather, the enforcement of those principles always require the active intervention of individuals [7, 8, 9, 10]. Another inherent constraint in the implementation of PbD principles, rightly observed by Bieker et al., Kamara and Rachovitsa, lays in the fact that ‘privacy’ is a qualified right subject to permissible limitations.

All authors studying PbD call for a multi/interdisciplinary approach taking into account substantive legal understandings of privacy as well as technology and software development [1, 2], [9], [11] to ‘operationalise PbD’. Multidisciplinary approaches see computer scientists joining forces with social scientists. Bieker et al. [10] combine PbD and legal approaches to develop a methodology for impact assessments. As for interdisciplinary approaches, Schartum proposes starting from substantive legal rules to develop a method transforming “privacy rules into computer routines and functions” [2] leading to legally compliant software.[1] Unfortunately, this is easier said than done. Legally, ‘privacy’ is not just a matter of statutory law, but, as noted above, also a right [9, 10], [12]. Yet, international law, which represents the universal framework to respect, protect and fulfil human rights, including privacy, is not immediately translatable into workable concepts for PbD [9]. In the end of the day, the applicable law addressing ‘privacy’ is specific to each jurisdiction.

In the European Union (hereafter EU), which I focus on in this paper, ‘privacy’ splits into two constitutionally protected rights: respect for private and family life, home and communications, and protection of personal data, enshrined respectively in Articles 7 and 8 of the Charter of Fundamental Rights [13]. These rights can be limited, yet, limitations cannot violate the essence of the rights. Just like PbD, there is an ongoing debate about the meaning of the essence of fundamental rights, [14, 15, 16] [31]. While this adds further variables to the search for a workable implementation of PbD, at the same time it can also make the identification of clear rules for PbD in EU law easier.

Thus far, however, scholarship has not linked PbD to the nature of private life and data protection in EU law, that is two rights whose essence cannot be violated. This paper fills the gap in the literature by asking how to reconcile the technical understanding of PbD with the nature of the two rights in EU law. My proposition is to map the

[1] Schartum’s method crosses four legally inspired ‘design techniques’ with four software ‘design elements’. The resulting matrix informs nine-stepped iterations (which he sketches, without unfortunately developing them).

equivalences between the legal concept of the essence of the fundamental rights to private life and data protection with the technical notion of privacy/data protection goals.

The paper develops as follows. In section two, I illustrate existing technical approaches to PbD. In section three, I expound the nature of privacy in EU law and seek to operationalize the two corresponding rights by introducing the concept of the 'attributes'. I propose how to reconcile legal and technological approaches in section four. The analysis shows the need for adjusting and further developing privacy protection goals. In the concluding section I summarize my findings, and advance the idea that establishing equivalences between technical and legal approaches can be applied beyond PbD.

2 Technological Approaches: Protection Goals and Threats to Privacy

Privacy by Design can be seen from two complementary angles. The first is a positive perspective, whereby PbD consists of devising technical and operational rules to protect privacy – a.k.a. protection goals. The second is a negative perspective, which consists in implementing rules to avert threats[2] embodied by technology that could damage data and communications, thereby affecting the rights of individuals. Hence Pbd represents for rules compliance what threat modelling is for rules violation.

The identification of protection goals and threats is derived from well-established approaches to information security. In information security, threats to information, and the corresponding rules or canons of protection, are the two sides of threat modelling for information security, which is performed by analyzing the system to be protected through the lenses of a potential attacker. Threat modelling is part of risk assessment, in turn a part of risk management,[3] which belongs with information security management.

There exist several models of threat modelling [18, 19, 20, 21], but a reference point in the field is Microsoft's STRIDE model [22, 23]. The name is the acronym of the threats that a network and information system could suffer from: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. These threats are the negation of information security canons, chiefly the triad of confidentiality, integrity and availability, a.k.a. CIA [5, 6], and also authentication, non-repudiation, authorization and utility,[4] which are canons that have been acknowledged over time [17], [24, 25]. Spoofing means that the attacker replaces the verified user of a system and is the opposite of authentication. Tampering means corrupting the data and is the opposite of integrity. Repudiation, which is the negation of non-repudiation, means that an action cannot be correctly associated with its origin. Information disclosure consists in making confidential information available to illegitimate recipients, and

[2] Defined by ENISA in [17].

[3] Define by ENISA in [17].

[4] Note that the canon 'utility' is defined by the ITU [24], but not by ENISA.

negates confidentiality. Denial of service means making a service unavailable as otherwise expected, thus negating availability. Finally, elevation of privileges consists in gaining access to a system without having the necessary privileges, which challenges authorization (a.k.a. control).

Identifying threats to personal data protection and confidentiality of communications, and the corresponding rules of protection, can be done by means of threat modelling. However, unlike information security, there is little work on threat modelling in the field of privacy [6]. The LINDDUN project [5] and the ENISA study on engineering PbD [6] fill the gap by defining protection goals. LINDDUN [5] also contains a fully-fledged privacy threat modelling.

2.1 Privacy Protection Goals

As for protection goals, LINDDUN [5] borrows from Danezis the idea that privacy can be either soft or hard. Hard privacy consists in the minimization of disclosure of information; consequently, the individual does not need to rely on the data controller for protection. It is identified with the protection goal of data minimization: the data, which is not disclosed, is secure. Soft privacy consists in the knowledge that information has been disclosed, and thus the data subject has to trust the data controller(s). Then, taking inspiration from the data protection goals identified by Pfitzman, LINDDUN identifies the relevant privacy canons by dividing them into the two categories of hard and soft privacy canons. Hard privacy canons are: ‘unlinkability’, ‘anonymity and pseudonimity’, ‘undetectability and unobservability’, with the addition of ‘plausible deniability’ and ‘confidentiality’. Soft privacy canons are extracted from applicable law and are ‘content awareness’ and ‘policy and consent compliance’ (see Table 1 below). While acknowledging the importance of availability and integrity to privacy, LINDDUN does not explicitly list them.

Differently, in the ENISA study [6], Danezis, Domingo-Ferrer, Hansen [26], Hoepman [27], Métayer, Tirtea, and Schiffner list protection goals starting from the classic information security CIA triad and then add unlinkability, transparency and intervenability. In the absence of a standard [8], I experimentally attempt to merge the two sets of canons. The so-merged protection goals produce: unlinkability (including anonymity & pseudonymity, and undetectability & unobservability), plausible deniability, availability, integrity, confidentiality, transparency (including content awareness and policy consent & compliance) and intervenability, as illustrated and described in Table 1.

Table 1. Privacy protection goals for LINDDUN and ENISA

Privacy canons	LINDDUN	ENISA
Unlinkability	**Unlinkability**: hiding the link between two or more actions, identities, and pieces of information.	Privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context, and that means that processes have to be operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy relevant data outside of the domain. Mechanisms to achieve or support unlinkability comprise data avoidance, separation of contexts (physical separation, encryption, usage of different identifiers, access control), anonymisation and pseudonymisation, and early erasure or data.
	Anonymity: hiding the link between an identity and an action or a piece of information. **Pseudonymity**: to build a reputation on a pseudonym and the possibility to use multiple pseudonyms for different purposes.	
	Undetectability and unobservability: hiding the user's activities (e.g. impossibility of knowing whether an entry in a database corresponds to a real person)	
Plausible deniability	The ability to deny having performed an action that other parties can neither confirm nor contradict (e.g. a whistleblower can deny his actions) [opposite of non-repudiation]	
Integrity	/	The fact that data is accessible and services are operational. (ENISA Glossary)
Confidentiality	Hiding the data content or controlled release of data content (e.g. encrypted email)	The protection of communications or stored data against interception and reading by unauthorized persons. (ENISA Glossary)
Availability	/	The confirmation that data which has been sent, received, or stored are complete and unchanged. (ENISA Glossary)
Transparency	**Content Awareness**: users are aware of their personal data and that only the minimum necessary information should be sought and used for the performance of the function to which it relates.	All privacy-relevant data processing including the legal, technical and organisational setting can be understood and reconstructed at any time. The information has to be available before, during and after the processing takes place. Mechanisms for achieving or supporting transparency comprise logging and reporting.
	Policy and consent compliance: the whole system – including data flows, data stores, and processes – has to inform the data subject about the system's privacy policy, or allow the data subject to specify consent in compliance with legislation, before users access the system	
Intervenability	/	Intervention is possible concerning all ongoing or planned privacy-relevant data processing, in particular by those persons whose data are processed. The objective is the application of corrective measures and counterbalances where necessary. Mechanisms for intervenability comprise established processes for influencing or stopping the data processing fully or partially, manually overturning an automated decision, data portability precautions to prevent lock-in at a data processor, breaking glass policies, single points of contact for individuals' intervention requests, switches for users to change a setting

2.2 Threat Modelling: LINDDUN and ENISA

In LINDDUN [5], each identified privacy protection goal or canon corresponds to a technology threat from which, similarly to Microsoft's STRIDE, the acronym of LINDDUN is derived: **L**inkability, **I**ndentifiability, **N**on-repudiation, **D**etectability, **D**isclosure of information, content **U**nawareness, policy and consent **N**on-compliance, as exemplified in Table 2. Each threat to an item of interest (hereafter IoI), understood variably as a user, action, content etc., is defined from the perspective of the attacker. Thus, 'linkability' means being able to establish whether two IoIs are related. 'Identifiability' means connecting a user to an IoI. 'Non-repudiation' allows proving that a user has performed a given action. 'Detectability' means that an IoI exists. 'Information disclosure' refers to loss of confidentiality. 'Content unawareness' means that either too much, or the wrong information has been disclosed, leading to the identification of wrong decisions. Finally, 'policy and consent non-compliance' indicates the case in which a system disregards the privacy policy it purports to respect.

Table 2. LINDDUN privacy threat modelling

Privacy canons (LINDDUN)	Threats to canons
Hard privacy	
Unlinkability	Linkability
Anonymity and Pseudonimity	Identifiability
Plausible deniability	Non-repudiation
Undetectability and unobservability	Detectability
Confidentiality	Disclosure of information
Soft privacy	
Content awareness	Content unawareness
Policy and consent compliance	Policy and consent non-compliance

LINDDUN follows the same steps as STRIDE (but does not reach the stage of risk analysis). Therefore, the most fundamental step is the identification of data flow diagrams, i.e. the essential sub-units to which the threats are applied [5]. Based on such associations, it becomes easier to study mitigation strategies, e.g. in the form of PETs applying PbD.

Danezis et al. [6] do not explicitly propose a privacy threat model. Yet, the only protection goal identified in the study conducted by Danezis et al. under the aegis of the ENISA [6] that was not considered by LINDDUN is intervenability, the threat to which can be identified, with a good degree of confidence, in non-intervenability, understood as the inability or impossibility to intervene at any level of the system to prevent or mitigate a threat.

Instead of threat modelling, Danezis et al. [6] propose design strategies safeguarding the protection goals which either apply directly to the data (data-oriented strategies) or apply to procedures (process-oriented strategies), following the work of Hoepman. In detail, a system of data processing should first of all (following Gürses, Troncoso and Diaz) minimize the amount of data, hide it from view, store data in separate batches, and aggregate data whenever possible. A system of data processing should enable its controllers to inform individuals whose data are being collected, enforce the rules, and demonstrate their enforcement; moreover, it should enable both controllers and individuals to control how the system works and to question the data.

Some of these practices correspond directly to protection goals: 'inform' corresponds to transparency, 'hide' to confidentiality, and 'control' to intervenability. As a result, they can be easily linked to threats. Yet, the other actions can also be linked to a protection goal, and therefore a threat. 'Separate', whereby data should be processed in compartments, can be connected to the goal of unlinkability. Similarly, 'minimize', whereby only the necessary categories of data are collected, enables pseudonimity (and anonymity). 'Aggregate', which encourages to process data at the highest level of aggregation and hence the minimum degree of detail, also pursues unlinkability. Intervenability is enabled by the strategies 'control', 'enforce' and 'demonstrate', which can be seen as three different stages of intervention. The link between privacy protection goals, design strategies and threats is illustrated in Table 3. Two design strategies could be linked to two different protection goals: control to intervenability and transparency; minimise to unlinkability and transparency (as in LINDDUN's content awareness).

Table 3. Relationship between protection goals, design strategies and threats

Privacy protection goals	Design strategies	Threats
Unlinkability- Anonymity and Pseudonymity -Undetectability and unobservability	Aggregate, minimise, separate	Linkability – Identifiability – Detectability
Plausible deniability		Non-repudiation
Integrity*	Control?	Tampering
Confidentiality*	Hide	Disclosure of information
Availability*		Denial of Service
Transparency	Inform Minimise?	Content unawareness - Policy and consent non-compliance
Intervenability	Control, enforce, demonstrate	Non-intervenability

The authors of LINDDUN [5] did not develop their privacy principles starting from the applicable law, but rather from Solove's list of privacy principles, which conflates privacy (i.e. private life) with data protection. As a result, there are some incongruences in their analysis. For instance, 'non-repudiation' is seen as a threat to privacy. Yet, non-repudiation could be deemed to be a threat only in the case of what the authors call hard privacy, and only when users actively pursue repudiation. In all other cases, non-repudiation is desirable because it is key to the accountability of data controllers. The problem, in my view, derives from conflating private life with data protection, which leads to overlooking their respective subtleties.

Danezis et al. [6] built their system based on the Data Protection Directive [28], and hence with a stronger degree of adherence to EU law. Yet, EU law has evolved since the Directive. First, new legislation has been adopted, which gives meaning to data protection not only as a statutory requirement, but also as a right, clearly independent from the right to private life. Second, both rights demand that additional requirements be taken into account when developing PbD, requirements that I illustrate in the following.

3 Legal Approaches to PbD in EU Law

In the EU, ‘privacy’ splits into two constitutionally protected rights: respect for private and family life, home and communications, and protection of personal data, enshrined respectively in Articles 7 and 8 of the Charter of Fundamental Rights [13]. The two rights are fully independent and tend to be mostly complementary but can also display clashes (as discussed in the conclusions).

To further complicate the matter, the requirement to implement PbD is not contained in the definition of the right, but rather comes from secondary law, i.e. Art. 25 of the General Data Protection Regulation [29] (hereafter GDPR). The GDPR, which implements the right to the protection of personal data, PbD becomes ‘data protection by design’ (hereafter DPbD). Legislation addressing Art. 7 of the Charter, such as the proposed e-Privacy Regulation [30] (which will repeal the e-Privacy Directive), does not contain rules on PbD. Nevertheless, the proposed Regulation is a lex specialis of the GDPR (draft Art. 1(3)). Therefore, the obligation of the controller to implement by design approaches contained in the GDPR should arguably apply to provisions of the e-Privacy Regulation, including those addressing confidentiality of communications that fulfil Art. 7 of the Charter.[5] Moreover, awareness of the interplay between technical and legal approaches to the right to private life has value beyond the application of PbD requirements, as discussed in the conclusions.

Secondly, both fundamental rights are subject to ‘permissible limitations’, i.e. limits defined in Art. 52 (1) of the Charter. Accordingly, the exercise of privacy rights can be limited for the sake of ‘objectives of general interest’ which must be clearly spelled out in the law. An example is Art. 23 of the GDPR, which lists, among others, national security, the protection of judicial independence, as well as the protection of the rights and freedoms of others. Yet, the limitation of both rights cannot violate the ‘essence’ of the rights. There is an ongoing debate about the meaning of the essence of fundamental rights in general, and data protection in particular [14, 15, 16], [31].

As I will argue in section four, any attempt to purse ‘by design’ approaches in EU law needs to come to terms with the dual nature of privacy, as well as the concept of the essence, to which I turn now.

[5] I am grateful to Marc van Lieshout for his comments, which prompted the clarification of this point.

3.1 Operationalizing Legal Approaches: the Essence and Boundaries of Articles 7 and 8 of the Charter

Not only the concept of the essence contained in Art. 52(1) of the Charter is not defined, but also the Court of Justice of the European Union (hereafter CJEU) has yet to provide a univocal interpretation on the matter. In the case law of the right to the protection of personal data, for instance, the CJEU seems to opt for a substantive understanding of the essence [31], that is a specific entitlement enabled by the right; following the case law of the CJEU, this entitlement should be expressed in a rule [31].

In the absence of guidance by the CJEU to identify the essence, I have borrowed the method for selecting the 'attributes' of a right that was developed by the UN Office of the High Commissioner on Human Rights (hereafter OHCHR) in the context of work on indicators [32], a method that was also implemented by the UK Equality and Human Rights Commission on which I rely for private life [33]. Attributes are the intrinsic and distinctive substantive dimensions of a right, which define its boundary; in turn, the essence is the 'core' of an attribute [31]. In other words, appraising the intrusion into fundamental rights entails answering the question: what does that fundamental right mean? It obliges one to perform the exercise, in the abstract, of dissecting the right into its substantive characteristics or attributes. Such an exercise, in turn, allows identifying the essence of the right (through a value-based approach [31]), the intrusion into which is legally prohibited.

In detail, attributes are "a limited number of characteristics of [a given] right." (…). To the extent feasible, the attributes should be based on an exhaustive reading of the standard, starting with the provisions in the core international human rights treaties; (…) the attributes of the human right should collectively reflect the essence of its normative content (...) To the extent feasible, the attributes' scope should not overlap" [32]. Attributes represent the synthesis of what would otherwise be the 'narrative' on legal standards of a human right. Note that I borrow from the OHCHR only the method (which was supported by the Fundamental Rights Agency [34]), and not the understanding of rights, which is rooted instead in EU law.

To be sure, the attempt to identify 'principles' synthetizing the two rights is an approach followed by different commentators, and stems historically from the formulation of both rights (e.g. the fair information principles concerning data protection), as well as the national and international case law on both rights [31]. Nevertheless, the scholars who have attempted the enterprise have neither singled out principles for both Art. 7 and 8 as understood in EU law, nor have they systematically identified the essence [15, 16], [35, 36], leaving an important gap in the literature. In the next two sections I synthetize the steps I followed to elaborate the attributes and essence of the right to respect for private life [12], and the protection of personal data [31]. The identification of attributes and essence is in turn instrumental to link the legal understanding of the rights with the technical approach to DPbD/PbD.

3.2 Attributes and Essence of Article 7 of the Charter

Elsewhere [12] I have distilled the attributes for the right to private and family life starting from the Human Rights Measurement Framework developed by the UK Equality and Human Rights Commission [33] duly modified to take into account the specificity of EU law. Accordingly, Art. 7 of the Charter is read in the light of Article 8 of the European Convention on Human Rights (hereafter ECHR) [37], which represents the minimum standard for the substantive understanding of the right, as well as the benchmark to assess permissible limitations (in harmony with Art. 52(3) of the Charter). I also argue that the scope of the right in EU law is different from Art. 8 ECHR; in particular, Art. 7 does neither concern the protection of personal data, nor physical integrity in the context of medicine and biology as well as environmental protection, which are covered instead by Arts. 3 and 37 of the Charter.

The specific contents of the attributes are refined on the basis of the case law of the following bodies: i) judgments of the CJEU concerning instruments of secondary law which give substance to the rights listed in Art 7; the ECHR, insofar as the scope of the two rights correspond; and iii) the case law of the UN which, according to settled case law, supplies guidelines.

Art. 7 reads "Everyone has the right to respect for his or her private and family life, home and communications. The definition contains four prongs (private life, family life, home and communications) which lead to seven attributes and essence.

The first prong includes those elements that are relevant to develop and maintain one's personality and identity, understood as unique and worthy of equal respect. It includes three sub-attributes.

The first is physical and psychological integrity. This includes the forum internum of the mind, i.e. one's thoughts, feelings and emotions; the forum internum of the body, meaning genetic characteristics and unique physical traits, and the forum externum of the body, that is the right to own one's body and protect it from undesired or forced access to it. This attribute could have as an experimental essence the forum internum of the mind and of the body.

The second is personal social and sexual identity, which consists in the 'forum externum' of mental integrity, which is substantiated in the coherent portrayal of one's personality and identity to the external world. It includes control over one's name, the upkeep of one's reputation, the expression of one's sexual orientation, but also the manifestation of one's beliefs and personality in the form of attitudes, behaviours and clothing. Following the case X and Others ([38], para 46), the expression of one's sexual identity is a good candidate for the essence. In Opinion 1/15 ([39], para 150), the CJEU alludes to the fact that information could constitute the essence of the right, without nevertheless providing clear indications. Further candidates for the essence could be the official recognition of one's original or acquired name, and the faithful social representation of one's identity.

The third is personal development, autonomy and participation, which relates to the partaking of individuals in the democratic society, which is threefold. The first way is the development of one's personality in the spirit of self-determination; the second way is autonomy of one's movements and actions; the third way is participation in the social and political life as one sees fit. All three ways require a minimum degree of control, even if conducted in public, and embody the possibility to develop social relations of an amicable or professional nature. In this sense, this sub-attribute concerns the 'outer circle' of one's life and links with the 'inner circle' of one's family. In the absence of clear indications by the Court, a candidate for the essence could be the absence of secret external constraints.

The second prong of the right, family life, leads to one attribute representing the 'inner circle', one's kin by blood and election, which represents the first mode of existence of individuals in society, which predates the state. It includes horizontal and vertical relationships regardless of their seal of legitimacy, and reside in emotional and material ties with individuals and surroundings. The CJEU pronounced that, for a father, the essence of family life lies in the possibility to apply for the right to custody ([40], para 55). Other candidates include the continuity and recognition of a relationship of care.

The prong 'communications' lies in expressing the ability of individuals to choose with whom and how to share information, and the presumption that information shared privately should remain confidential, regardless of its content and the mode of communication. This includes the expectation that information shared privately will not be used against the individual. In the case Digital Rights Ireland [41], the CJEU found the essence to be "the content of one's [electronic] communications as such" (para 39).

The prong 'home' corresponds to the last attribute, which refers to one's settled and secure place in the community, where individuals can develop ties of an intimate nature and nurture self-determination, far away from the public gaze and undesired intrusion. The essence of this attribute could be found in a minimum zone of physical intimacy (e.g., in a home, the toilet, or the bed).

Table 4. Attributes and essence of Art. 7 of the Charter ('private life')

Attributes of art. 7	Core
PL(1) Physical and psychological integrity	The forum internum of the mind and of the body
PL(2) Personal social and sexual identity	The expression of one's sexual identity (CJEU) Official recognition of one's original or acquired name Faithful social representation of one's identity
PL(3) Personal development, autonomy and participation ('outer circle')	Absence of secret external constraints
Family	For a father, the possibility to apply for the right to custody (CJEU) Continuity of relationship of care Recognition of relationship of care
Communications	The content of one's communications (CJEU)
Home	A minimum zone of physical intimacy

3.3 Attributes and Essence of Article 8 of the Charter

Attempts to identify the attribute and the essence of Art. 8 of the Charter are scant [16] and non-conclusive, as I discuss in [31]. Hence, I identified the attributes and essence of the right to the protection of personal data based on the method developed by the OHCHR, and a value-based approach to the right. Differently from the right to private life, the right to the protection of personal data does not derive from the ECHR, and should be read instead in the light of article 52(2) of the Charter, whereby the interpretation of the CJEU of EU secondary law has preeminent importance in defining the contents of the right.[6] In this case, the case law of the ECHR on Convention 108 [43] (one of the sources of the right) 'supplies guidelines' in accordance with settled case law.

Art. 8 is composed of three paragraphs, which read: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority." The three paragraphs contained in the formulation of the right to the protection of personal data lead to 4 attributes; the rationale is explained in [31].

The fist limb of Art. 8(2) embodies the attribute of legitimate processing. This attribute expresses the expectation for the data subject that the processing must be legitimate, which refers to three interconnected principles stemming from the rule of law, namely fairness and transparency, purpose limitation (& storage limitation), and lawful legal basis. In para 150 of Opinion 1/15 [39], the CJEU found that rules concerning purpose limitation constitute the essence of the right.

The second limb of Art. 8(2) concerns data subjects' rights, which correspond to one single attribute: data subjects' control over their personal data, enabling them to intervene in the processing. It includes the following steps, which should be seen as a range of options available to the data subject depending on the situation: i) accessing the data and obtaining a copy; ii) rectifying inaccurate data; iii) objecting to processing, including profiling; iv) restricting the processing of one's personal data. Whilst the CJEU has yet to identify the essence concerning this attribute, a candidate is the right to access. Milder options are the right to rectify and object to profiling.

Art. 8(3), which concerns oversight, paves the way to[7] the attribute of supervisory authority, which concerns the ability of the individual to claim without hindrance the intervention of an authority for the protection of his or her right. This attribute embodies a form of legal remedy.[8]

[6] This is because the CJEU has found, in ground 69 of Google Spain and Google (42. Judgment of 13 May 2014 in Google Spain and Google, C-131/12, EU:C:2014:317, (2014)), that requirements of Article 8(2) and 8 (3) of the Charter "are implemented inter alia" by provisions contained in the DPD. I justify my argument in [31].

[7] See footnote above.

[8] Note that the CJEU invalidated the Safe Harbour Agreement in Schrems [44] on grounds of disrespect of this requirement, which it found to be the essence of the right to effective judicial

The combination of Art. 8(3), literature and international law [31], could also support the attribute ‘human intervention’, whereby decisions significantly affecting an individual cannot be taken by a machine, and that a human being must be involved in the process. A potential essence of this attribute is the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the automated decision (a requirement poised to become essential with further expansions of datafication and applications of data science).

The last attribute, data security and minimization, stems from secondary law (but is an old fair information principle), but can be linked to Art. 8(1), as it expresses essential components of the right [31]. It embodies the expectation to trust that personal information is protected against risks of a varying nature and likelihood, which could effect physical, material and non-material damage. It further includes the right to communicate the minimum amount of personal data possible for a given purpose.[9] In Digital Rights Ireland (para 40) and Opinion 1/15 (para 150) the CJEU found the essence in the provision of integrity, confidentiality and security safeguards in the legal basis relied upon for the processing of personal data.

As a last note, sensitive data should not be seen as an attribute, nor as the essence of data protection, but rather as a requirement that automatically lowers the threshold of permissible interferences.[10]

Table 5. Attributes of Art. 8 of the Charter (data protection)

Attributes	**Essence**
Legitimate processing	Purpose limitation (CJEU)
Data subjects’ rights	Access (Experimental); Rectification and objecting to profiling (experimental)
Supervisory authority	
Human intervention	The right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision (Experimental)
Security and minimization	The provision of security safeguards in the legal basis relied upon for the processing of personal data (CJEU)

The identification of attributes and essence enables us to link the legal understanding of the rights with the technical understanding of privacy/data protection goals (and related threat scenarios), onto which I move next.

protection enshrined in Art. 47 of the Charter, with no mention to the essence of the protection of personal data.

[9] In the version of this research discussed at the conference, I had proposed ‘minimization and accuracy’ as a separate attribute. While accuracy is very well expressed by the requirement to rectify the data, which is part of data subjects’ rights, the question remains as to whether data minimization should form part of a different attribute. The importance of minimization as a prerequisite for Privacy by Design is well argued, for instance, by Gürses, Troncoso and Diaz [45].

[10] That is, by making the interference of limitations to the right automatically serious.

4 Blending Legal and Technical Approaches to Privacy

Any attempt to pursue ‘by design’ in EU law needs to come to terms with the dual nature of privacy, as well as the concept of the essence. This is because ‘by design’ approaches will always be confronted with privacy and data protection not just as statutory requirements, but as rights, too.[11] The use of personal data-driven technology, in fact, always engenders the competition between the two fundamental rights and objectives of general interests. If the data controller is a private individual, and therefore technology is used for business purposes, the protection of personal data and the right to respect for private life stand in dialogue with the objective of general interest of developing an internal market as well as the rights and freedoms of others, which find joint expression in the controller’s freedom to conduct a business (Art. 16 of the Charter). If the data controller is a law enforcement official, and therefore technology is used to support the fight against crime, the protection of personal data and the right to respect for private life stand in dialogue with the objective of general interest of public security, and the rights and freedoms of others.

To answer the research question, which concerns the way how DPbD/PbD approaches can incorporate the understanding of privacy as two rights and the ensuing requirement of respecting their essence, I propose to map the interaction between protection goals and attributes. Actually, there are more connections between the legal and technical concepts than may appear at first sight: the essence is to law what protection goals are to technology, namely a boundary which cannot be crossed, lest violating the right.

4.1 Legal and technical approaches to private life

As for private life, Table 7 shows the correspondences between privacy protection goals and the attributes for respect for private and family life. The first column to the left lists the attributes. The second column lists the essence relating to an attribute, if any (those found by the Court are marked with the acronym ‘CJEU’, the ones I am proposing are marked as ‘Exp.’ for experimental). The third lists the privacy protection goals, or canons, corresponding to each attribute. The fourth and last column lists the corresponding design strategy.

The attribute of communications concerns the ability to share information with other individuals, under the presumption that information shared privately should remain confidential, regardless of its content and the mode of communication, and with the expectation that information shared privately will not be used against the individual.

[11] I believe this reflection addresses the important point raised by Bieker et al. [10], whereby the risk management performed in the context of technology is different than that performed in the case of privacy rights, because the first enables to factor in some risks, whereas the latter does not. While in abstract this is the case, in practice, particularly in the case of Art. 8, the applicable law allows to factor in a degree of risk. This is the case, for instance, of personal data breaches, which need to be notified only when they entail an appreciable risk to the rights and freedoms of data subjects (Art. 33 GDPR). I articulate the many reasons for this in [46].

The content of communications represents, for the CJEU, an element of essence. This attribute is also of central importance for information security, and corresponds to confidentiality, which possibly carries with it the desirability of plausible deniability, for instance in the case of a whistle-blower wishing to deny her or his actions.

The attribute home, which refers to one's settled and secure place in the community, where individuals can develop ties of an intimate nature and nurture self-determination, far away from the public gaze and undesired intrusion, is also enhanced by confidentiality, e.g. in the case of measures of surveillance (e.g. listening devices, cameras etc.), and thus calls for the design strategy 'hide' particularly in relation to a minimum zone of physical intimacy. Unlinkability, as the strategy 'separate', would enable to discard information violating the essence.

Table 6. Relationship between privacy canons and attributes of article 7

Attributes of Art. 7	Core	Protection goal	Design strategy
Private life	See sub-attributes		/
i.Physical and psychological integrity	The forum internum of the mind and of the body	/	/
ii.Personal social and sexual identity	The expression of one's sexual identity (CJEU) Official recognition of one's original or acquired name; Faithful social representation of one's identity	/	/
iii.Personal development, autonomy and participation ('outer circle')	Absence of secret external constraints	/	/
Family	For a father, the possibility to apply for the right to custody (CJEU) Continuity of relationship of care; Recognition of relationship of care	/	/
Communications	The content of one's communications (CJEU)	Confidentiality [Plausible deniability] Authentication/authorization	Hide
Home	A minimum zone of physical intimacy	[Unlinkability confidentiality]	Separate Hide

4.2 Legal and technical approaches to the protection of personal data

Table 8 shows the correspondences between protection goals and the attributes of personal data protection. The first column to the left lists the attributes of the right. The second column lists cores relating to an attribute, if any (the essence found by the Court is marked with the acronym ‘CJEU’, whereas the essence I proposed is marked with ‘Exp.’, which stands for experimental). The third lists the privacy protection goals, or canons, corresponding to each attribute, while the fourth column shows the design approach corresponding to the protection goal.

The attribute ‘legitimate processing’ includes three requirements, two of which relate to a canon. Fairness and transparency corresponds to transparency (particularly in the LINDDUN sense of policy and consent compliance) in a self-explanatory manner. Purpose limitation, which also expresses a core of the right, relates to confidentiality and the design strategy hide, in that data which is not disclosed to unauthorized parties is less likely to be processed unlawfully. It also relates to unlinkability, in that personal data kept in separate batches, aggregated, or minimized is also less likely to be processed without authorization. Confidentiality and unlinkability would be therefore important canons to comply with the essence.

The attribute ‘data subject’s rights’ as a whole relates to intervenability and transparency (in the LINDDUN sense of content awareness) and the design strategies ‘control’ and ‘inform’. The step ‘access’ relates to intervenability (control) and availability of the data, whereas ‘rectification’ relates to integrity, and non-repudiation of the data. The steps objection, particularly to profiling, and rejection, concern unlinkability; objection calls, in particular, for separation. Rejection could call for minimize (e.g. anonymization of the data), or a new design strategy, e.g. ‘delete’.

Oversight, expressed by two attributes, is linked to intervenability, i.e. the possibility to request and apply corrective measures and counterbalances where necessary, and the design strategy control. Note that intervenability presupposes non-repudiation, which pertains to information security and means the ability to prevent a sender from denying later that he or she sent a message or performed an action, so that liability can be attributed. Intervenability and the related strategy of control would be important requirements to satisfy the experimental notion of the essence I propose here. Note that these findings support an important lesson against believing that DPbD/PbD can be an easy fix to compliance with privacy rights, as expressed for instance by Pagallo [7], Koops and Leenes [1] and Kamara [8].

Security calls for availability, confidentiality and intervenability, and the related design strategies hide and control. Minimization relates to unlinkability (in the self-explanatory form of ‘minimise’).

Finally, sensitive data, which is not, per se, an attribute, but rather lowers the threshold of permissible limitations, is supported by unlinkability and the design strategy separate, as well as confidentiality and the design strategy hide, for the same reasons that apply to the attributes discussed above. In addition, plausible deniability may be very important to protect sensitive data, and hence exercise other rights freely.

Table 7. Relationship between privacy canons and attributes of Article 8

	Attributes of Art. 8	**Essence**	**Protection goals**	**Design strategies**
Legitimate processing	**Lawful legal basis**			/
	Fairness and transparency		Transparency (policy & consent compliance)	Inform
	Purpose limitation	Purpose limitation [CJEU]	Confidentiality Unlinkability Intervenability	Hide Separate (minimize, aggregate) Demonstrate
Data subjects' rights			Intervenability Transparency	Control Inform
	Access	Access [Exp]	Availability Non-repudiation Integrity	
	Rectify			
	Object	objecting to profiling [Exp]	Unlinkability	Separate
	Restrict		Unlinkability	/
Oversight	**i. Supervisory authority***		Intervenability (Non-repudiation!)	Control
	ii. Human intervention	The right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision [Exp]	Intervenability (Non-repudiation!)	Control
Security and minimization	**Security**	CJEU: The provision of security safeguards in the legal basis relied upon for the processing of personal data	Confidentiality Availability, Intervenability	Hide Control
	Minimization		Unlinkability Transparency	Minimize
	Sensitive data: lowers the threshold of permissible interferences		Unlinkability, confidentiality [Plausible deniability]	Separate

4.3 Considerations: essence, attributes and obligations of the data controller

The analysis carried out allows drawing some conclusions. The first is that two design strategies - hide and separate (minimize, aggregate) - and the corresponding protection goals – confidentiality and unlinkability - seem crucial for respecting the proposed notions of the essence of both rights. In addition, respecting the essence of Art. 8 calls for the design strategy control and the protection goal intervenability.

However, in both cases, not all potential notions of the essence seem to be matched by an existing design strategy; similarly, not all attributes seem to be matched by a protection goal. The case could be different, however, if all information security canons (see Section 2) had been taken into account. By means of example, the information security canon ‘utility’, whereby the information is relevant and useful for the purpose for which it is needed [24], links both with the attributes of private life (Art. 7) and the attributes data subjects’ rights and security and minimization (Art. 8). As a result, there is room for further developing privacy protection goals and design strategies.

Moreover, some design strategies described in section 2 seem underrepresented (e.g. enforce, demonstrate). Yet, it does not follow that the missing protection goals and design strategies are superfluous. In the case of data protection, the reason why some protection goals and design strategies are missing is that they express obligations of the data controller. Such duties do not feature in the definition of the right but are actually implied by them in the form of (data protection) principles in the applicable law. For instance, the two attributes of data protection which express oversight relate to the principle of accountability, which links to the protection goal of intervenability, and the strategies ‘enforce’ and ‘demonstrate’. Similarly, the sub-attribute ‘rectify’ relates to the principle of accuracy, which expresses the duty to ensure that data are adequate, relevant and not excessive, which is fulfilled by the protection goal integrity.

The conclusion is that DPbD/PbD approaches should take into account both the definition of the rights, which represent a minimum threshold, and the applicable law which implements the right and lays down corresponding duties. The mapping between protection goals, essence and attributes, should be complemented by an equivalent mapping between protection goals and the obligations of the data controller stemming from the applicable law, as exemplified in Table 8. As a result, further protection goals and design strategies could be added (e.g. to embrace the important principle of minimization [45, 48], or protect the essence).

Table 8. Comprehensive approach to PbD/DPbD

<table>
<tr><th>Essence</th><th>Attribute</th><th>Principles expressed in the law</th><th>Duties of data controller</th></tr>
<tr><td>Protection goal</td><td>Protection goal</td><td>Protection goal</td><td>Protection goal</td></tr>
<tr><td>Design strategy</td><td>Design strategy</td><td>Design strategy</td><td>Design strategy</td></tr>
<tr><td colspan="2"><b>Right</b></td><td></td><td></td></tr>
<tr><td colspan="4"><b>Secondary law</b></td></tr>
</table>

5 Conclusions and further research

In this paper I tackled the question, currently unaddressed in the literature, of how to reconcile the technical understanding of ‘privacy by design’ with the nature of the rights to private life and data protection in EU law, whose essence cannot be violated. My proposition was to map the equivalences between, on the one hand, the legal understanding of the attributes and essence of the fundamental rights to private life and data protection with, on the other hand, the technical notion of privacy protection goals developed in privacy threat modelling.

The analysis unveiled hidden connections between the legal and technical concepts: the essence is to law what protection goals are to technology, namely a boundary which cannot be crossed, lest violating the right. As a result, the identification of the concept of the essence and subsequent linking with privacy protection goals eases the implementation of ‘by design’ approaches in EU. Indeed, the design strategies hide, separate (minimize, aggregate) and control, and the corresponding protection goals confidentiality, unlinkability and intervenability, seem crucial for respecting the proposed notions of the essence of the two rights.

The analysis also showed mismatches between, first, attributes and essence, and second, protection goals and design strategies, suggesting there is a need to further develop the latter, e.g. by considering other information security canons (and related threats), as well as to take a comprehensive approach to PbD/DPbD. This means taking into account both the definition of the rights, which represent a minimum threshold, and the applicable law which implements the right and lays down corresponding duties. Such a comprehensive approach, could be applied beyond building privacy-compliant technology.

First, a comprehensive approach can be used to unveil existing tensions inherent in technological design, not just among protection goals, but also between and among rights. For instance, while non-repudiation can be of crucial importance for personal data protection, it can be problematic for confidential communications, because it negates plausible deniability, which is important for confidentiality (e.g. of a whistleblower). Hence, there can be a clash between personal data protection and private life (which testifies to their independence). Clashes may also appear within a right: plausible deniability may be very important to protect the meta-attribute of sensitive data, and hence exercise other rights freely, but is at odds with the other attributes of the right.

Secondly, a comprehensive DPbD/PbD approach which takes into account also information security canons/threats can underpin tensions in the fight against cybercrimes (understood as data crimes [47]), thus informing the development of informed and sustainable approaches to cybersecurity, as I illustrate in [12] in relation to an off-the-shelf intrusion detection and prevention system for universities.

Finally, the comprehensive approach can be used to perform meaningful impact assessment of technologies (as in [10], [25]) and policies. The attribute and essence can be used as a powerful instrument to capture the granularity of the intrusiveness of technologies and policies addressing public security into any fundamental rights (hence beyond data protection, as discussed in section 3), whilst protection goals and design strategies could be used as a corrective approach, as I intend to show in future research.

Acknowledgements. An early draft of this chapter appeared in a restricted deliverable of the FP7 SURVEILLE project (grant agreement no. 284725), as well as my PhD thesis, partly funded by SURVEILLE. Completion of this chapter was funded by the EPSRC research project "Combatting cRiminals In The Cloud" (CRITiCal - EP/M020576/1).

6 References

1. Koops, B.-J., Leenes, R.: Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. International Review of Law, Computers & Technology 28, 151-171 (2014)
2. Schartum, D.W.: Making privacy by design operative. International Journal of Law and Information Technology 24, 151-175 (2016)
3. International Conference of Data Protection and Privacy Commissioners: Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (The Madrid Resolution). 30th International Conference of Data Protection and Privacy Commissioners, Madrid (2009)
4. Cavoukian, A.: Privacy by Design…Take the Challenge (2010). http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf.
5. Wuyts, K., Scandariato, R., Joosen, W.: LINDDUN: a privacy threat analysis framework. https://people.cs.kuleuven.be/~kim.wuyts/LINDDUN/LINDDUN.pdf
6. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Métayer, D.L., Tirtea, R., Schiffner, S.: Privacy and Data Protection by Design – from Policy to Engineering. ENISA (2014)
7. Pagallo, U.: On the Principle of Privacy by Design and its Limits. In: Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y. (eds.) European Data Protection: in Good Health? Springer (2012)
8. Kamara, I.: Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'. European Journal of Law and Technology 8 (2017)
9. Rachovitsa, A.: Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human right issues. International Journal of Law and Information Technology 24, 374-399 (2016)
10. Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M.: A Process for Data Protection Impact Assessment under the European General Data Protection Regulation. In: Privacy Technologies and Policy. Annual Privacy Forum 2016, LNCS, pp. 21-37. Springer, Heidelberg (2017)
11. Tsormpatzoudi, P., Berendt, B., Coudert, F.: Privacy by Design: From Research and Policy to Practice – the Challenge of Multi-disciplinarity. In: Privacy Technologies and Policy. Annual Privacy Forum 2015, LNCS, pp. 199-201. Springer, Heidelberg (2015)

12. Porcedda, M.G.: Cybersecurity and Privacy Rights in EU Law. Moving beyond the trade-off model to appraise the role of technology. PhD Thesis. European University Institute (2017)

13. Charter of Fundamental Rights of the European Union, OJ C 303/01. vol. Official Journal C 303/01, pp. 1–22, European Union (2007)

14. Brkan, M.: In search of the concept of essence of EU fundamental rights through the prism of data privacy. Maastricht Working Paper (2017)

15. Lynskey, O.: The foundations of EU Data Protection Law. Oxford University Press, Oxford (2015)

16. Tzanou, M.: EU Counter-terrorism Measures and the Question of Fundamental Rights: The Case of Personal Data Protection. PhD Thesis. European University Institute (2012)

17. ENISA, Glossary, available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

18. Microsoft, Threat Modeling, available at: https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx

19. OWASP, Risk Modeling, available at: https://www.owasp.org/index.php/Threat_Risk_Modeling

20. OWASP, Threat Modeling, available at: https://www.owasp.org/index.php/Application_Threat_Modeling

21. Jouinia, M., Rabaia, L.B.A., Aissab, A.B.: Classification of Security Threats in Information Systems, 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014). Procedia Computer Science 489 – 496 (2014)

22. Microsoft, The STRIDE Threat Model, available at: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

23. Microsoft, Applying STRIDE, available at: https://msdn.microsoft.com/en-us/library/ee798544%28v=cs.20%29.aspx

24. International Telecommunication Union: Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications (2015)

25. Berendt, B.: Better Data Protection by Design through Multicriteria Decision Making: On False Tradeoffs between Privacy and Utility. In: GDPR & ePrivacy, Annual Privacy Forum 2017. Springer, Heidelberg (2017)

26. Hansen, M., Jensen, M., Rost, M.: Protection Goals for Privacy Engineering. In: Security and Privacy Workshops (SPW), IEEE (2015)

27. Hoepman, J.-H.: Privacy Design Strategies. Privacy Law Scholars Conference (PLSC) 2013, Cornell University, Ithaca, NY, USA (2013)

28. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (Data Protection Directive) OJ L 281. vol. OJ L 281, pp. 31-50 (1995)

29. Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 (2016)

30. European Commission: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2017)
31. Porcedda, M.G.: On boundaries. In search for the essence of the right to the protection of personal data. In de Hert, P., van Brakel, R., Leenes, R. Proceedings of the 11th Computers, Privacy and Data Protection Conference, Hart (forthcoming)
32. United Nations, High Commissioner for Human Rights (OHCHR): Human Rights Indicators. A Guide to Measurement and Implementation. (2012)
33. Candler, J., Holder, H., Hosali, S., Payne, A. M., Tsang, T., Vizard, P.: Human Rights Measurement Framework: Prototype panels, indicator set and evidence base. Equality and Human Rights Commission, London (2011)
34. Fundamental Rights Agency: Using indicators to measure fundamental rights in the EU: challenges and solutions. (2011)
35. Koops, B.-J., Clayton Newel, B., Timan, T., Skorvanek, I., Chokrevski, T., Galic, M.: A Typology of Privacy. University of Pennsylvania Journal of International Law 38, 483 (2017)
36. Finn, R.L., Wright, D., Friedewald, M.: Seven Types of Privacy. In: Serge Gutwirth, R.L., Paul de Hert, and Yves Poullet, (ed.) European Data Protection: Coming of Age. Springer, Dordrecht (2013)
37. Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No 11 and 14), Council of Europe, ETS n° 005, 4 November 1950. Rome (1950)
38. X and Others v. Austria, no. 19010/07 CE:ECHR:2013:0219JUD001901007, (2013)
39. Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592, (2017)
40. Judgment of 5 October 2010 in McB, C-400/10 PPU, ECLI:EU:C:2010:582, (2010)
41. Judgment of 8 April 2014 in Digital Rights Ireland and Seitlinger and Others, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, (2014)
42. Judgment of 13 May 2014 in Google Spain and Google, C-131/12, ECLI:EU:C:2014:317, (2014)
43. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS n. 108, 28 January 1981. In: Europe, C.o. (ed.), vol. CETS No. 108, Strasbourg (1981)
44. Judgment of 6 October 2015 in Schrems, C-362/14, ECLI:EU:C:2015:650, (2015)
45. Gürses, S., Troncoso, C., Diaz, C., Engineering Privacy by Design. Paper discussed at the 4th Computers, Privacy & Data Protection Conference, Brussels, 2011
46. Porcedda, M.G.: Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. Computer Law & Security Review 34, (forthcoming (2018))
47. Porcedda, M.G., Wall, D.S.: Data Science, Data Crime and the Law. In: Berlee, A., Mak, V., Tjong Tijn Tai, E. (eds.) Research Handbook on Data Science and Law. Edwar Elgar (forthcoming (expected 2018)

48. Gürses, S., Troncoso, C., Diaz, C., Engineering Privacy by Design Reloaded, available at: http://carmelatroncoso.com/papers/Gurses-APC15.pdf.