Articles

Privacy: Back to the Roots

By J.C. Buitelaar[*]

A. Introduction

Phenomena such as cloud computing,[1] but also ambient technology,[2] chain informatization,[3] and social networking sites put into question the continuing applicability and relevance of existing legal frameworks, in particular the European Data Protection Directive (henceforth the DPD or the Directive),[4] which dates back to 1995.[5] Its framework of assigning roles of controller[6] and processor[7] appears to stand up no longer.[8] It can be

[*] Drs J.C. (Hans) Buitelaar MA (Oxon) is Ph.D student and researcher at University of Tilburg, TILT, The Netherlands. In addition, Mr. Buitelaar is the Data Protection Officer of the Ministry of Education, Culture, and Science, as well as the Ministry of Social Affairs and Employment in the Hague, the Netherlands.

[1] *Cloud computing* knows many definitions, but for the purpose of this article it is sufficient to describe it as a networked body of web-based services providing online storage capacity and applications.

[2] *Ambient intelligence* (AmI) implies a real-time adaptive environment, in which most adaptive decisions are taken by machines in a process of machine-to-machine communication. These decisions are based on what is called *autonomic profiling*, which severely restricts human intervention while needing a continuous and dynamic flow of information.

[3] "Chain informatization" refers to the automated sharing of information between private-sector organizations and government agencies, but also between the organizations within the concerned sector itself.

[4] Directive 95/46/EC, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31. Incidentally, there are more major frameworks in this area which are growing old. Compare, for example, the OECD Guidelines, which date back to 1980. David Wright, Paul De Hert & Serge Gutwirth, *Are the OECD Guidelines at 30 Showing Their Age?*, 54 COMM. ACM 119.

[5] For a useful discussion of the relevance of existing frameworks for privacy protection for this new technological phenomenon, compare Ann Cavoukian, *Privacy in the Clouds*, 1 IDENTITY INFO. SOC'Y 89 (2008), *available at* http://www.springerlink.com/content/e13m644537204002/fulltext.pdf.

[6] "Controller" means "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." Council Directive 95/46/EC, *supra* note 4, art. 2.

[7] "Processor" "shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller . . . ." *Id.*

[8] NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE 176 (2011). Dr. Purtova claims that the rigid structure of this framework causes confusion and thus undermines the effectiveness of its mechanisms of accountability.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

argued that it does not help any more in assigning responsibility for the processing of personal data.[9] By a strict application of the DPD, the data subject can even be construed as playing the role of controller.[10] Not only does the functioning of the principles of the roles need a reconsideration, but other essential principles, such as that of purpose-binding, require it, as well. For example, because data, which in a social networking context are disclosed to friends, are also used for targeted advertising and tailoring services, etc., the purpose-binding called for by the DPD becomes, at the very least, opaque. Furthermore, assigning responsibility to the actual processor in charge is just as unclear. Therefore, these current phenomena make clear that the conceptual foundations of the legislative frameworks, which purport to facilitate and protect privacy, require reflection.

This reconsideration should be placed in the context of the current evaluation of the DPD.[11] Besides the fact that the evaluation is a formal necessity, it is interesting to note that the motivating arguments are for the revision of the DPD according to the responsible EU Commissioner, Mrs. Viviane Reding.[12] She paints a tantalizing picture of a market of 500 million consumers in the E.U. She wants to help these consumers and the businesses active in this market to get the most out of the single market. She places her announcement in this economic context. However, at the same time, she also proclaims

---

[9] *Opinion 1/2010 of the Article 29 Data Protection Working Party on the Concepts of "Controller" and "Processor"* (16 Feb. 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[10] *Compare Opinion 5/2009 of the Article 29 Data Protection Working Party on Online Social Networking*, §3.1 (12 June 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (dealing with the concept of data controller in the context of online social networking).

[11] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, COM (2010) 609 final (4 Nov. 2010). The Commission conducted a public consultation in 2009 on the review of the current legal framework. See the replies to this consultation archived at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. At the time of putting the finishing touches on this article, an unofficial version of the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (General Data Protection Regulation) circulated. On the whole, the general gist of the Proposal was much in line with objectives as mentioned in the Commission document announcing the review. In summary, the main policy objectives for the Commission are to: (1) Modernize the EU legal system for the protection of personal data, in particular to meet the challenges resulting from globalization and the use of new technologies; (2) strengthen individuals' rights, and at the same time reduce administrative formalities to ensure a free flow of personal data within the E.U. and beyond; (3) improve the clarity and coherence of the EU rules for personal data protection and achieve a consistent and effective implementation and application of the fundamental right to the protection of personal data in all areas of the Union's activities.

[12] Viviane Reding, Vice-President of the European Comm'n Responsible for Justice, Fundamental Rights and Citizenship, Doing the Single Market Justice (16 Sept. 2010), *available at* http://www.lisboncouncil.net/component/downloads/?id=368. *See also* Viviane Reding, *The Upcoming Data Protection Reform for the European Union*, 1 INT'L DATA PRIVACY L. 3 (2011), *available at* http://idpl.oxfordjournals.org/content/1/1/3.full.pdf+html.

that key themes in this revision effort will be strengthening the concept of data minimization, strengthening the rules of consent, lessening the administrative burden, enhancing the responsibility of data controllers, and streamlining the procedures for data transfer. Technical measures, such as privacy by design and the creation of a cyber-crime-safe environment, should also be developed in this quest for obtaining smart, sustainable, and inclusive growth. Still, the EU Commissioner makes clear that the other foundation stone of the DPD, the economic motive, will provide an equally important guideline for this long-awaited revision.[13]

In this article, I will argue that this two-pronged review attempt will fail in making the legislative framework of the DPD sufficiently suitable for the protection of the privacy of EU citizens in the Internet era. I will set up my argument along the following lines. First, I will present an analysis of the shortcomings of the current DPD framework. It will turn out that the basic tenets of privacy protection as already present in the DPD deserve attention in the reconsideration of privacy. To be effective, however, they should be securely grounded in a concept that will enhance the protection of privacy. To this end, I will present foremost a return to the basics—so to speak—by grounding the concept of privacy in the ethical/philosophical context of informational self-determination.[14]

I discern strong support for this view in the German legal and philosophical discussion, where the right to informational self-determination and a general right to privacy are mentioned in the *Grundgesetz* (German Constitution).[15] A very poignant example is the recent partial annulment of the implementation of the Data Retention Directive by the *Bundesverfassungsgericht* (German Constitutional Court).[16] One of the reasons for this potentially explosive ruling was the presumed incursion the Data Retention Directive

[13] "There is an inherent conflict between the protection of personal data and the free trans-border flow of personal data." Wright, De Hert & Gutwirth, *supra* note 4, at 123.

[14] For clarity's sake it is noted here that the opinions expounded in this paper are informed by a liberal-democratic outlook.

[15] The German Constitutional Court traced the right to privacy to the fundamental right to the free development of one's personality. Article 2(1) of the German Constitution states, "The value and dignity of the person based on free self-determination as a member of a free society is the focal point of the order established by the Basic Law." GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [GRUNDGESETZ] [GG] [BASIC LAW], 23 May 1949, BGBl. I. The general personality right as laid down in Article 2(1) GG in connection with Article 1(1) GG serves to protect these values.

[16] Bundesverfassungsgericht [BVerfG - Federal Constitutional Court] Case No. 1 BvR 256/08, 2 Mar. 2010, 121 BVERFGE 1 (Ger.); Press Release, Bundesverfassungsgericht, *Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäss*, BVerfG Press Release 11/2010 (2 Mar. 2010), *available at* http://www.bverfg.de/pressemitteilungen/bvg10-011.html (English translation available at http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html).

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

makes into the right to informational self-determination.[17] Using the idea underlying the German approach as a starting point, I will discuss in this paper whether this point of view may provide a revitalization of privacy and thereby contribute to the revision of the DPD. This leads to the following research question: *Can the protection of privacy in theory and practice be revitalized by grounding it in informational self-determination?*

B. Analysis of the Data Protection Directive

At the European level, the protection of privacy, as a human right, has been encased most prominently in Article 8 of the European Convention on Human Rights as well as in Article 8 of the EU Charter, which has been implemented in the EU Data Protection Directive.[18] The atrocities of the Second World War, when large record systems were used to facilitate genocide, made it painfully clear that these systems facilitated public intrusion into the private sphere. This led to the incorporation of privacy as a human right in a number of regulatory texts, such as the Universal Declaration of Human Rights (1948) and the European Convention on Human Rights (1950). These regulations focused on privacy as a fundamental human right. In the 1970s, the private sector began to systematically record and use personal data after the arrival and broad uptake of Information and Communication Technology (ICT). At this point, the need for protection of personal data could no longer be assessed with sole regard to what states might do; the private sector also presented a threat. Internationally, this led to the Organization for Economic Cooperation and Development (OECD) Guidelines (1980)[19] and Council of Europe Convention No. 108 (1981).[20] At the national level in Europe, several initiatives[21] were taken, but these national frameworks soon inhibited the free transfer of information between the member states of the European Union.[22] Thus arose a barrier against the

[17] Christian DeSimone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, 11 GERMAN L.J. 291, 316 (2010) (arguing that Germany by this ruling risked a supranational legal crisis with adverse impact on European Union integration).

[18] Council Directive 95/46/EC, *supra* note 4. Article 8 of the Charter of the European Union states, "Everyone has the right to the protection of personal data concerning him or her." Charter of Fundamental Rights of the European Union art. 8, Dec. 18, 2000, 2000 O.J. (C 364) 1.

[19] Organization for Economic Co-operation & Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (23 Sept. 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[20] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 Jan. 1981, E.T.S. No. 108, *available at* http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm.

[21] In the U.K., for example, reference can be made to the Data Protection Act (1984) and in France to the Act Regarding Informatics, Files and Liberties (1978). For an insightful table of the world-wide diffusion of data protection legislation, see COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 127 (2006).

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

development of the internal market, the first "Pillar" of the European Union. In this context, the Directive was drawn up: An instrument designed to improve cross-border trade in the internal market by enabling free flow of information and harmonizing data protection legislation. As such, the Directive is tied to the concept of personal data rather than to a broader notion of privacy.[23] Next to the protection of personal data, the Directive has as an important purpose: Enabling the free flow of information.

Undeniably, the Directive has been very influential in a number of ways. It set the standard for the legal definition of personal data. It clarified the scope of data protection rules, defined rights of data subjects, established provisions regarding sensitive personal data, and established supervisory authorities and transnational oversight arrangements, such as the Article 29 Working Party. Its principle-based framework permits flexibility. Another important asset is its technology-neutral approach. The definition of personal data has been left vague, so that it can be applied in a number of technological contexts. It relies on considerations of "content," "purpose," and "result," and does not concern itself with the way its provisions should be applied.[24] Compared to other international guidelines and regulations, the Directive notably focuses not only on principles but also on procedures to reach the desired goals.

It can be argued that data protection regimes were designed to alleviate the risks to individual self-determination that resulted from the development of information technologies. This development of IT technologies resulted in a worsening of the "power asymmetries"[25] between data subjects and data controllers. Data subjects no longer understand the selection, purpose, and duration of use of their data. In addition, they have no control over the degree to which the processing of their data is needed by public and private bureaucracies, and have little check on those organizations' purposes.[26] Because a lack of control can be discerned, in general, and because the notion of control is a central one in the theory of privacy, it is important to pay attention to how the Directive tries to address this lack of control.

---

[22] Some member states applied strict limitations whereas other states applied no limitations at all. NEIL ROBINSON ET AL., RAND EUROPE, REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 6 (2009), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf.

[23] *Id.* at 7.

[24] *Id.* at 24.

[25] Antoinette Rouvroy & Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, *in* REINVENTING DATA PROTECTION? 45, 68 (Serge Gutwirthet al. eds., 2009).

[26] *Id.*

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

There are several levels of individual control that can be distinguished in the Directive. First, there is the notion of consent as contained in Article 7. The data subject has to give his consent unambiguously to make the data processing possible.[27] In fact, the data subject's consent is considered by the Directive to be the normal way to make the processing of sensitive data legitimate. Second, there are the norms of data quality in Article 6; i.e., data must be collected for a specific purpose, they must be adequate, relevant, and not excessive in relation to the purpose, and they must be accurate and up to date. These norms, when implemented, confer a certain kind of control on the data subject, because protecting the integrity of the process permits the data subject to form stable expectations about how information about him will be handled. After all, to be able to exercise control, the data subject has to be aware which data are processed. Third, the data subject is granted control by the requirement to actively inform himself about the processing of his information. Article 10 in the Directive requires that the data subject be informed about the identity of the controller, the purposes of the processing, and the types of information that is processed. To be fully informed about this is an important prerequisite both for being able to take part in the control of the flow of personal data, and to know for what purposes information about him will be processed. Next, the Directive gives the data subject the right to access and to correct information about himself. These rights on the part of the data subject make it possible for him to control information about himself more actively. Finally, the Directive also in some cases uses passive consent. In Article 14, the data subject is given the right to object to processing for certain purposes. This is the case, for example, with processing for the purpose of direct marketing. In the unofficial Proposal for the new DPD, it is also proposed to add a right to be forgotten.

C. Weaknesses of the DPD

I. Consent

The consent principle is meant to empower the individual to exercise his decisional power to determine what information about him is disclosed. As such, it is an essential provision in the Directive, and therefore also in the effort to grant the individual control over his information's processing. The Directive in Article 8 explicitly acknowledges consent as a sufficient condition to legitimize processing. It is, however, a controversial concept. The growing conflation of (passive) consent and interaction makes the condition of consent less demanding and meaningful. Many websites include consent in the transactional process as a stepping stone to opportunistic processing of visitors' data for profit. The consumer often does not have much choice. One may very well wonder whether this type of consent is clearly given, and further, whether it sufficiently legitimizes processing.

[27] The notion of consent is, however, controversial. It will be discussed later on, in the section dealing with the weaknesses of the DPD.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

However, in Article 2(h), one finds an opportunity to declare the processing illegitimate, even though the consent has been granted, on the grounds that the processing is disproportionate.

Consent is thus given in a positive action, by which a user of personal data is authorized, ex ante, by the actor concerned, to obtain access to and use of his personal data legally. In practice, this consent is thought to be obtained through the passive consent measure of publishing privacy policies. However, an important feature in this respect should be that a click-through functionality is provided, by which the consumer can indicate his consent to and acceptance of the privacy policy. However, this is a rather ineffective measure, because most users use the click-through functionality blindly. Important in this respect is that consent can be limited in accordance with the purpose for which the information is processed. However, as Bygrave notes, even in the Directive consent is rarely laid down as the sole precondition. It tends to be one of several prerequisites.[28] Its value is undermined by the large number of criteria that justify processing without the prior consent of the data subject.[29]

Consent and the revocation thereof are inextricably linked. However, the extent and effectiveness of revocation of consent is questionable. Retrospective revocation of consent is obviously impossible. The privacy implications are aggravated by the problem of the Internet's inability to forget.[30] It is obvious that the past cannot be altered and that data disclosures cannot be undone. All that can be achieved by revocation of consent is to stop further processing. In fact, it can be argued that consent has become an increasingly toothless tool, whereas it ought to be a preeminent measure for the user to effectuate control over the use of his personal data.

II. Concept of Personal Data

Another essential matter is the lack of clarity concerning the risks presented by the Directive's concept of personal data. This poses a growing problem because the information thirst of both the private as well as the public sector is almost unquenchable. It is very much a question whether the essential principle of data minimization stands up here. The key concept of personal data—DPD Articles 2(d) and 2(e)—triggers the ensuing

[28] LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 66 (2002).

[29] Bygrave observes that these criteria can be classified into 5 categories. The two most pertinent categories here are (1) that the processing is necessary to execute a task in the public interest and (2) that it is carried out in pursuance of legitimate interests that override the conflicting interests of the individual. *Id.* at 66 n.251.

[30] In the Proposal a new article is introduced providing the conditions of the right to be forgotten, including the right to obtain erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

obligations on data controllers.[31] It is at this point that the Directive has shown itself increasingly a source of confusion.[32] It can be said that the DPD exhibits a flexible approach, allowing for its application to various situations and developments affecting fundamental rights. However, the consequence is that numerous situations have arisen in which it is not clear whether the data to be protected are actually personal data. A good case in point is that of IP addresses.[33] This vagueness provides data collectors the opportunity to collect these data freely without the ensuing obligations that the DPD would make incumbent upon them.[34]

III. Transparency

Another weakness in the DPD is formed by the measures aimed at providing the data subject with transparency of data processing. These measures are often ineffective. An important obligation the DPD introduced in this respect is providing information to the data subject when personal data about him are being processed. This can be done by privacy notices or privacy policies. Aside from the publication of these policies, the involvement of the user is sought by asking his consent. These requests are usually published on a website, and their effectiveness depends upon the interaction between the provider and the user. Privacy policies, for example, contain specific legal information stating rights and obligations. Consent notices are aimed at obtaining the data subject's informed consent about certain processing of his data by way of ticking a box. In practice, these ways of providing information to the data subject turn out to be ineffective because they are not read[35] and seem to be written by lawyers for lawyers.[36]

---

[31] Council Directive 95/46/EC, *supra* note 4, pmbl., recital 25.

[32] The Article 29 Working Party has tried to provide a solution in a rather broad definition of the concept of personal data. It suggests that in order to find that data relate to a person, they must contain an element of content, a purpose element, or a result element. Only then, says the Working Party, can the data be classified as personal. A "content" element is present when it relates to a person in the most common understanding of the word, *e.g.*, an RFID chip in a passport. A "purpose" element is present when the data are (likely to be) used with the purpose to treat an individual or influence his behavior, *e.g.*, a call log for a telephone. A "result" element is present when the use of data may have an impact on a person, *e.g.*, monitoring of a taxi's position to optimize service having an impact on drivers. *Opinion 4/2007 of the Article 29 Data Protection Working Party on the Concept of Personal* Data, at 10–11 (20 June 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[33] *A Comprehensive Approach on Personal Data Protection in the European Union*, *supra* note 11, at 5. Furthermore, in data-mining situations, decisions are taken about persons based on data that fit a profile, but these are not necessarily applicable to every individual affected by this decision.

[34] Cavoukian, *supra* note 5, at 90.

[35] In the Eurobarometer report of 2008 the survey results show that 64% of respondents are aware that organizations that collect personal information must provide individuals with information about their identity, the purpose of the collection, and the intention to share the data with other organizations. Even though this is a high percentage, it may still be doubted whether the respondents have actually read the required statements. THE

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

The other measure, viz., the obligation to register a notification of intended data processing with a data protection authority, is just as ineffective.[37] In practice, individuals rarely consult the registers holding these notifications. These registers are often only used by lawyers conducting due diligence procedures.[38] The complaints about the administrative burden of the notification process have also been frequently brought to the fore.[39] The Commission recognized these complaints and abolished this obligation altogether in its proposal for the revised DPD.

Consequently, consumers feel that present mechanisms as formulated in the DPD do not help them in understanding and exercising their rights.[40] These measures seem intended more to legitimize data processing than to provide consumers with effective tools to enforce their rights. This is especially worrisome because providers consider the publication of their privacy policies to be an adequate way to solicit consumers' express consent to terms.

IV. Accountability

In spite of its assets, the Directive also has several weaknesses as an instrument to protect privacy. An important one is the way in which the Directive deals with the question of

---

GALLUP ORG., FLASH EUROBAROMETER 225: DATA PROTECTION IN THE EUROPEAN UNION: CITIZENS' PERCEPTIONS 31 (2008), *available at* http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[36] Robinson et al., *supra* note 22, at 29 ("Privacy policies are written by lawyers, for lawyers, and appear to serve little useful purpose for the data subject due to their length, complexity and extensive use of legal terminology.") Consumers themselves appear to feel that current mechanisms do not help them to understand their rights. *Cf.* OFFICE FOR DEVELOPED & TRANSITION ECONOMIES, CONSUMERS INT'L, PRIVACY@NET: AN INTERNATIONAL COMPARATIVE STUDY OF CONSUMER PRIVACY ON THE INTERNET 26–27 (2001), *available at* http://www.consumersinternational.org/media/304817/privacy@net-%20an%20international%20comparative%20study%20of%20consumer%20privacy%20on%20the%20internet.pdf.

[37] The Commission is of the opinion that the Directive already offers the Member States the possibility to provide for wide exemptions from notification in cases where low risk is involved or when the controller has appointed a data protection official. At most, some further simplification would be useful and should be possible without amending the existing Articles. *Commission of the European Communities First Report on the Implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265 final (15 May 2003).

[38] ROBINSON ET AL., *supra* note 22, at 32.

[39] Robinson notes that the cost to the US national economy just for reading each privacy policy was estimated to be $365bn, based on the length of time it takes to read a privacy policy and the monetary value of that time. *Id.* at 30. Because the current obligation to notify all data processing operations to the DPAs is considered a cumbersome obligation which does not in itself provide "any real added value for the protection of individuals' personal data," the Commission proposes to revise and simplify the current notification system. *A Comprehensive Approach on Personal Data Protection in the European Union*, *supra* note 11, at 10.

[40] ROBINSON ET AL., *supra* note 22, at 29.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

accountability. The Directive was written at a time when data processing involved filing systems and computer mainframes. The roles of data subject, processor and controller were easily assigned and relatively clear to all concerned. Thus, obligations and procedures could easily and clearly be linked to each role. In the ICT-pervaded society, however, personal data is everywhere. As noted earlier, technological developments, such as cloud computing and social networking services, make personal data increasingly difficult to track and control. In this world, where unlimited data is passing from individuals to organizations, between organizations and between individuals worldwide, accountability is increasingly difficult to organize. This is worrisome because the majority of this data is personally identifiable. Virtual representations of us are available in a multitude of locations worldwide and are often under the control of third parties in foreign jurisdictions. Even though one of the dual purposes of the DPD—i.e., promoting cross-border dataflow—seems to be enabled in this way, it simultaneously raises the question of whether the equally important aim of privacy protection is not endangered.

V. Oversight

It has often been stated that one of the values of the DPD is the establishment of independent supervisory bodies, the Data Protection Authorities (DPAs).[41] The Commission itself poignantly proclaims that "[t]hey are independent guardians of fundamental rights and freedoms with respect to the protection of personal data, upon which individuals rely to ensure the protection of their personal data and the lawfulness of processing operations."[42] However, the way they are institutionalized in the DPD has increasingly turned out to be inadequate for guaranteeing the users' fundamental rights. The data protection agencies see themselves as struggling uphill with few resources, a view illuminated in the often ambiguous and weak laws they are tasked to enforce against more powerful interests in the commercial and technological worlds.[43] Provisions for remedies and liability are quite broad and allow data subjects apparently ample opportunity to obtain compensation for damages. However, the approach does not function in practice because the value of the damages likely to be incurred is difficult to calculate. In fact, there are often no immediate damages, and their extent may be difficult to quantify. If misuse or abuse of data is unlikely to have serious consequences or any consequences at

[41] According to Bennett and Raab, because normative information privacy principles are not self-enforcing, public agencies play a role in the enforcement and oversight of data protection legislation. The most important are the supervisory bodies required under the EU Directive. BENNETT & RAAB, *supra* note 21, at 133.

[42] *A Comprehensive Approach on Personal Data Protection in the European Union*, *supra* note 11, at 17. In the Proposal the Commission has taken note of these complaints and introduced a centralized European Data Protection Board with stronger enforcement powers.

[43] BENNETT & RAAB, *supra* note 21, at 146.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

all, there is no incentive for data controllers to comply with the DPD.[44] For DPAs, consequently, it is hard to enforce the DPD. An additional problem is that many DPAs combine duties of complaint handling and promotion of good practices along with their primary sanctioning roles.[45] This does not make their role clear to the regulated. There is a generally-felt need to clarify the enforcement means available to the DPAs, the scope and impact of enforcement actions, and the choice of enforcement priorities. It seems as if there is a multitude of formal legislation and policy aimed at protecting privacy, even while much unchecked processing of personal data occurs in spite of the efforts of the supervisory agencies.

VI. Process Orientation, Not Outcome Orientation

It can be contended that these weaknesses of the Directive are indicative of a regulatory framework that focuses not only on important principles of data protection, such as legitimacy, transparency, and purpose binding , but also on the processes used to implement these principles, without considering whether the processes promote the outcome. It might even be argued that the Directive in this way creates an organizational culture that focuses on meeting formalities to create regulatory compliance on paper, rather than promoting effective good data protection practice.[46] This accumulation of weaknesses does not give much hope that the more profound question of whether the DPD achieves its underlying first purpose of protecting individuals' privacy can be answered positively. The scope of this article does not permit consideration of whether the other purpose of the DPD (promoting the free flow of information) is achieved, but the lack of harmonization of regulations implemented in the member states, as well as the difficulties experienced by international companies in exchanging information across borders, could point to a similar conclusion.[47]

As noted, the Directive contains a well-thought-out set of principles which goes a long way in safeguarding the fundamental right to privacy of European citizens. Its shortcomings, as

[44] *Id.* at 35. Suggestion by the Commission is made with the goal of strengthening the existing provision on sanctions by including criminal sanctions in cases of serious data protection violations. In addition, DPAs and other associations representing data subjects' interests should also be granted the power to bring an action before the courts when infringements of data protection rules affect more individuals than one. *A Comprehensive Approach on Personal Data Protection in the European Union*, *supra* note 11, at 9. This proposal returns in the unofficial Proposal. The suggested fines that may be imposed by supervisory authorities in the Proposal are quite daunting—up to a maximum of €1,000,000.

[45] Many are the roles of the data-protection authorities. Bennett and Raab denote seven roles: ombudsmen, auditors, consultants, educators, negotiators, policy advisers and enforcers. BENNETT & RAAB, *supra* note 21, at 134.

[46] ROBINSON ET AL., *supra* note 22, at 39.

[47] *Cf.* GALLUP ORG., *supra* note 35.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

described above, stem mostly from its emphasis on data protection rather than on the fundamental rights of the data subjects whose data are processed. This is especially evident in its orientation on the process rather than on the outcome of its regulatory measures. Accountability and oversight shortcomings, as well as a lack of effective implementation of the consent principle, are the consequence. As argued before, then-prevalent economic motives behind securing an easy and unimpeded flow of information between member states made this focus on personal data the *raison d'etre* of the Directive. The foregoing analysis of the DPD's struggle against turbulent developments in the data processing landscape demands a shift away from the Directive's ambivalent foundation to a clear and convincing choice for the basic principles of protecting the privacy of the data subjects. In the next section, I will turn to the principles underlying the concepts of privacy and data protection in a consideration that aims to discover whether concentrating more on these principles could provide a better basis for a data protection regime to protect the privacy of individuals in the Internet era.

D. The Concept of Privacy

The meaning of the concept of privacy has proven elusive.[48] Many are characterizations and many are efforts by legal scholars and philosophers to reinterpret the meaning of privacy in order to adjust it to the prevailing technological and societal changes.[49] In the Western world, the assertion that privacy occupies a central place in the western liberal tradition, as an essential component of self-definition and individual development, will not find much objection.[50]

I. Human Dignity

In a discourse about privacy, it is my opinion that much can be learned if we return to the basic concept of human dignity. In Kantian philosophy, dignity is an indispensable part of human nature. As noted before, the German Constitution, as inspired by Kantian philosophy, clearly sets out that personality rights are a core value. The free unfolding of

---

[48] Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. & TECH. L. REV. 115, 123–29 (2005) (presenting a helpful and succinct overview of the concepts of privacy and privacy laws). *See also* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand D. Schoeman ed., 1984).

[49] BENNETT & RAAB, *supra* note 21, at 7. According to Bennett and Raab, the concept has "an aesthetic and humanistic affinity with individual autonomy and dignity." But also that it can be justified in "philosophical, political, or utilitarian terms."

[50] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2009) ("Commentators have declared it 'essential to democratic government,' critical to 'our ability to create and maintain different sorts of social relationships with different people,' necessary for 'permitting and protecting an autonomous life,' and important for 'emotional and psychological tranquility.'"). It has been hailed as "an integral part of our humanity," "the heart of our liberty," and "the beginning of all freedom." *See also* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

personality is the guiding principle that obligates the state to adhere to the rule of law, requiring that legal measures have a legal basis and discernible content, provide fair notice, and be necessary and proportional to the ends they seek to accomplish.[51] These are, of course, very much the common *Rechtsstaat* principles, but more importantly, they also remind us of privacy concepts such as the proportionality principle, the legitimacy principle, transparency, and purpose-binding. It can be observed that the German Constitutional Court carved out a private, intimate sphere, in which the individual is able to develop his personality free from external coercion. Indeed, by the important work of the German Court, the Kantian ideal of moral autonomy was thus adjusted to the conditions of the modern age.[52]

This is further illustrated in the German Constitutional Court's case law. The well-known *Census* case (*Volkzählungsurteil*) shows how this principle is made concrete.[53] The Court says that people are depersonalized when they are treated merely as sources of information. In fact, this approach jeopardizes their essence as spiritual-moral persons. Nevertheless, the Court also takes notice of an overriding public interest in the census, but only to the extent that it is necessary to satisfy the public interest. It is interesting to note that the Court regarded the rights of the individual in the interconnection of being community-bound and community-connected. The community as a whole has obligations to the individuals, just as the individuals are responsible as rights-holders. Still, dignity, as such, acts as a higher law by which individuals and society are judged.[54]

Several other cases are illustrative of how the Court viewed the overriding importance of the value of dignity. The *Mephisto* case is often pointed to as the way in which the Court defended the reputation of even a deceased actor by giving an injunction against the publication of a novel in which the memory of this deceased actor was defamed.[55] In other words, freedom of communication may have to yield to the value of dignity. This underlining of the need to preserve the integrity of human personality against the intrusive influences of the outside world resonates even more in the *Lebach* case.[56] The privacy

[51] Edward J. Eberle, *Human Dignity, Privacy and Personality in German and American Constitutional Law*, 1997 UTAH L. REV. 963 (1997).

[52] *Id.* at 1000.

[53] Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], Case No. 1 BvR 209/83, 15 Dec. 1983, 65 BVERFGE 1 (Ger.).

[54] Eberle, *supra* note 51, at 1010.

[55] Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], Case No. 1 BvR 435/68, 24 Feb. 1971, 30 BVERFGE 173 (Ger.).

[56] Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], Case No. 1 BvR 536/72, 5 June 1973, 35 BVERFGE 202 (Ger.).

interest a convicted robber had in being let alone resulted in the halting of a planned television broadcast so as to allow him to concentrate on his reentry into society. The arguments of the Court are, in fact, a small step on the way to a right of informational self-determination.[57] These decisions of the German Court illustrate how, at least in the context of the German Constitution, personal autonomy is an aspect of human dignity which unfolds in a manner consistent with moral obligations.

II. Autonomy

The connection that the German Court made between autonomy and human dignity calls for some elaboration of the former concept. The concept of dignity implies that man has an intimate sphere in which he is able to develop his personality free from coercion. This basic principle of being free from coercion makes the individual an autonomous person. How does this relate to the connection made in the previous section between the common *Rechtsstaat* principles and privacy concepts such as proportionality and legitimacy? In an attempt to clarify these relations, it is helpful to introduce the understanding of the concept of privacy as entailing a concern about intrusion or invasion of a "private zone." In today's information society, this zone is interpreted as a zone with information about oneself, about one's self-identity[58]. However, much of the information about one's person is out there in the public zone—in the "commons"—without any opportunity for the individual to control it. One could object that, when a third party gathers this information, the gathering really is no more than copying, and one could wonder why this should be a cause of concern that requires countermeasures. But there remains a feeling of irritation or dismay when something personal is appropriated by others without our input. Shoemaker contends that this zone contains information about properties that are part of one's self-identity.[59] From this self-identity the individual derives his self-esteem. In his opinion, people need to be able to control this normative zone. In this age of data mining and profiling, publicly available bits of information about oneself are gathered and reconstituted into a new digital identity with which the individual cannot associate. This is what causes the dismay.

Frankfurt has developed a theory of identification that helps to give color to these conceptualizations. He says that a person enjoys freedom of the will when he is free to want what he wants.[60] This freedom allows man to choose what he wants motivated by a

[57] "The rights to the free development of one's personality and human dignity secure for everyone an autonomous sphere in which to shape one's private life by developing and protecting one's individuality." *Id.*

[58] David W. Shoemaker, *Self-Exposure and Exposure of the Self: Informational Privacy and the Presentation of Identity*, 12 ETHICS & INFO. TECH. 3, 13 (2010).

[59] *Id.*

[60] Harry G. Frankfurt, *Freedom of the Will and the Concept of a Person*, 68 J. PHIL. 5 (1971).

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

set of desires that are truly his. These so-called second-order volition capacities of man are about the nature of self-determination. Seen in this context, it can be said that it is not the profile, drawn up without one's influence, providing a wrongful picture of oneself, that gives rise to irritation or distress. Rather, as Agre says, it is the prevention from being able to present my self-identity to others in the manner I see fit.[61] In other words, my autonomy is undermined insofar as I am unable to do what I want with my "self."[62] Informational privacy as conceptualized here concerns breaches of the self which take away the key element of self-determination. This reminds us of the control theory. To have informational privacy is to have control over the access to and presentation of information about one's self-identity.[63] Thus, autonomy is, in my opinion, an essential value that underlies informational privacy.

III. Dignity and Autonomy as Constitutive Elements of the Privacy Concept

At this point, I tender the suggestion to consider the two concepts of dignity and autonomy, as described, as together constituting the foundation of the concept of privacy. The concept of privacy, made up of these fundamental elements, can thus be positioned meaningfully in the ethical and philosophical discourse. The two constitutive concepts of dignity and autonomy, underlying privacy, permit modern man to pursue ideals of life and character, which it would be difficult to achieve were privacy not safeguarded. This view of privacy as a respectful approach of one's fellow man at the same time is conducive to a society where ideals are made possible for a politically free individual. Autonomy and dignity permit a person to see himself as a person with infinite, indeterminate possibilities. In this line of thinking, I follow Benn's argument, in which he says that if the individual has the confidence that he can be himself, he can believe in himself as a person. He then can also not only accept the scrutiny of the other but also value this gaze as respectful regard.[64] My conceptualization goes further. To respect a person involves a two-way process. A person in this sense is a subject with a consciousness of himself as agent, as a chooser, and as one attempting to steer his own course through the world. To respect a

[61] PHILIP E. AGRE, INTRODUCTION TO TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 1, 8 (Philip E. Agre & Marc Rotenberg eds., 1998) (following ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959), "People construct their identities, [Goffman] suggested, through a negotiation of boundaries in which the parties reveal personal information selectively according to a . . . moral code that [Goffman] called the 'right and duty of partial display.'").

[62] Shoemaker, *supra* note 58, at 13.

[63] James Rachels, *Why Privacy Is Important*, 4 PHIL. & PUB. AFF. 323, 331 (1975) (stating that if we cannot control who has access to us, we cannot control patterns of behavior we need to adopt).

[64] Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY at 223, 228 (Ferdinand D. Schoeman ed., 1984).

subject, who is in this sense a person, is to concede that one ought to take account of the way in which the enterprise of that person might be affected by one's own decisions.[65]

As observed above, privacy was first seen as seclusion but this was a seclusion, or a right to opacity, that was grounded in the principle of human dignity[66]. The German Constitutional Court decision in the *Census* case is illustrative here of how the values of dignity and autonomy can be made applicable to the prevailing technological and social circumstances at a certain point in time. In its ruling, the Court established a direct link between the data protection regime and two basic values enshrined in the Constitution.[67] These are the constitutional rights to respect and protection of one's dignity[68] and self-development[69]. Privacy and data protection are intended to foster autonomous capabilities of individuals that are necessary to sustain a vivid democracy. Privacy will operate to reduce or to eliminate pressure brought on by the actual or perceived views of others. The individual will be enabled to exercise his right to self-development.

IV. Control

Besides the foundational values of dignity and autonomy, it has been noted before that the aspect of control is an essential precondition to the right to privacy. Rachels puts it very clearly that "there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of relationships with different people."[70] This view ties in with Goffman's theory of privacy as boundary control,[71] but also with Post's view of the individual personality as being constituted by observance of rules of deference and demeanor.[72] Post argues that intrusion on privacy is intrinsically harmful, because it is defined as that which injures social personality. An individual is entitled to a form of respect. When he is being discredited, for example, because people gossip about him, this can be seen as excluding

[65] Benn puts it succinctly: "By the principle of respect for persons, then, I mean the principle that every human being, insofar as he is qualified as a person, is entitled to this minimal degree of consideration." *Id.* at 229.

[66] Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[67] Rouvroy & Poullet, *supra* note 25, at 53.

[68] GG, art. 1.

[69] GG, art. 2.

[70] Rachels, *supra* note 63.

[71] ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).

[72] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957 (1989).

the person concerned from a so-called chain of ceremony.[73] This social concept of privacy implicates an understanding of identity maintenance as a core concept of privacy. It involves a protection of relations through which one develops a sense of oneself as unique, i.e., a sense of identity.[74] The aspect of control clearly plays a role in Post's social theory of privacy as well, because the individual possesses the ability to press or waive the territorial claims he holds over the information about him.[75] This ability can be said to empower the individual as an autonomous person. It is also up to the individual to decide who has access to what kind of information about him. The contextual integrity theory of Nissenbaum[76] builds on the same principle of controlling the separation of associations we have with certain people so that we can behave differently with different people or in different contexts. Questions of respect, demeanor, and civility furnish us with social norms, which privacy upholds.

E. Informational Privacy and Informational Self-Determination

The linkage of the notion of the protection of personal data to the concept of privacy has certainly been a fruitful exercise in the past decades. It knows many shortcomings but undoubtedly also contributed towards enhancing the safeguarding of the human rights oriented concept of privacy. It is common to coin this kind of privacy informational privacy.[77]

I. Informational Privacy

This is not a new kind of privacy but, in a sense, a subcategory of the concept. When the widespread use of computers became ever more prevalent, concern soon arose about the potential harmful effects for the personal sphere by the processing and storage of what were often very intimate details about individuals in large databanks. Whereas, up to that point in time, the harm done to the personal sphere was usually spatially defined, viz., in terms of the integrity of the home, thereafter the reputations of all individuals, not only famous personalities, were in danger. In an attempt to create some clarity in the definition of privacy, the concept of informational privacy was introduced.

---

[73] *Id.* at 963 (referring to Goffman, who says that for a complete man to be complete, "individuals must hold hands in a chain of ceremony, each giving deferentially with proper demeanor to the one on the right what will be received deferentially from the one on the left," ERVING GOFFMAN, *The Nature of Deference and Demeanor*, *in* INTERACTION RITUAL: ESSAYS ON FACE-TO-FACE BEHAVIOR 47, 84–85 (1967)).

[74] Jonathan Kahn, *Privacy as a Legal Principle of Identity Maintenance*, 33 SETON HALL L. REV. 371 (2003).

[75] Post, *supra* note 72, at 973.

[76] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

[77] *Compare, e.g.*, Post, *supra* note 72.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

In this same period of time, Alan Westin defined the concept of privacy as "the claim of individuals, groups or institutions to determine for themselves, when, how and to what extent information about them is communicated to others."[78] The emphasis that was put on the control the individual held over information concerning himself even at that time was interesting. The problem is revealed in concerns about the right to self-determination of the individual. Already, there appears a starting point for a discussion about privacy. In this same period, A.R. Miller said that "the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to himself; a power that often is essential to maintaining social relationships and personal freedom."[79] If the individual can no longer decide for himself to what extent he can reveal himself to the outside world, privacy is robbed of its core value, viz., the free opportunity to decide for oneself. This highlights the concept of informational self-determination and the role it plays in safeguarding the concept of privacy. The concepts of dignity and autonomy, it is my suggestion, point the way.

II. Informational Self-Determination

The attempt to understand the concept of informational self-determination finds strong support in the German approach to the concept of privacy. As said, the German Constitutional Court created the basic constitutional right to informational self-determination in the *Census* case.[80] Moreover, German constitutional law bases its protection of privacy on three spheres: The *Individualsphäre*, the *Privatsphäre*, and the *Intimsphäre*. This set of rights is developed by the *Bundesverfassungsgericht* as a manifestation of the general right to personality. The essential characteristic of this set of rights is the control the individual has over the information about his personality that is available to others.[81] People should be enabled to intentionally include or exclude certain features of their personality relative to the role being played in order to retain the integrity and consistency of their personal identities. Informational privacy, closely interconnected with the decisional freedom of the individual, is the key characteristic of the *Bundesverfassungsgericht* policy of protecting privacy. This is the *Leitmotiv* of all three aforementioned spheres of privacy. In other words, informational privacy, informational self-determination, and *Menschenwürde* reinforce each other considerably. The

[78] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

[79] ARTHUR RAPHAEL MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971).

[80] Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], Case No. 1 BvR 209/83, 15 Dec. 1983, 65 BVERFGE 1 (Ger.).

[81] DeSimone, *supra* note 17, at 294. DeSimone contends that this line of thinking stems from the theory of role playing as developed by the German legal philosopher Paul Tiedemann.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

Bundesverfassungsgericht clearly states that: "[S]elf-determination is a prerequisite for a free democratic polity based on its citizens' capacities of civic action and collaboration."[82]

At this point, it is helpful to allude briefly to the way in which the Court has elaborated on this principle of informational self-determination. Protection of individual autonomy is carried out under a subdivision of personality rights, viz., the right to self-determination. It should be noted that the Court did not establish an absolute right, nor did it intend to create a right of control over personal data. The Court states that "[t]he individual does not have a right in the sense of an absolute, unlimitable 'mastery' over 'his' data; he is rather a personality that develops within a social community and is dependent upon communication."[83] According to Paul Schwartz, the Court did not rely on any legal notion of privacy. Instead, it accepted the social nature of information and called for measures to structure the handling of personal data.[84] In that way, the person affected will be able to anticipate who will use his personal data and the purpose for which it will be collected and processed. The State is called upon to create a legislative setting of precise goals before collecting individual data. Because of the deep impact of data processing on the citizen, the right to informational self-determination should be protected by adequate legal measures. Independent monitoring and judicial review will assist the citizen in gaining knowledge of data processing practices.[85] Adequate legislative measures should guarantee that the individual will not run the risk of being impeded in his freedom of expression and acting. In my opinion, this shows a clear link between informational self-determination and privacy with dignity and autonomy as constitutive values.

F. Discussion and Analysis

The essential question at hand, after this discussion of the value of more philosophical and ethical approaches to the privacy question, is whether this approach will point to a solution to the weaknesses detected in the Data Protection Directive, thereby helping to revitalize privacy. Recapitulating these weaknesses, they may be said to boil down to a number of main issues: Accountability, effectiveness of controlling authorities, and especially the lack of control over personal data. This is due to vagueness and uncertainties caused by an unclear definition of personal data and correspondingly unclear transparency measures. It

[82] Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], Case No. 1 BvR 209/83, 15 Dec. 1983, 65 BVERFGE 1, para. 43 (Ger.).

[83] *Id.* at para. 44.

[84] Paul Schwartz, *The Computer in German and American Constitutional Law: Towards and American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675, 690 (1989).

[85] Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], Case No. 1 BvR 209/83, 15 Dec. 1983, 65 BVERFGE 1, para. 46 (Ger.). All legislation must be checked for a valid legislative basis, clarity of norms, and observance of the principles of proportionality.

seems as if the DPD has resulted in an infrastructure where lawyers earn a living without their efforts achieving a better protection of the privacy of the individual in the Internet era. It can be said that the DPD results in an infrastructure which is more process-oriented than outcome-based.[86]

All in all, it appears as if the DPD is fighting a rearguard battle and is sorely in need of modernization. It is therefore promising that the European Commissioner, Viviane Reding, has emphasized that the reform of data protection rules in the European Union is her "top legislative priority."[87] She asserts once again that this can be done by enhancing individuals' control over their own data. I believe, however, that this will not be sufficient in today's networked society. Indeed, I believe that it will be more helpful to go back to the roots and infuse the concept of privacy with its two constitutive elements of dignity and autonomy.

Thus far, I have tried to present arguments for a fresh, renewed look at privacy and its essential constitutive elements in order to point the discussion in a direction which will afford the concept of privacy a new lease of life in the Internet era. In this section, I will elaborate on these principles. It is the aim of this section to show that a return to the roots also provides a helpful basis for the specific review of legislative infrastructures like the DPD.

The recurring weakness in the DPD is that of the lack of control of the individual over his personal data. In the foregoing analysis, I have argued that the introduction of the principle of informational self-determination as an underlying principle may provide a solid ground for the revitalization of the privacy concept. But it is my contention that the control element, in more general terms, is also a precondition of privacy. This interpretation of privacy, or more correctly, informational privacy, goes back a long way—as we have seen. Westin, as a professor emeritus in 2003, started his overview of the social and political dimensions of privacy by repeating his definition of privacy, which he first formulated as far back as 1967, recognizing the concept as an individual's claim to determine what information about himself or herself should be known to others.[88] In the Internet era, it is easy to take the next step and assume that informational self-determination and the control mechanisms provided for in data protection legislative structures are equivalent concepts. After all, the individual today is very much a digital person, for whom his personal data act like proxies for the real self. Still, I agree with

[86] ROBINSON ET AL., *supra* note 22.

[87] Viviane Reding, Vice-President of the European Comm'n, E.U. Justice Comm'r, Your Data, Your Rights: Safeguarding Your Privacy in a Connected World (16 Mar. 2011), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183.

[88] Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 J. SOC. ISSUES 431, 431 (2003).

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

Westin that the individual must have some form of control over information produced about him. In the DPD, the principle of consent is introduced to enable the individual to put the control principle into effect. But, as I have argued, it is exactly this principle that is an eminent example of a severe shortcoming of the DPD, visible in light of confusing new paradigms in the processing of personal data, such as those caused by social network sites.

The consent principle is meant to empower the individual to exercise his decisional power to determine what information about him is disclosed. It needed substance, but this was prominently provided by marketing organizations trying to circumvent easily the question of what a meaningful consent should be.[89] After all, the desire of private sector organizations, such as marketing associations (but also government bodies), to be able to transfer as much information as possible about citizens, was curbed by the general aims of privacy law, such as purpose-binding and data minimization requirements. The choice was then left to the individual whether to agree with the processing of his personal data and, if so, to actively indicate his consent therewith (to "opt-in"). Marketing organizations, however, are strong supporters of the "opt-out" principle, which has a starting point of passive consent. This is less burdensome for them because it allows them to go forward with various uses of personal data as long as there are some means, however inefficient, for consumer objections. As was argued before, the consequence has been that in and by the Internet era,[90] the consent principle has become an empty shell altogether.[91] It is my opinion, therefore, that solely relying on the element of control to revitalize privacy will fall short.

I. Ethical View of Privacy Vis-à-Vis Some Important DPD Weaknesses

Calling in mind the discussion of the principle of informational self-determination, it is worthwhile to attempt to build a bridge between the philosophical/ethical view of privacy, on the one hand, and the legal constructs geared to protect privacy, such as the DPD, on the other. As Rouvroy and Poullet argue, "[privacy is] essential to human dignity and individual autonomy, and translating these moral principles in the legal sphere, privacy is a necessary precondition to the enjoyment of most other fundamental rights and

[89] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶¶ 29–30.

[90] Simitis presciently predicted the same development in the pre-Internet era already. "The process of consent is no more than a 'mystification' that ignores the long-standing experience that the value of a regulatory doctrine such as 'informed consent' depends entirely on the social and economic context of the individual activity." Spiro Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 737 (1987).

[91] Note also Rotenberg's painfully accurate attack on Lessig's reference to a single web certification association as proof that a standard response to questions of data practices is "choice". Rotenberg, *supra* note 89, at ¶ 33.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

freedoms."[92] The analysis of the consent concept by the Article 29 Working Party illustrates aptly how the ethical cornerstones of privacy can be put into legal practice. The Working Party does so especially by placing emphasis on the active involvement of the data subject in expressing his consent with the processing of his data. This action must be well-informed, specific, unambiguous, and freely given. It is interesting to note that from the legal history of the DPD, this need for an unambiguous indication of consent was added.[93] This is much more specific than marketing organizations would regard as desirable. The data subject's autonomy and dignity thus stand a better chance of being safeguarded.

The conditions proposed here for giving the principle of consent substance, and taking ethical principles as their starting point, deserve additional attention in addressing other weaknesses of the DPD. Relevant here especially are the unclear definitions of personal data and transparency measures. In the discussion of the weaknesses of the DPD, special reference was made to the confusion caused by the too-flexible approach of the DPD to defining what, exactly, personal data are. Is the digital shadow, such as an individual's IP address, a true representation of a real and identifiable person in the sense of the DPD? The argument that this technologically-neutral setup of the DPD makes it amenable to any sort of IT development increasingly falters, considering its attendant risks that data processors will not feel any need to abide by the ensuing obligations. As a consequence, the data subject encounters no transparency in the processing of his personal data. The procedures of notification to DPAs, in themselves already outdated, become correspondingly unwieldy and useless. Keeping in perspective the lack of harmonization in oversight measures between the member states, even the second motive for the DPD, viz., the promotion of the free flow of information, suffers under the Directive's obsoleteness. Thus, a reconsideration of the fundamental tenets of the DPD seems called for. This can be done by switching the emphasis from the defense of data to the defense of the foundation stones of the fundamental right to privacy. The German Constitutional Court has shown in several landmark cases how this perspective works out in practice.

It is apposite to refer at this point to the 2008 decision of the German Constitutional Court in which it deepens the foundational work of the *Census* case by interpreting personality rights as encompassing not only informational self-determination but also the right to a guarantee of confidentiality and integrity in information-technology systems.[94] The *Census*

[92] Rouvroy & Poullet, *supra* note 25, at 61. They refer to Burkert, who said that privacy may be considered a "fundamentally fundamental right."

[93] *Opinion 15/2011 of the Article 29 Data Protection Working Party on the Definition of Consent*, at 5 (13 July 2011), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

[94] Michael Scott Moore, *Germany's New Right to Online Privacy*, SPIEGEL ONLINE, 28 Feb. 2008, http://www.spiegel.de/international/germany/0,1518,538378,00.html (last visited 12 Mar. 2012). The court president admitted it was an unprecedented move to introduce a new civil right in this way.

case,[95] stating that people are depersonalized when they are treated merely as sources of information, provides a pointer to the essence of the basic principles which are at stake in protecting privacy in the information society. From these opinions of the German Court, it can be surmised that dignity is a higher law by which individuals and the processing of data about them are to be judged. This constitutional groundwork of the Court is also reflected in its judicial work in the *Esra* case.[96] In a case against the state of Nordrhein-Westfalen in 2008, the Court virtually established a new right to online privacy.[97] By overturning a surveillance law of the state,[98] it established a guarantee of confidentiality and integrity in information systems. In this way, the Court is reading a general right of personality in its decisions on the basic rights of dignity and autonomy,[99] which is creating a barrier against the erosion of privacy in the personal domain during the Internet era. These judgments of the German Constitutional Court go to show that weaknesses of the DPD, such as the question of the definition of personal data and the ensuing lack of transparency about whether personal data are processed, can be successfully mitigated by taking a human-rights view of the values that due respect for privacy can safeguard.

A strong case in point in this respect is seen in the discussion about the propertization or commodification of personal data. It may be said that the idea of the propertization of personal data could conceivably result naturally in the principle of consenting to the use of one's personal data.

Propertization of Personal Data

Especially in American circles,[100] assigning every individual a property interest in his personal data is often seen as a solution to the faltering attempts to structure privacy rules

[95] Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], Case No. 1 BvR 209/83, 15 Dec. 1983, 65 BVERFGE 1 (Ger.).

[96] In the *Esra* case, the Court arrived at the conclusion that information about the core area of private life is subject to absolute protection. It even trumps the artistic freedom of the author of the roman a clef, entitled *Esra*, in which the author depicted his former girlfriend and her mother very vividly and intimately while it contained a traditional disclaimer that all characters in it were invented. Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better Than One Unitary Concept?*, 98 CALIF. L. REV. 1925, 1960 (2010) (citing BVerfG 13 June 2007 (*Esra* case), BVERFGE 119(1), para 88).

[97] Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], Case No. 1 BvR 370/07, 27 Feb. 2008, 120 BVERFGE 274 (Ger.).

[98] The law gave police and state officials too much power to spy on individuals using "trojan horse" software which can be delivered by email.

[99] *Cf.* GG, arts. 1 & 2.

[100] It appears that the property discussion has definitely crossed the Atlantic. See the recent impressive doctoral thesis by Nadezhda Purtova from Tilburg University in The Netherlands. PURTOVA, *supra* note 8.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

for the Internet. The virtue of the propertization argument is that it aims to restore the right of control to the individual in the traditional sense of information privacy. When propertizing personal data, the idea is that those who value their privacy more than others will put a higher price on it. As a consequence, it is only natural that they will require the party interested in processing their data to pay more for it. This will presumably stimulate investment in and promote the use of technology, thereby more or less automatically generating an optimal amount of privacy. Conceptualizing personal data as property will therefore entail negotiations before these personal data are taken and processed.

This free-market assumption, however, fails in two respects. For one, the privacy market is not perfect. This is due to the fact that individuals lack bargaining power as well as the instruments necessary to fully exert their rights. Privacy price discrimination will not occur.[101] Second, the instruments available to the users to exert their rights as consumers suffer from the "blinking twelve" problem, which is a nice way of saying that most people do not understand the nature of graphical computer interfaces that stand between them and the surrender of their personal data.[102] More fundamentally, some of the same problems that arise with any other commodity also exist with viewing personal information.[103] This is caused by the difficult interrelationship of personal information with the Lockean conception of property as the fruit of labor. Personal information as property is justified by viewing it as an extension of one's personality. However, even though the self is the expression of the self to others, this does not entail a right to ownership of this information. This, in turn, comes about by the fact that information, once known to others, cannot be easily eradicated. Moreover, personal information is of a complex nature, because it is both a partial expression of the self and a set of facts, uniquely identifying with respect to the individual. The ownership of personal information is also debatable, because in the Internet Age it is created in the interaction with websites.

Purtova, in her recent thesis, interestingly posits against this critique of the commodification of personal information the so-called *erga omnes* feature of property.[104] She sees in this feature the possibility of a system of rights that provides a degree of

[101] Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 764 (2000).

[102] *Id.* at 754 (coining the "blinking twelve" problem because many Americans already with VCRs did not bother to read the manual, which would instruct them on how to set the time on the recorder, and therefore the display kept showing a blinking twelve).

[103] Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1113–14 (2002).

[104] Purtova, *supra* note 8, at 73 (arguing that there is a logic of property in one's entitlement to defend one's own against the world). The erga omnes effect stems from the discussion in English legal literature as to when a right is admitted into a category of property rights. *Id.* According to some, the right must be alienable, it must die when the object perishes, or it must take effect against an indefinite number of persons until that time (erga omnes effect). *Id.*

control, including control over personal data, which can then be translated into the language of property.[105] By intertwining this theory of the property of information with the Lockean principle that "[e]very man has a property in his own person,"[106] the principle of autonomy is evoked, as is the principle of informational self-determination.[107] Indeed, the control aspect of privacy is very much at play here. If the privacy market were in better shape, the commodification argument might have been the answer to the problems associated with the Internet privacy paradigm. Since this is a mirage,[108] I believe the property argument certainly provides a promising legally-framed approach to implementing the fundamental concepts of dignity and autonomy underpinning privacy in the Internet era.[109]

The discussion about the various aspects of the concept of privacy and their use in creating a totally new legislative regime in the imaginary state of Atlantis, as presented by J. Kang and B. Buchner,[110] ties these apparently conflicting strands of thought of dignity and property together. The debate reported in the article shows a very heated discussion between property and privacy, on the one hand, and between dignity and privacy, on the other. In the end, at the dialogue's closing, the contradiction was seen to be unhelpful. Individual determination is the essential element of both market-based and dignity-based privacy regimes.[111] Indeed, the Counselor leading the discussion decides not to focus on form but on substance. In the aftermath of that dialogue, it is contended that purely formal control does not lead to privacy protection.[112] Control should therefore be questioned as a leading paradigm. Instead, a case is made for a move towards "a constitutive conception of privacy."[113] Suggestion is made to establish some guidelines

[105] *Id.* at 259.

[106] JOHN LOCKE, SECOND TREATISE OF GOVERNMENT ch. V, § 27 (C.B. Macpherson ed., Hackett Publ'g Co., Inc. 1980) (1690).

[107] PURTOVA, *supra* note 8, at 265. Purtova even goes as far as claiming that her theory of propertization of personal data is consistent with the principle of informational self-determination as it occurs in Article 7 of the Data Protection Directive.

[108] Koops & Leenes, *supra* note 48, at 186–87 (deeming the commodification solution "ineffective" and concludes that it "ultimately fails").

[109] Dommering argues in a sense along the same line when he says the organization of a market of personal data will never replace public law supervision but will be a welcome addition. E.J. Dommering, *Recht op persoonsgegevens als zelfbeschikkingsrecht*, *in* 16 MILJOEN BN'ERS? BESCHERMING VAN PERSOONSGEGEVENS IN HET DIGITALE TIJDPERK 83, 98 (J.E.J. Prins et al. eds., 2010).

[110] Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH. 229 (2004).

[111] *Id.* at 263.

[112] Look at the reality TV shows and blogging. Apparently the individuals concerned do not exercise their control to enhance their privacy but rather transform themselves into entertainment packages.

[113] Kang & Buchner, *supra* note 110, at 266.

that achieve a kind of privacy that best harmonizes goals such as autonomy, human flourishing, democracy, or accountability.[114] These profound approaches of the privacy concept in the twenty-first century can be interpreted also from the point of view developed earlier in this article—that seeing privacy as being constituted of the foundational principles of dignity and autonomy.

II. Technological Bridges

Besides the construction of legal instruments, recent technological propositions also have the potential to supply the individual with instruments to wield against the attacks on his privacy in the Internet era. Indeed, Poullet believes that "[i]f technology created the problem, technology can solve the problem."[115]. A frequently-used technological measure to put the individual in control is that of identity-management systems. I believe that identity-management systems incorporating various best practices[116] are a viable measure for putting the individual in control in a user-friendly manner.[117] In the context of my view of privacy, these identity-management systems should be achieved by using various tools, such as federated identity management, audit tools, and "sticky policies."[118]

Other valuable architectural propositions which potentially equip users with the means to understand and act upon the information that is collected and used about them—*e.g.*, in profiling techniques—are Transparency Enhancing Techniques (TETs) and Platform-for-Privacy Preferences (P3P). TETs provide the required insight and feedback about what happens to data collected in profiles, and about how profiles make decisions about individuals.[119] According to the definition of TETs, it is exactly this transparency-enhancing

[114] Schwartz, *supra* note 101, at 761.

[115] Yves Poullet, *Data Protection Legislation: What Is at Stake for Our Society and Democracy?*, 25 COMPUTER L. & SECURITY REV. 211, 223 (2009).

[116] See also the results obtained in EU research projects, such as FUTURE IDENTITY INFO. SOC. [FIDIS], http://www.fidis.net (last visited 12 Mar. 2012), and especially *D16.3: Towards Requirements for Privacy-Friendly Identity Management in eGovernment*, FIDIS (J.C. Buitelaar, M. Meints & E. Kindt eds., 14 June 2009), *available at* http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/2009_06_14_Fidis_D16.3_Reqs_PF_eGov_v1.2_final.pdf. *See also* PRIME - PRIVACY & IDENTITY MGMT. EUR., https://www.prime-project.eu (last visited 8 Mar. 2012); PRIMELIFE—PRIVACY & IDENTITY MGMT. EUR. LIFE, http://www.primelife.eu (last visited 12 Mar. 2012). An effort also worth mentioning here is the introduction of "a new 'species,' the Personal Data Guardian, created through a fusion of law and technology." Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809 (2012).

[117] Poullet, *supra* note 115, at 224.

[118] Marco Casassa Mont et al., *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing* Services, HP LABORATORIES BRISTOL (19 Mar. 2003), *available at* http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf.

[119] See for example the summary descriptions of two PRIME tools in *D 7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools*, FIDIS 57–59 (Mireille Hildebrandt ed., 4 Mar. 2009), *available at* http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.12_behavioural-

and empowering aspect of the individual's right to counteract the intangible actions of the profiling actors that makes them candidates for workable defense mechanisms.[120]

P3P also offers an interesting approach to allowing the individual to exercise his self-determination. P3P facilitates the collection of personal information from individuals visiting commercial sites by enabling a negotiation over privacy preferences.[121] Unfortunately, it appears that P3P experiences many problems in practice and receives many critiques.[122] Nevertheless, P3P's basic purpose of intending to supporting individual determination as to whether to disclose personal data is in line with my view that individual determination is the essential element of a dignity-based privacy regime.[123]

---

biometric_profiling_and_transparency_enhancing_tools.pdf. The PRIME Data Track Tool allows the user to exercise his rights of deletion of, correction of, or access to the data about the user currently stored by a profiling server. Another PRIME tool relevant here is the Assurance Control Function. This is a kind of counter-profiling tool, because it is based on audits, seals, and reputation mechanisms. It will give the user information on the presence of the data controller in blacklists or disclosure lists and will indicate whether the controller has been certified by privacy seals of different kinds. The user can thus reach an informed decision on whether to trust the data controller or not.

[120] I cite in this respect part of the definition formulated in the FIDIS deliverable, *D7.7: RFID, Profiling, and AmI*, FIDIS (Mireille Hildebrandt & Martin Meints eds., 31 Aug. 2006), *available at* http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf.

> The point would be to have some idea of the selection mechanisms (application of profiles) that may be applied, allowing a person adequate anticipation. To be able to achieve this the data subject needs access—in addition to his own personal data and a profiling/reporting tool—to additional external data sources, allowing some insight in the activities of the data controller. Based on this additional information the data subject could perform a kind of counter profiling.

Id.

[121] P3P was developed by a group of private companies, known as the World Wide Web Consortium. *Cf.* TIM BERNERS-LEE & MARK FISCHETTI, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB BY ITS INVENTOR (1999). *See also P3P 1.0: A New Standard in Online Privacy*, PLATFORM FOR PRIVACY PREFERENCES INITIATIVE (12 May 2006), http://www.w3.org/P3P/brochure.html (last visited 12 Mar. 2012).

[122] The Art 29 Working Group of the E.U. has rejected P3P because it leads to an inversion of responsibility, since use of P3P in the absence of a framework of enforceable data protection rules risks shifting the onus primarily onto the individual user to protect himself, a development which would undermine the internationally established principle that it is the 'data controller' who is responsible for complying with data protection principles. It is, of course, interesting that this opinion is exactly contrary to my argument of taking individual freedom of choice as a starting point. *Opinion 1/98 of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data on Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, at 1–3 (16 June 1998), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp11_en.pdf.

[123] Kang & Buchner, *supra* note 110, at 262.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

Lessig, in fact, is a great supporter of P3P, because in his view, it will enable informed and autonomous consumers to negotiate and assert proprietary interest in personal data automatically and efficiently.[124] At least, I do believe with Kang and Buchner that a P3P-like implementation "might become one valuable element among others in an ideal solution set."[125]

Finally, from a system-development perspective, paying special attention to user centricity in Privacy by Design will also hold the potential for putting into practice the principle of the freely-choosing autonomous person.[126] Indeed, Privacy by Design is recognized by the Commission in its plans for the evaluation of the Data Protection Directive as an important measure to ensure that privacy rights are put into action.[127] The Commission prefers to call it "privacy by default."[128] Responsibility for realizing this solution should lie with those who created the risk, i.e., the ICT companies. Privacy Enhancing Technologies may also be of use here, even though they seem to be, by and large, a pet of data-protection commissioners and privacy lobbyists.[129] By appealing to the basic principles of the DPD, such as proportionality and transparency,[130] it is recognized as a viable and necessary proposition to at least set limits to the unrestrained collection thirst of data processors. But this should then be done by embedding it in the data-processing systems and procedures, themselves. In the kind of review of the DPD the Commission and I advocate, the above-mentioned technological measures should and apparently do receive special attention. The traditional data-protection principles should be applied to the new technologies to allow users to put the advantages of these technologies to full and safe use while making them operate fairly and transparently. This will make for an information society that gives due opportunity for man's dignity and autonomy to be put into practice.

---

[124] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160–61 (1999).

[125] Kang & Buchner, *supra* note 110, at 263.

[126] The principles of Privacy by Design can be summarized as follows. Technology should be designed in such a way that as little personal data are processed as are necessary; the ICT system should grant the user effective means for control; designers and users of a new ICT system must take care that the user is informed about the way of functioning of the system; access should be limited to authorized persons; quality of data should be supported by technical means; in case of the use of data for different purposes within the same system, the separate processes should be separated in a safe manner.

[127] Interestingly the Proposal introduces the data protection impact assessment which is to be submitted to the supervisory authority before the processing begins.

[128] Reding, *supra* note 87, at 2.

[129] Koops & Leenes, *supra* note 48, at 187. *But see* J.J.F.M. BORKING, PRIVACYRECHT IS CODE: OVER HET GEBRUIK VAN PRIVACY ENHANCING TECHNOLOGIES 453 (2010).

[130] On the priority of these two data concepts, see Paul De Hert & Serge Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power*, *in* PRIVACY AND THE CRIMINAL LAW 61, 74 (Erik Claes et al. eds., 2006).

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

III. Outcome-Oriented, Not Process-Oriented

It is worthwhile to see what can be learned from the review of the DPD as commissioned by the UK Information Commissioner in 2009.[131] The authors, Robinson et al., do recommend a recasting of the Directive, which should contain a description of globally consistent General Principles. These consist, in their view, of the well-known principles of legitimacy, purpose restriction, security, confidentiality, transparency, data subject participation, and accountability. In other words, the report believes that the general principles of the DPD should be upheld even in today's networked society.

Fortunately, the report also widens its scope to human rights principles.[132] But it does not elaborate on this. Instead, it recommends so-called back-end processes to ensure that these General Principles are respected. Of primary importance is that the General Principles should be matched to real outcomes. This can be achieved by principles-based "front-end" and harms-based "back-end" measures. Measures proposed should be developed, it is suggested, commensurately with the risk that personal data is being exposed to. I mention here the back-end measures which would enable consumers to make a meaningful and constructive choice as to whether to provide the data controller with their personal data. These measures especially concern privacy policies that communicate how an organization intends to achieve the General Principles. They also provide sufficient information to be used, when necessary, for audit and review. Thus, the privacy policy becomes more an instrument for accountability than the privacy notices, which go to serve transparency.[133] Still, these privacy notices can be made more useful by taking an exceptions approach instead of bothering the user with already-known information. They could also be made dependent on the transaction to be entered into.[134]

Finally, relevant from the point of view of girding the data subject with rights of autonomy and self-determination is the fostering of trustmarks since these permit consumers to exercise choice in the market.[135] Indeed, Robinson et al. are convinced that their results-oriented recommendations aim "to protect data subjects against personal harm resulting

[131] ROBINSON ET AL., *supra* note 22.

[132] It is fair to note that the report is aware of the importance of a human rights approach. "Our research indicated broad agreement that a human rights approach is important and should be retained." *Id.* at 47.

[133] *Id.* at 51.

[134] *Id.* at 51–52.

[135] *See D17.4: Trust and Identification in the Light of Virtual Persons*, FIDIS ch. 3, at 16–37 (David-Olivier Jaquet-Chiffelle & Hans Buitelaar eds., 25 June 2009), *available at* http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp17-del17.4_Trust_and_Identification_in_the_Light_of_Virtual_Persons.pdf.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

from the unlawful processing of any data, rather than making personal data the building block of data protection regulations. It would move . . . towards a framework that . . . requires certain fundamental principles to be respected . . . ."[136] In this manner, the DPD will no longer focus so heavily on the process of its measures, instead taking a view that better considers their outcomes.

G. Conclusion

This article began with an analysis of the weaknesses of the 1995 Data Protection Directive in the present Internet society. Even though the Directive evidently suffers from many shortcomings, its essential principles still stand. This is so because these principles can still stand as useful tenets for guaranteeing the right to privacy, on the condition that they are grounded in a more philosophically sound and focused theoretical basis. By using the principle of informational self-determination in the attempt of seeking a revitalization of the concept of privacy, I believe to have shown that the individual can be re-granted a meaningful position in the legislative structure that was once meant to protect his personal data. To achieve this necessary target, I believe to have shown that the DPD should concentrate on the human rights stance and not confuse it with the economic motive of guaranteeing the free cross-border flow of data in the European Union.

It is therefore reassuring to note that human rights, as formulated in Article 8 of the European Convention on Human Rights, have been declared applicable in the economically-inspired legal infrastructure of the E.U.[137] In other words, the revision of the DPD allows a broader view than merely the economic interests of a free cross-border flow of information. As such, a grounding of this revision on the Kantian ideal of an intrinsic human dignity, which acts in support of individual autonomy, is not precluded in advance. In the Kantian view, man owes himself a duty of self-esteem but also a claim to and duty to respect other humans.[138]

In the last section of this article, I have attempted to show how this renewed view of privacy may work out in practice. Adopting Floridi's analysis of man being his information,[139] it can be said that this conception leads to a much broader view of privacy than merely protecting personal data. Indeed, reinterpreting privacy in such a manner makes it possible to take the individual's development, his dignity, and his autonomy as

---

[136] ROBINSON ET AL., *supra* note 22, at 60.

[137] Dommering, *supra* note 109, at 97. Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community art. 6, 19 Dec. 2006, 2006 O.J. (C 321 E) 1, in conjunction with the Charter of Fundamental Rights of the European Union, *supra* note 18, ch. VII, art. 52(3).

[138] ROGER BROWNSWORD, RIGHTS, REGULATION, AND THE TECHNOLOGICAL REVOLUTION 41–43 (2008)

[139] Luciano Floridi, *The Ontological Interpretation of Informational Privacy*, 7 ETHICS & INFO. TECH. 185 (2005).

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press

the principal starting points for giving privacy a new lease of life. This revitalized concept of privacy can be undergirded by technological and system development measures such as Identity Management, TETs and Privacy by Design. The 2008 decision on the right to online privacy of the German *Bundesverfassungsgericht* goes to show how the constitutive concepts of dignity and autonomy make an online right to privacy legally possible and practical. The privacy in Atlantis discussion, where it is advocated that the optimal starting point has the individual being granted a dignity right in personal data, presents a parallel argument that is in line with the results of the analysis presented in this article.

The principle of informational self-determination goes a long way in readjusting the concept of privacy to the present age of staggering computational processing power and confusion as to where accountability lies. It will perhaps be a continually evolving concept, but this article has advocated that it should be grounded in the ethical/philosophical conceptualization of privacy. Essential DPD principles of legitimacy, purpose binding, minimalism, security, confidentiality, transparency, data subject participation, and accountability should be continually reinterpreted and customized, with the primary starting point as leading principle.[140] Concern should no longer be just with banning the processing of personal data, nor with merely redressing the imbalance of power between the information processors and the subjects of that processing.[141] In the discussion to which I have alluded, some workable examples of measures and theories implement this way of thinking. Robinson's plea for a risk-based analysis and his General Principles offer a useful interpretation of how upholding the essential principles of the DPD, just mentioned, could work out in practice today. The echo, in Floridi's definition of the control the individual should have over "his" information,[142] of Westin's definition of privacy from forty years ago seems to support the argument presented in this article that, if adequately redefined, privacy will survive the ravages of time.[143]

In sum, there is no need to discard privacy, but rather a need to revitalize it. In this paper, I have tried to show that by returning to the basic roots of privacy—which is, in essence,

[140] The Proposal takes the same stance and works this out in a modernized setting, but it is still hampered by the double motive for the DPD. It is the digital economy which is to be strengthened or at least not held back by bothersome protection measures for the privacy of its citizens. Note the extensive attempt the Proposal makes to improve consistency of the measures across the E.U. so as to enable a prosperous internal market. "Personal data protection therefore plays a central role in the Digital Agenda for Europe, and more general in the Europe 2020 Strategy."

[141] Yves Poullet & Jean-Marc Dinant, *Towards New Data Protection Principles in a New ICT Environment*, 5 INTERNET, L. & POL. E-JOURNAL 1 (2007).

[142] Floridi, *supra* note 139, at 195 ("[T]he right to informational privacy [is] . . . a right to personal immunity from unknown, undesired or unintentional changes in one's own identity as an informational entity . . . .").

[143] Westin's definition says it is the claim of an individual to determine what information about himself or herself should be known to others. Westin, *supra* note 88, at 431.

formed by the principle of informational self-determination and grounded in the concepts of human dignity and autonomy—it is possible to bestow privacy with a function and reason even in the networked society.

https://doi.org/10.1017/S2071832200020460 Published online by Cambridge University Press