Article │ Received 7 May 2024; Accepted 12 June 2024; Published 15 June 2024
https://doi.org/10.55092/let20240005

An environmental understanding of privacy and data protection law

Chunxiao Zhang

School of Juris Master, China University of Political Science and Law, Beijing, China

Email: chunxiao.zhang@cupl.edu.cn.

Abstract: This article provides a two-layered framework to conceptualize privacy and data protection law. Drawing upon Kirsty Hughes' behavioural understanding of privacy, this article argues that a common denominator in mainstream privacy theories can be identified by defining privacy as the guarantee of a free environment for social interaction. Data protection law serves as not only normative barriers to obtain and maintain privacy, but also crushers of unnecessary barriers created in the construction of the digital environment, which may insert existing social bias and create new forms of digital divide. This theoretical framework provides a better link to the 'group privacy' debate and challenges several orthodoxies in data protection law such as the centrality of the concept of 'personal data' and 'individualistic control' as the essence of the right to data protection. This article concludes that enhancing public participation and deliberation in digital environmental decision-making can be a promising direction forward to safeguard social freedom in a digital era.

Keywords: privacy; data protection; digital environment; essence of fundamental rights; public participation and deliberation

1. Introduction

Despite their perplexing relationships, privacy and data protection are two closely related terms and sometimes used interchangeably. Privacy has a long history in theoretical discussions across various disciplines such as philosophy, anthropology, sociology and legal studies. Ironically, the consensus regarding the meaning of privacy is that there is no consensus on its definition. The unsuccessful attempt of influential privacy theories to find a common denominator towards a top-down conceptualization nonetheless provides valuable insights of the rich meaning of privacy. In particular, recent literature has shifted from understanding privacy via an individualistic-oriented approach to uncovering its social values [1]. By contrast, data protection is a recently developed terminology, which is commonly used in the European context. The threats to dignity, freedom and democracy by ubiquitous digitization and large-scale data processing activities have attracted increasing regulatory

attention and facilitated the development of data protection law. Despite the inextricable link with privacy in its early evolution, data protection has arguably been recognized as an independent fundamental right in the European Union (EU) [2]. Nevertheless, many theoretical queries, such as the essence of the right to data protection and its relationship to privacy, have not been satisfactorily responded.

This article provides a two-layered theoretical framework for understanding privacy and data protection. Firstly, it argues that a common denominator can be identified within the mainstream taxonomy of privacy theories, i.e. the guarantee of the environment for free social interaction. This position echoes the behavioural understanding of privacy introduced by Hughes [3]. Secondly, inspired by her 'barrier theory' and considering the distinction between data and information, this article emphasizes the role played by data protection law in the digital environment as not only normative barriers but also barrier crushers for safeguarding social freedom. Taking into account the purely constructive nature of the digital environment, data protection law should be regarded as the normative infrastructure in the digital environment, guaranteeing that the digitization progress and subsequent digital environmental decision-making provide additional spheres for free social interaction rather than introducing discrimination, social exclusion and distributive injustice.

Other scholars have also drawn upon certain similarities between environmental pollution and data misuse to seek for common regulatory lessons in environmental law and data protection law [4]. This article provides a more comprehensive argument: data protection should go beyond individual control over personal data and put an emphasis on the control of the digital environment; it is not merely an issue of 'data pollution'[5] but more about public participation and deliberation in the construction of the digital environment. The subsequent data processing related decision-making should go beyond individual choice and consent and concern more about the sustainability of the digital environment.

The two-layered model can fill the gaps within existing literature in the following aspects. Firstly, it provides a new perspective to understand the mysterious 'entangling and disentangling' relationship between the right to privacy and the right to data protection: the common role played by these two concepts in facilitating social interaction at different levels explains why they are intrinsically linked but different. Secondly, the environmental understanding of data protection provides a better link to the new round of debate about group privacy. Thirdly, this theoretical framework puts forward a new perspective to consider two key presumptions in data protection law: 1) the centrality of the concept of 'personal data' [6]; 2) individual control over personal data as the essence of the right to data protection [7].

Following the introduction, Section 2 provides the details of an environmental understanding of privacy and how it links to existing literature. Section 3, by elaborating the difference between data and information and highlighting the constructive nature of data and the digital environment, sets out a new theoretical basis for understanding data protection. Section 4 explains the legal implications of this theoretical framework. Section 5 concludes.

2. An environmental understanding of privacy

Social and behaviour studies have noted the relationship between privacy and social interaction [8]. Schoeman provides a comprehensive examination of the important role of privacy in facilitating social interaction and upholding social freedom [9]. His observation starts from the criticism of Mill's individualistic definition of liberty and freedom, pointing out the vulnerability of individuals when faced with various social control (formal, such as law; or informal, such as social pressure) in the social contexts surrounding them [10]. He then emphasizes privacy's role in counterbalancing social control and ensuring social interaction and freedom [9]. More recent literature has put forward similar criticisms of the individualistic-oriented conceptualization of privacy and has attracted increasing attention to environment's constructive effects on individuals' understanding of themselves and their decision-making [11].

This section argues that other privacy theories, with less obvious relevance to social interaction and some of them individualistic-oriented, can be interpreted as sharing a similar emphasis on privacy's role in facilitating free social interaction. For instance, Fried's privacy theory is often labeled as '(individual) control over personal information' and 'intimacy' [12]. A closer examination of Fried's expression, however, suggests his emphasis on privacy as 'the necessary context' for developing certain important social relationships [13]. Through a social interaction-based theoretical lens, Fried's critics' theories can also be included in this line of argument. Reiman's theory treating privacy as a precondition of personhood also reflects an environmental understanding of privacy. He argues that '"selves" are created in social interaction rather than flowering innately from inborn seeds' and that privacy is the 'necessary conditions to the creation of selves' [14]. Thus a common rationale in Reiman's and Fried's theories is that privacy functions as an essential element in the environment surrounding individuals to develop social relationships and shape their personhood.

If the privacy conceptions of Remain and Fried are limited to certain special categories of social relationships such as love and friendship, later theoretical developments break such restrictions. For instance, Rachels' relational privacy theory places a special emphasis on the broader scope of social interaction enabled by privacy [15]. Rachels argues that privacy is necessary for individuals to control access to their information, to regulate their behaviour and to develop various social relationships with different people [15]. He emphasizes that a 'social relationship' does not mean 'anything especially unusual or technical' and instead includes various usual social relationships [15]. Roessler and Mokrosinska further develop this line of argument via an examination of privacy's role in three types of relationships: intimate relationships, professional relationships and interactions between strangers [16]. They conclude that privacy is 'a necessary condition for the efficient functioning of these different forms of interaction' [16], and 'by facilitating social interaction, norms of privacy contribute to creating the social conditions that are required for the successful exercise of individual autonomy' [16].

The right to be let alone and secrecy can also be included in the interaction-based theoretical framework. For instance, Poullet points out that the two aspects of privacy – 'the

right to seclusion' (opacity, secrecy or intimacy) and the 'possibility to develop our capacity to choose' – serve as the conditions for pursuing a common objective: to allow individuals to freely develop relationships and to fully participate in social life [17].

A similar perspective to understand privacy through an environmental-oriented lens can be found in Cohen's privacy as autonomy theory. Cohen highlights the power asymmetry between individuals and institutions in the current social and technological context, considering (data) privacy as the necessary conditions for individuals to exercise meaningful autonomy [18]. She argues that 'the nature and importance of privacy can be understood only in relation to a very different vision of the self and of the self-society connection' [18]. But she fails to interpret the collaborative relationships between privacy norms and other elements in the environment that may also influence our autonomy and freedom [19].

As Hughes points out, these theories still require a definition of the 'self', which may 'fall back on the identification of universally accepted privacy-related interests' [3]. Shifting the focus of attention from access control to social interaction-related elements can better manifest the subjective component of privacy, which is a state experienced by individuals [3].

By emphasizing 'experience' as the central point in understanding privacy, Hughes draws upon Altman's theory and provides a more elaborated explanation of privacy's role in facilitating social interaction [8]. According to Hughes, three types of barriers can be employed to obtain and maintain privacy: 1) physical barriers; 2) behavioural barriers (including both verbal and non-verbal forms of communication to show desire for privacy); 3) normative barriers [3]. Privacy is experienced when these barriers are respected. Normative barriers play an especially important role when physical and behavioural barriers are challenged by 'penetrating-technologies' and fail to provide adequate protection [3]. Privacy norms thus form an essential element in forming the baseline in an environment for free social interaction.

A new common denominator of various privacy theories can thus be identified: privacy norms serve as the normative infrastructure in the social environment which permits free interaction. Hughes' barrier theory can provide a basis for developing a two-layered approach to understanding privacy and data protection law. In the following section, by examining the difference between data and information, it is observed that unnecessary barriers and thus new forms of digital divide can be created during the digitization process. Privacy law can be perceived as the normative barriers at information level; data protection law functions as both normative barriers and barrier crushers at data level.

3. Normative barriers and barrier crushers in constructing a free digital environment

3.1. Tracing back to the 'legal irrelevance' of the difference between data and information

In comparison to privacy, 'data protection' is a recently developed term: it originated in Europe and has become influential around the world [20]. Interestingly, the German word *Daten* did not exist before the invention of computers; it originally referred only to the digital codes operated by computers. Compared to 'information', the German word *Daten* had a narrower meaning and covered only information in digital format [21].

Such technical difference between *information* and *data* (the English equivalence of *Daten*) was, however, lost in translation during the subsequent legislative process in Europe [22]. In 1973, the Council of Europe released a resolution on the protection of electronic personal data in the private sector [23]. Its explanatory report stated that data and information can be used interchangeably despite slight differences in nuance [24]. Afterwards, the translation of the *Datenschutz* concept into English and French in Convention 108 'subtly made the traces of automated processing present in *Daten* legally irrelevant' [25, 22]. The EU Data Protection Directive defines 'personal data' as 'any information relating to an identified or identifiable natural person' [26]. The General Data Protection Regulation (GDPR) does not change the interchangeable usage of data and information [27]. But the GDPR shows a clear tendency to detach data protection from privacy: the term 'privacy' has been removed from central concepts; instead 'data protection' is adopted throughout the GDPR [28].

It can thus be observed that the legal irrelevance of the technical difference between data and information is not intrinsic to any rationale of data protection law; it was rather a legal construction at the emerging stage of digital technologies. The radical digital transformation and automated decision-making pose serious doubts to the legal irrelevance of the distinction between data and information. Scholars from other disciplines have critically assessed the misleading expressions such as 'raw data', and have disclosed the bias and unfairness embedded in the digitization process [29]. In legal discourse, however, there are very limited discussions about the difference between data and information. As Bygrave points out, the regulatory importance of data and information-related concepts has not received enough weight within legal discussion; the current legal definitions thus fail to provide a stable analytical apparatus to effectively respond to the social problems shaped by rapidly changing technologies [30].

The mainstream understanding of data protection law in the European context, where the terminology 'data protection' originated, regards data protection rights and principles as the regulation of the conditions under which personal data can be lawfully processed [31]. Bygrave describes the function of data protection principles as the sanitization of the informational environment [32]. But as the difference between information and data will elaborate (see below), data protection should be understood more broadly as concerning not only the conditions for the processing of personal data (from collection to deletion), but also the regulation of the digitization process. The digitization process determines what features of the real-world entities will be included and excluded from the digital environment, how the included elements will be translated into data and how they will be weighed in the subsequent automated decision-making process. These factors have impacts on individuals, including both data subjects (people included in the digital environment) and non-data subjects (people excluded from the digital environment). Data protection thus needs to concern not only the digitized part but also the peripheral non-digitized part of the real world. It goes beyond serving as the normative barriers in maintaining privacy and concerns more about the distribution of resources and risks.

3.2. Understanding 'data': 'abstractions' or 'representations' of the real-world entities?

Mainstream information theories equate information to 'data plus meaning' (semantic content) [33]. Following a comprehensive examination of the definitions of data and information, Gellert points out that the semantic and pragmatic facets of information which emphasize the meanings represented by information in communication process have been widely adopted [34]. In contrast to information, data has been widely understood as representational and purely syntactic in both traditional and contemporary contexts [34]. Departing from this conceptual lens, Gellert reminds the overlooked syntactic dimension of information: information as signs existing independently of any cognitive agent [34]. He suggests that data and information 'equally represent the properties of objects and events' and their difference is merely that information represents entities in a more 'compact and useful way' [34].

The DIKW (data-information-knowledge-wisdom) pyramid is a well-established description of the relationship between data and information [35]. It is a summary of the steps in the knowledge production process. The DIKW pyramid contends that data can serve as the raw materials to generate information; information can then be used to generate knowledge; and wisdom can be extracted from knowledge [36]. Drawing upon the DIKW model, Gellert argues that data represent real-world entities not because they are signs but because they are 'an ensemble of features or attributes, which, put together, will allow for a representation of such entity' [34]. He thus defines data as 'abstractions of real-world entities', rather than representations of such entities [34]. The simple and linear information flows in a communication logic are not applicable in the current big data era where the goal of data processing is not to 'communicate' information but to 'learn' from data and 'create' new knowledge [34].

Data protection regimes were designed within a communication logic, with their main focus on the regulation of linear data flows such as collection, storage, retrieval and transfer of data [34]. The insufficient regulatory attention to the knowledge production dimension of data processing reflects a mismatch between data protection law and current technological context [34]. Gellert concludes that algorithmic regulation should shift from the regulation of 'information technology' to the regulation of 'knowledge technology'; a potential entry point is to model algorithmic regulation on the basis of the DIKW pyramid which reflects the 'learning' nature of data processing [34].

The following paragraphs, however, argue that the DIKW pyramid is quite a simplistic description of the relationship between data and information, without paying sufficient attention to the constructive nature of data. This article adopts Gellert's definition of data as 'abstractions of real-world entities' but argues that data are never just existing there. Data are the ensemble of features or attributes of the represented entities; but the selection of particular features or attributes are conducted by human beings. Data are never neutral or objective representation of real-world entities. Modelling data protection law and algorithmic regulation on the DIKW pyramid will overlook the constructive nature of the digitization process.

3.3. Challenging the DIKW pyramid

Data can carry semantic information; but this does not mean data are the digital equivalence of that information. Compared to the widely used expression of the 'collection' of data, 'creation' of data is a more accurate description of the very first stage of data processing. A translation from semantic information to data is involved in the data 'collection' process. There is no single objective route for such translation. Social norms and bias can be inserted in the translation regimes in an invisible manner [37]. Born-digital data, such as sensor data and smart meter records, seem not to involve the translation from information to data. However, as Morozov comments, in the data gathering process, human beings' subjective judgments in the design of data systems will decide what elements will be measured for what purposes, under what methodological approach, with what devices and under what circumstances certain elements will be highlighted or shaded [38]. Data are not neutral abstractions of real-world entities. Rather, they reflect how people 'slice up' and interpret social facts in the environment [38].

When data are analyzed to generate information, another translation process is involved. Data miners must translate a problem into a question (the 'target variable') with some quantified elements (the 'class labels') so that computers can solve the problem. Some target variables, such as 'creditworthiness' and 'good employees', do not have conclusive definitions. When designing the class labels to quantify different aspects of the target variables, there exist risks of bias and discrimination. Even if the biased and discriminatory models are not intentionally designed, they inherit the shortcomings of prior assessment mechanisms [39].

The translation in the digitization process casts serious doubts to the DIKW pyramid. As explained above, the translation between data and information is by no means in a single direction. Apart from information, relevant knowledge, wisdom, values, bias and social norms are also used to create data. These concepts can never be clearly separated and summarized in a single-direction pyramid. Rather, they form a continuous process, within which the complexities can be better illustrated by the circle in Figure 1 (DIKW-plus Circle).

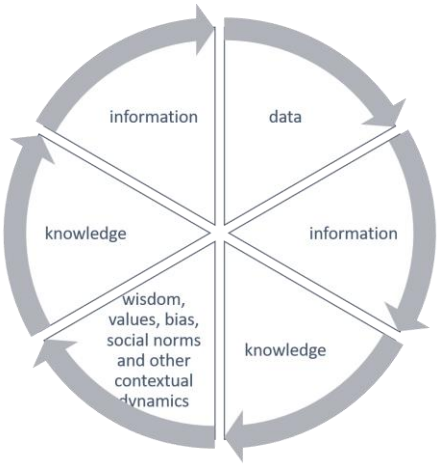

Figure 1. DIKW-plus (Data-information-knowledge-wisdom, values, social norms, bias and other contextual dynamics) Circle.

The controllers of the digital environment can create new groups by selecting specific attributes of real-world entities as the parameters for data processing. The formation of these new groups establishes new barriers in the digital world. Individuals may develop new behavioural barriers and social norms to mitigate the negative effects resulted from these digital barriers. As the 'ethics of indifference' developed in parallel with people's changing attitudes and learning capacity suggests, technological transformation and norm development cannot be separated [40]. But due to the information and power asymmetries between individuals and the controllers of digital environment, it is hard to remove the barriers by individual choices. Within the new groups created in the digital environment, individuals do not know other members of the group and can hardly comprehend the consequences of belonging to such groups. The lack of knowledge of their group memberships eliminates the premise for individuals to adopt behavioural measures to demolish the unnecessary barriers created by digital environment controllers. The large-scale data processing and automated decision-making are 'extremely powerful and potent due to their networked, continuously updated, dynamic and pervasive nature'.[41] According to Karen Yeung, the legitimacy of big data technologies cannot rely solely on individual consent and should be strictly checked by effective and enforceable constraints to guarantee the appropriate design of digital environment [41].

3.4. A two-layered model for understanding privacy and data protection law

Data protection law and norm should serve as such effective and enforceable normative constraints, going beyond merely protection of 'personal data' and functioning as not only normative privacy barriers or barriers for protecting 'personal data' but also normative tools to demolish unnecessary barriers which create new forms and degrees of social divide, so as to facilitate social interaction and freedom. The real value of data protection is thus the control of digital environment, which shapes 'socio-digital interaction' [40]. If privacy law is perceived as the guarantee of the necessary environment for social interaction at information level, data protection law can be understood as providing an additional layer of protection of the environment for free social interaction at data level.

As current privacy and data protection regimes largely overlook the 'nuanced' difference between data and information, the typical legal tools fail to pay sufficient attention to the bias and discrimination generated in digitization process. Their regulatory failure can be observed from the following aspects. Firstly, the individualistic-oriented concept of 'personal data' cannot fully accommodate the distributive issues in the design process of digital environment [42]. The precautionary measures which can cover the design of the data processing systems, such as data protection impact assessment (DPIA) and the requirement of data protection by design, operate on the prerequisite where 'personal data' are involved. Secondly, the impact assessments are premised on the condition that individuals have been included in certain digital environment; subsequent impact assessments evaluate whether collected 'personal data' are processed lawfully and fairly, or more broadly whether the processing interferes with data subjects' fundamental rights [43]. But the impacts on individuals who have not

been included or who refuse to be included in the data processing systems cannot be evaluated within the framework of DPIA. A serious problem would be that an individual without digital footprints might be regarded as too 'suspicious' or 'risky' [44]; whereas people who have 'valuable credentials, clean medical records, and impressive credit scores' can get advantaged economic treatment [45]. This may intensify the digital divide. Thirdly, scholars have called for a right to off-line alternatives or a right to de-networking to mitigate the negative impacts resulted from radical digitization [40]. But the importance of off-line alternatives is not simply about to be unconnected or de-networked, but about the guarantee of equivalent quality of (unconnected) life. That is to say, choosing to get out of the digital environment should not disproportionately affect the individuals' social interaction.

The following section thus explores how the two-layered model for understanding privacy law and the added-value of data protection law can contribute to legal discourse and normative development. It also demonstrates that these regulatory deficits can be mitigated by such layered thinking.

4. Legal implications of an environmental understanding of privacy and data protection

4.1. A better link to the concept of 'group privacy'

The two-layered environmental understanding of privacy and data protection law can provide a better response to the problems resulted from group identities and thus a better link to the concept of 'group privacy', the central idea derived from the new round of theoretical debate led by Taylor and others [46]. As the multi-disciplinary research in this debate demonstrates, the traditional rationale in privacy law fails to tackle the problems generated in large-scale data processing; the idea of group privacy provides new perspectives to consider how 'privacy interacts with data protection' [46, p. 234].

Departing from the individual control theory, the 'spherical or contextual notion of privacy' emphasizes the circumstances for data processing and the sphere (contexts and purposes) for defining such circumstances [46, pp. 37-66]. The collective dimension of privacy has shifted the regulatory focus from confidentiality to risks of discrimination and other negative impacts associated with unfair and harmful data processing [46, p. 148]. A systematic thinking about the risks embedded in various modern data systems would highlight the importance of impact assessments [46, pp. 159-173]. Some connection between privacy and environmental rights can be built via the view of group rights, suggesting that the key challenging point in the current social context is not the specific individual choices affected by various nudges but the radical digitization of the environment where human beings reside [46, p. 219].

These arguments share a common emphasis on the inadequacy of a sole focus on individual decision-making and the importance of normative architecture in the digital environment. The environmental understanding of data protection in this article can thus provide a better response and connection to the issue of 'group privacy'. It shows that data protection regimes are not only about granting individuals several rights while leaving them to make their own decisions, but also about promoting participation and deliberation in

constructing the digital environment. The two-layered structure of this conceptual framework can provide a more granular observation of how different factors in the environment interact with each other, how unnecessary and undesirable barriers can be created in digital environmental decision-making, and why behavioural barriers largely fail to function effectively and normative elements are thus especially important.

4.2. A problematic 'law of everything'?

In connection to the issue of 'group privacy', it is demonstrated that the dominant definition of 'personal data', which requires data subjects to be identified or identifiable at an individual level [47], cannot address the problems caused by data processing based on group identities. In such circumstances, data protection law does not apply. The identifiability criterion in the concept of personal data, although broadly defined and praised as protective [6], still falls behind technological developments. It is suggested that additional protection for group privacy is needed to complement the individual rights-based approach [46, p. 236].

By contrast, Purtova argues that the definition of personal data in EU data protection law is over-broad; it can turn data protection law into a 'law of everything' in the future [48]. The broad definition of personal data has good intention to provide high level protection; but such 'highly intensive and non-scalable' data protection regime 'will not simply be difficult but impossible to maintain in a meaningful way' [48]. For addressing such tensions between the protective aim and regulatory feasibility, Purtova suggests to abandon the distinction between 'personal data' and 'non-personal data' as the starting point of data protection law [48]. She then argues that data protection law should instead focus on seeking remedies for broadly defined 'information induced harms', including both individual and collective negative impacts [48]. But the concept of 'harm' is by itself very controversial; a broad definition of 'information-induced harms' might find difficulties to fit within existing legal frameworks.

The environmental understanding of data protection can provide an alternative theoretical basis to consider the issue of 'law of everything'. Purvota's concerns are for pragmatic reasons: the effectiveness of law might be compromised due to the apparently broad scope of application. But understanding data protection law as the normative infrastructure of a fair and free digital environment goes beyond the protection of personal data. In this sense, the environmental understanding of data protection law also departs from the 'personal data' centred approach. It instead suggests that a 'law of everything' is not intrinsically problematic. If the value to be protected is so important, embedded everywhere in the environment surrounding individuals and can significantly shape human behavior [49], a 'law of everything' can be justified. The pragmatic difficulties in enforcement cannot vacate the need for a holistic and broadly designed data protection regulatory framework; they rather suggest the need for more innovative enforcement strategies and instruments.

This article does not suggest the current data protection laws to completely abandon the concept of 'personal data' and the individual rights-based approach. But it should be recognized that the protection of personal data is insufficient. The precautionary measures in data protection laws, such as DPIA and data protection by design, are also restricted by the

scope of 'personal data' and focus on the impacts on individual rights. They cannot provide sufficient normative safeguards to demolish unnecessary barriers created in the digitization process. As Steele insightfully points out, the construction of environmental problems, risks and assessments should be understood as an issue of collective societal interests, rather than private or group interests [50]. An environmental understanding of data protection law fits better with the collective dimensions of the issues in constructing the digital environment.

4.3. The essence of the rights to privacy and data protection: from maintaining normative barriers to facilitating public participation

The environmental understanding of data protection can respond to another theoretical confusion reflected in the jurisprudence of the Court of Justice of the European Union (CJEU): the essence of the rights to privacy and data protection [51].

The CJEU has consistently recognized the distinction between the rights to privacy and data protection, but it fails to provide convincing explanations about the details of such distinction. In *Digital Rights Ireland* [52], concerning the validity of the Data Retention Directive which permitted blanket retention of metadata for a maximum of two years, the Advocate General (AG) explicitly embraced the idea of an 'autonomous' right to data protection but failed to provide elaborated interpretation of this right [53, point 55]. His argument that the blanket retention of metadata in this case was 'primarily' related to the right to privacy and only 'secondarily' to the right to data protection is deeply problematic: it is unclear why privacy in this case was the primary concern whereas data protection was only secondary [53, point 66]. The reasoning in the final judgment by the CJEU was even more controversial [54]. The Court held that the essence of the right to privacy was not adversely affected as the content of communication was not interfered [52, para. 39], without explaining why the content information could serve as a benchmark for assessing the interference to the 'essence' of this right. In addition, the Court addressed the essence of the right to data protection for the first time: the essence of this right was not adversely affected because the Data Retention Directive provided explicit data security requirements, mandating appropriate technical and organizational measures against 'accidental or unlawful destruction, accidental loss or alteration of the data' [52, para. 40]. In *Schrems II*, the AG provided a similar explanation as regards the essence of these two rights, with privacy's emphasis on the content of communication and data protection's focus on data security [55]. Such an interpretation touched upon only very limited aspects of the essence of the right to data protection.

As Brkan points out, the CJEU has yet provided a clear, convincing and coherent interpretation of the essence of these two rights [56]. Brkan argues that the infringement of the essence of a fundamental right can be established only where the interference is so serious as to 'make it impossible to exercise this right or call into question the existence of this right' [56]. She further explains that the specific data protection requirements in Article 8 of the Charter of Fundamental Rights of the European Union (Charter), such as fair and lawful processing and the establishment of independent data protection authorities, should not be interpreted as

the direct benchmark for assessing the interference with the essence of the right to data protection [56].

This article agrees that the specific requirements in Article 8 of the Charter should not be interpreted as direct indicators of the essence of the right to data protection. The theoretical framework in this article does not aim to provide a top-down definition of the essence of these two rights. But it can provide an alternative perspective to consider this question.

In the light of the judgment in *Digital Rights Ireland*, serious flaws in data security and confidentiality would constitute infringements on the essence of the right to data protection [52, para. 40]. In subsequent cases such as *Schrems II*, the AG consistently explained that the essence of the right to data protection was respected because certain safeguards, although imperfect, were adopted to protect the security, confidentiality and integrity of data [55, points 279-280].

This reasoning may not necessarily suggest that data security itself is the essence of data protection rights. Rather, in such circumstances the essence has been infringed because serious security flaws in the organizational or technical measures can cause systematic influence on both particular data systems and unpredictable impacts on the whole digital environment (especially considering the currently hyper-connected technological context), negatively affecting indefinite number of people and lasting for long periods. Petkova and Boehm's argument that unfair profiling can infringe the essence of the right to data protection also makes sense under an environmental understanding of data protection [51]. Their emphasis on unfair profiling, rather than the identification of individuals, is consistent with the suggestion to abandon the increasingly blurring distinction between personal data and non-personal data. The focus on the fairness of profiling systems also concerns important architectural elements within the digital environment.

Some insights in environmental law can also inform the fundamental aspects of the right to data protection. The conservation of biological diversity and ecological integrity has been argued as the 'fundamental' aspect for achieving ecological sustainability [57]. Biological diversity and ecological integrity thus need to be granted sufficient weight and priority in environmental decision-making. Similarly, when thinking about sustainable development of a digital environment, the conservation of diversity and social integrity in the digital environment should be considered as a 'fundamental' or 'essential' aspect, and thus the essence of the right to data protection. Like environmental problems in the physical world, inappropriate design of the digital environment and subsequent data processing may have disproportionate impacts on vulnerable groups, exacerbate digital divide and harm social integrity [58]. The failure to adopt appropriate organizational and technical measures to protect data security may create new types of vulnerabilities that distribute unequally among different social groups. As suggested in previous sections, under-regulated digitization and unfair profiling may exacerbate existing social bias and even promote covert social exclusion, which would be contradictory with the conservation of diversity and social integrity.

As for the right to privacy, the CJEU has appeared to consider the access to content data as an important 'benchmark', or at least the most explicit factor to be considered, when assessing the infringement of its essence [56]. For instance, in *Digital Rights Ireland*, the

Court ruled that there was no infringement of the essence of the right to privacy as the content of the communications was not required to be processed under the Data Retention Directive [52, para. 39]. In *Schrems*, the Court held that the US public authorities' blanket access to the content of electronic communications impaired the essence of the right to privacy [59]. Consistently, in *Schrems II*, the AG reiterated that there was no breach of the essence of this right as the data transfer framework in question did not permit generalized access to the content of communications [55, points 273, 278].

The two-layered theoretical framework in this article can answer why the essence of privacy connects to the content of communications. Considering the difference between information and data, information has a stronger emphasis on the content layer. Thus privacy law can be understood as the normative guarantee of the environment for free social interaction at information level, in both pre-digital and the digital society. The right to data protection is a newborn right in response to the social problems complicated by digitization and the evolution of digital technologies. It can be understood as providing an additional layer of protection for the environment that permits free social interaction at data level.

This two-layered framework can thus provide a new perspective to explain the difference and 'intrinsic' link between privacy and data protection. It can also help explain that on the one hand, in many CJEU cases, the AG and judges explicitly recognize that the right to data protection is distinguished with the right to privacy and has its separate legal basis; on the other hand, in their reasoning, it is hard to find a case where the assessments of the infringements of these two rights have really been separated. It is also rare to find that the right to data protection has been infringed without infringing the right to privacy; the infringements of these two rights are often analyzed together. As in *Schrems II*, the AG pointed out that although the frameworks for analyzing the infringements of these two rights are 'conceptually distinct', 'they overlap in the case of Article 8 of the Charter' [55, footnote 120]. In a subsequent note, the AG further explained that granting public authorities undifferentiated access to the content of communications would constitute infringements to the essence of both the rights to privacy and data protection [55, footnote 147].

It should be noted that the two-layered model does not suggest to separately consider the protection of the digital environment and the natural environment. Digital environment permeates to the real world and the influence is not in any sense 'less real or vital' [60]. When digital identities find either individual or group connection with real human beings, the risks of compromising free social interaction in the physical world will increase. The regulatory insights from the two-layered model still need to be considered within the holistic social context.

5. Conclusion

The two-layered theoretical framework puts forward a granular perspective to consider the added-value of data protection law. Different from privacy law, data protection law serves as not only normative barriers for safeguarding privacy but also crushers of unnecessary barriers created in the construction process of the digital environment.

The environmental understanding of privacy and data protection law can provide policymakers with a solid conceptual basis for adopting a more proactive stance to interpret these two rights. This theoretical framework further suggests the necessity to introduce precautionary measures against up-stream privacy and data protection risks. The unchecked expansion of digitization and large-scale data processing may cause severe impacts on the environment; whereas the harms might be 'systematically downplayed' by the more traditional approaches to conceptualizing harms in legal discourse [61]. Controllers of digital environment may misrepresent consumers and hide their privacy and data protection concerns in front of policymakers, so as to lobby against legal intervention [62]. Individuals' voice regarding their diverse understanding of risks and harms involved in the digitization process cannot be heard. In such circumstances, 'extra precaution' should be justified [63].

In-depth discussions about the concretization of the precautionary principle in data protection law [64] and the facilitation of public participation and deliberation in digital environmental decision-making need to be explored more thoroughly by future research. The deliberative dialogue (in the form of 'citizen jury') conducted by the RSA's Forum for Ethical AI provides a good example of a promising way forward to democratize the digital environmental decision-making process [65].

Acknowledgments

Funding: This work is supported by China University of Political Science and Law, Young Scholars Support Scheme, under Grant 1000-10824821.

Conflicts of interests

The author declares no conflict of interests.

References

[1] Roessler B, Mokrosinska D, *Eds. Social dimensions of privacy: Interdisciplinary perspectives*. Cambridge: Cambridge University Press, 2015.
[2] Lynskey O. Deconstructing Data Protection: the 'Added-value' of A Right to Data Protection in the EU Legal Order. *Int. Comp. Law Q*. 2014, 63(3):569–597.
[3] Hughes K. A Behavioural Understanding of Privacy and its Implications for Privacy Law. *Mod. Law Rev.* 2012, 75(5):806–836.
[4] Hirsch DD. Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law. *Ga. Law Rev*. 2006, 41(1):1–63.
[5] Ben-Shahar O. Data Pollution. *J. Legal Anal*. 2019, 11:104–159.
[6] Urgessa WG. The Protective Capacity of the Criterion of 'Identifiability' under EU Data Protection Law. *Eur. Data Prot. Law Rev*. 2016, 2(4):521–531.
[7] Clifford D, Ausloos J. Data Protection and the Role of Fairness. *Yb Eur Law*. 2018, 37:130–187.

[8] For example, Altman I. *The Environment and Social Behaviour: Privacy, Personal Space, Territory, Crowding*, Monterey: Brooks/Cole Publishing Company, 1981.
[9] Schoeman FD. *Privacy and Social Freedom*, New York: Cambridge University Press, 1992.
[10] Mill JS. *On Liberty*, New York: Cambridge University Press, 2011.
[11] For example, Nissenbaum H. Privacy as Contextual Integrity. *Wash. L. Rev.* 2004, 79:119–157.
[12] Solove DJ. *Understanding Privacy*, Cambridge, MA: Harvard University Press, 2009. p. 13.
[13] Fried C. *An Anatomy of Values*, Cambridge, MA: Harvard University Press, 1970. p. 142.
[14] Reiman J. Privacy, Intimacy, and Personhood. *Philos. Public Aff.* 1976, 6(1):26–44.
[15] Rachels J. Why Privacy Is Important. Schoeman FD, Ed. *Philosophical Dimensions of Privacy*, New York: Cambridge University Press, 1984. pp. 290–299.
[16] Roessler B, Mokrosinska D. Privacy and Social Interaction. *Philos. Soc. Crit.* 2013, 39(8):771–791.
[17] Poullet Y. Data Protection Legislation: What Is at Stake for Our Society and Democracy? *Comput. Law Secur. Rev.* 2009, 25(3):211–226.
[18] Cohen J. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Rev.* 2000, 52:1373–1438.
[19] Hoofnagle CJ. *Federal Trade Commission Privacy Law and Policy*, New York: Cambridge University Press, 2016. p. 151.
[20] Greenleaf G. The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108. *Int. Data Priv. Law.* 2012, 2(2):68–92.
[21] Hondius FW. *Emerging Data Protection in Europe*, Amsterdam: North-Holland Publishing Company, 1975. p. 85.
[22] Fuster GG. *The Emergence of Personal Data Protection as A Fundamental Right of the EU*, Cham: Springer, 2014. pp. 264–265.
[23] Council of Europe, Resolution (73) 22 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector. 26th December 1973.
[24] Council of Europe, Resolution (73) 22, Explanatory Report, point 16.
[25] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No. 108, 1981.
[26] Art 2(a) Personal Data Protection Directive (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).
[27] Art 4(1) General Data Protection Regulation (Regulation (EU) 2016/679 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).
[28] Costa L, Poullet Y. Privacy and the Regulation of 2012. *Comput. Law Secur. Rev.* 2012, 28(3):254–262.
[29] Gitelman L. Ed. *Raw Data Is An Oxymoron*, Cambridge, MA: The MIT Press, 2013.
[30] Bygrave L. Information Concepts in Law: Generic Dreams and Definitional Daylight. *Oxf. J. Leg. Stud.* 2015, 35(1):91–120.

[31] Gellert R, Gutwirth S. The Legal Protection of Privacy and Data Protection. *Comput. Law Secur. Rev*. 2013, 29(5):522–530.
[32] Bygrave L. *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague: Wolters Kluwer, 2002. p. 137.
[33] For example, Floridi L. Is Semantic Information Meaningful Data? *Philos. Phenomenol. Res*. 2005, 70(2):351–370.
[34] Gellert R. Comparing Definitions of Data and Information in Data Protection Law and Machine Learning: A Useful Way forward to Meaningfully Regulate Algorithms? *Regul. Gov*. 2022, 16(1):156–176.
[35] Rowley J. The Wisdom Hierarchy: Representations of the DIKW Hierarchy. *J. Inf. Sci*. 2007, 33(2):163–180.
[36] Ackoff RL. From Data to Wisdom. *J. Appl. Syst. Anal*. 1989, 16:3–9.
[37] Johnson JA. How Data Does Political Things: The Process of Encoding and Decoding Data Are Never Neutral. 2015. Available: https://blogs.lse.ac.uk/impactofsocialsciences/2015/10/07/how-data-does-political-things/ (accessed on 28 April 2024).
[38] Morozov E. *To Save Everything, Click Here*, London: Allen Lane, 2013. pp. 245–246.
[39] Barocas S, Selbst AD. Big Data's Disparate Impact. *Calif. Law Rev*. 2016, 104(3):671–732.
[40] Karaboga M, Matzner T, Obersteller H, Ochs C. Is There A Right to Offline Alternatives in A Digital World? in Leenes R, van Brakel R, Gutwirth S and de Hert P (eds). *Data Protection and Privacy: (In)visibilities and Infrastructures*, Cham: Springer, 2017. pp. 40–41, 54.
[41] Yeung K. 'Hypernudge': Big Data As A Mode of Regulation by Design. *Inf. Commun. Soc*. 2017, 20(1):118–136.
[42] The centrality of the concept of 'personal data', see for example, Finck M and Pallas F. They Who Must Not Be Identified – Distinguishing Personal from Non-personal Data under the GDPR. *Int. Data Priv. Law*. 2020, 10(1):11–36.
[43] Janssen HL. An Approach for A Fundamental Rights Impact Assessment to Automated Decision-making. *Int. Data Priv. Law*. 2020, 10(1):76–106.
[44] Christl W, Spiekermann S. Networks of Control — A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy. 2016. p. 129.
[45] Peppet SR. Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future. *Northwest. Univ. Law Rev*. 2011, 105(3):1153–1204.
[46] Taylor L, Floridi L, van der Sloot B. Eds. *Group Privacy*, Cham: Springer, 2017. pp. 37-66, 148, 159-173, 219, 234, 236.
[47] Article 29 Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 20 June 2007).
[48] Purtova N. The Law of Everything: Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law. *Law Innov. Technol*. 2018, 10(1):40–81.

[49] Hildebrandt M, Koops BJ. The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Mod. Law Rev*. 2010, 73(3):428–460.
[50] Steele J. *Risks and Legal Theory*, Portland: Hart Publishing, 2004.
[51] Petkova B, Boehm F. Profiling and the Essence of the Right to Data Protection. Selinger E, Polonetsky J, Tene O. Eds. *The Cambridge Handbook of Consumer Privacy*, New York: Cambridge University Press, 2018. pp. 285–300.
[52] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (CJEU GC) ECLI:EU:C:2014:238, paras. 39, 40. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 (accessed on 28 April 2024).
[53] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (Opinion of AG *CRUZ VILLALÓN*) ECLI:EU:C:2013:845, points 55, 66. Available: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CC0293 (accessed on 28 April 2024).
[54] Lynskey O. The Data Retention Directive is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland. *Common Mark. Law Rev*. 2014, 51(6):1789–1811.
[55] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Schrems* (Opinion of AG SAUGMANDSGAARD ØE)ECLI:EU:C:2019:1145, points 273, 278-280, footnotes 120, 147. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CC0311 (accessed on 28 April 2024).
[56] Brkan M. The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *Ger. Law J*. 2019, 20:864–883.
[57] Preston BJ. The Judicial Development of Ecologically Sustainable Development. Fisher D. Ed. *Research Handbook on Fundamental Concepts of Environmental Law*, 1st ed. Cheltenham: Edward Elgar, 2016. p. 506.
[58] van Deursen AJ, van der Zeeuw A, *et al*. Digital Inequalities in the Internet of Things: Differences in Attitudes, Material Access, Skills, and Usage. *Inf. Commun. Soc*. 2021, 24(2):258–276.
[59] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (CJEU GC) ECLI:EU:C:2015:650, para 94. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 (accessed on 28 April 2024).
[60] Floridi L. Informational Ethics: An Environmental Approach to the Digital Divide. *Philos. Contemp. World*. 2001, 9(1):1–7.
[61] Solove DJ, Citron DK. Risk and Anxiety: A Theory of Data-Breach Harms. *Tex. L. Rev*. 2018, 96:737–786.
[62] Turow J, Hennessy M, Draper N. How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation. Annenberg School for Communication, University of Pennsylvania, 2015.

[63] Persson E. What are the Core Ideas behind the Precautionary Principle? *Sci. Total Environ*. 2016, 557-558:134–141.

[64] For example, Narayanan A, Huey J, Felten EW. A Precautionary Approach to Big Data. Gutwirth S, Leenes R, de Hert P. Eds. *Data Protection on the Move*, Dordrecht: Springer, 2016. pp. 357–385.

[65] The Royal Society for the encouragement of Arts, Manufacturers and Commerce (RSA) Forum for Ethical AI. Democratising Decisions about Technology — A Toolkit. 2019.