Anisia Mandro

Together as stewards of the fundamental right of data protection
From the notion of consent and accountability to moral responsibility

Abstract
Once falling under the right to privacy as a mere sub-set, now the right to data protection enjoys a fundamental status. The introduction of the famous General Data Protection Regulation marks especially an important step towards elevating the status of the fundamental right to data protection. The new Regulation provides a stronger framework for contested issues such as consent under a strong accountability regime, however mere compliance with the law is not sufficient. This paper emphasizes the need for an integrated ethical approach, which combines 'the concern for the law' with a very strong emphasis on managerial responsibility for the firms' organizational privacy behaviors. What is ultimately required is a value-driven data protection approach, executed by privacy officers with due concern for the very real impact that data related practices may have on the lives of people.

Keywords: fundamental rights, GDPR, consent, accountability, ethics.

1. Introduction

Privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves[1]

As society faces a relentless pace of technological change, we witness the continuous struggles of governments, companies and individuals to keep up with this fast moving world, especially with regard to data protection. Reflections on the changes happening in front of our eyes are often outpaced by an inherently unpredictable future, which also renders regulation an increasingly elusive exercise.

[1] C. Fried 'Privacy' in Schoeman, F.D. (ed.), *Philosophical dimensions of privacy* (1984, Cambridge University Press) 209.

Against this backdrop, the EU forcefully asserted privacy and data protection as core objectives by conspicuously flexing its regulatory clout with the introduction of the General Data Protection Regulation[2] (GDPR), which came into force on 25 May 2018.

Both the Council of Europe and the EU have expressed shared concerns on protecting the privacy and online identity of individuals, emphasizing especially the fact that even mandatory rules on data and privacy protection can become meaningless if their implementation is not supported by moral and ethical considerations. As expounded upon in the section below, these two organizations were instrumental in elevating privacy concerns, with the Council of Europe initially taking a leading role and the EU now cementing data protection as a fundamental right with the introduction of GDPR.

The protection of our individual online identity, however, did not garner much attention among internet users before affairs such as Snowden or *Schrems* revealed the risks[3] and paved the way for unilateral EU imposed regulatory globalization – through the mechanism dubbed the *Brussels Effect*.[4] These revelations increased EU's resolve to push forward the protection of data while taking an exceptionally uncompromising stance in support of full EU standards of privacy protection. This allowed for the EU to impose its regulatory preferences upon third countries, thereby also exporting the underlying norms and values[5]- most notably the notion of privacy protection as a fundamental right.[6] Now, the right to data protection is more strongly embedded than ever before in our legal and political discourse and can be expected to stay for at least the next decades.[7]

GDPR outlines highly contentious issues as consent, while advancing the accountability principle. This approach aims towards rebalancing the relationship between individuals and data collectors to the benefit of the former.

---

[2] The General Data Protection Regulation [2016] OJ 119/89.

[3] Statement Of The Article 29 Working Party On The Consequences Of The Schrems Judgment. (2016). For further information follow: <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf>.

[4] H. Hijmans, 'The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU' Vol31 (2016) Springer.

[5] Ibid.

[6] A. Brandford, 'The brussels effect' (2012) 107(1) Northwestern University Law Review.

[7] B. van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' 2017. In Leenes, R., Van Brakel, R., Gutwirth, S., & De Hert, P. (Eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures* (2017, Vol36, New York, Springer).

However, considering the ethical implications of the digital era- challenging not only existing data protection principles, but also our (shifting) societal mores and values- mere compliance with GDPR is not enough. Data protection should thus cannot be regarded from a purely legal or administrative perspective.

Therefore, this paper explores the urgency of an ethical reflection at the intersection of the digital environment and fundamental rights. Principles such as consent[8] or accountability,[9] once simple concepts, spur a lot of discussion when considered under the GDPR. This paper will argue that consent should be seen in the light of an overarching principle of accountability, where any data privacy related issues should be principally guided by ethical considerations. This approach emphasizes organizations' corporate social responsibility.

2. Data protection as a fundamental right

The origins of the right to data protection can be partially traced to the data protection rules from northern European countries[10] during the 1970s, and the Council of Europe Resolutions on data processing.[11] Indeed, the Council of Europe issued the first frameworks for data protection on a European level.[12] Interestingly enough, early instruments developed for the protection of data were mostly announced as relating to the right to privacy. Rather than a self-standing right, data protection was seen as a subcategory of the fundamental right to privacy. Such was the case also with the Council's Resolutions with regard to

---

[8] The General Data Protection Regulation [2016] OJ 119/89. See: Articles 4, 7, 8.

[9] Ibid. See: Articles 22, 25, 35, 37-39.

[10] Supra 7 at 2. See also: B. Van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4 no.4 *International Data Privacy Law* 307.

[11] U. Dammann, O. Mallmann and S. Simitis, '*Data Protection Legislation: An International Documentation' Engl.–German: 'Eine internationale Dokumentation: Die Gesetzgebung zum Datenschutz'* (Frankfurt am Main: Metzner 1977); F. W. Hondius, '*Emerging Data Protection in Europe'* (Amsterdam North-Holland 1975); H. Burkert, '*Freedom of Information and Data Protection'* (Bonn: Gesellschaft für Mathematik und Datenverarbeitung 1983).

[12] Council of Europe Resolution (73)29 'On the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector' (1973); Council of Europe Resolution (74)29 'On the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector' (1974).

protecting the privacy of individuals vis-à-vis electronic banks. These Resolutions regarded the processing of data, which takes place in the private and public sector, as integral part of and falling under the right to privacy.[13]

Gradually the EU started to engage in the field of the protection of data by adopting a slightly different stance on data protection than the Council of Europe, which regarded the matter through a human rights lens. Within the EU the processing of the data was two-faceted. Firstly, it was partially seen as an *economic matter*, as the EU traditionally focused on perfecting the internal market- in this particular case accommodating the free flow of data. This is reflected by the legal basis of Directive 95/46 was Article 100a of the Treaty Establishing the European Community, which indeed concerned the regulation and functioning of the internal market. Secondly and similarly to the perspective of the Council of Europe, the EU also connected the right to data protection to the fundamental right to privacy.[14] This was also reflected in the data protection Directive that preceded the GDPR[15], where under the Article 1, concerning the objective of the Directive, it is held that Member States should offer protection to *fundamental rights* and freedoms of natural persons, and in particular their right to privacy with respect to the processing of data.

Since the entry into force of the EU Charter of Fundamental Rights (Charter) in 2009, the right to data protection has enjoyed fundamental right status. This happened after the European Court of Human Rights (ECHR) had already acknowledged that it *partly* fell under the protective scope of Article 8 of the European Convention of Human Rights (ECHR) which refers to the right of respect of private life. Following this, Article 7 of the Charter guarantees the right to privacy, while the following Article 8 introduces the right to data protection. The ultimate interpretative authority of all EU law, the European Court of Justice (CJEU) is also clear in its position with regard to data protection. Dating back to the time when the Directive was still in effect, the Court reaffirmed the status of the right to data protection in its *Coty*

[13] The Resolution (74)29 of the Council of Europe (on the public sector) also stated explicitly 'that the use of electronic data banks by public authorities has given rise to increasing concern about the protection of the privacy of individuals' 87.

[14] See G. González, '*The emergence of personal data protection as a fundamental right of the EU*' (2014) Vol. 16 Springer Science & Business chapter 5.

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 'On the protection of individuals with regard to the processing of personal data and on the free movement of such data'.

judgment, [16] regarding it as a fundamental right of every person while making reference to Article 8 of the Charter and Directive 95/46 and considering the overall implementation of the Directive in relation to the mentioned Article 8 of the Charter. Additionally, the Court in *Digital Rights Ireland* maintained that the Retention Directive 2006/24 did not provide clear and precise rules governing the interference with the *fundamental rights* enshrined under Article 7 and 8 of the Charter.[17]

Since the days of mere 'engagement', the role of the EU in the field of data protection has evolved significantly. With the introduction of GDPR the Union now decidedly assumed a leading role as it effectively exports its data protection regulatory regime and respect for a fundamental right. Importantly, the rights to privacy and data protection are no longer used as interchangeable concepts. By the removal of seemingly all reference to privacy, data protection has been fully disconnected from the right to privacy- at least on a terminological level.[18] As a fundamental right on its own, it now is essentially comparable to other more classic human rights such as the right to a fair trial, the right to privacy or freedom of expression.[19] This is also reflected in the legal basis by which the GDPR was adopted. Contrary to Directive 95/46, the GDPR is founded on Article 16 of the Treaty of the Functioning of the European Union, which safeguards protection of the data.

The new Regulation thus affirms the position of the EU as the guardian of the individuals' data while very importantly introducing the right to be forgotten, data portability and accountability. It also a included clearer notion of consent with stricter requirements.[20] GDPR guarantees full protection of individuals with consistent and clear obligations to all stakeholders involved in the process. The extraterritorial nature of the Regulation also binds companies

---

[16] ECJ, Coty Germany GmbH v. Stadtsparkasse Magdeburg, Case C-580/13, 16 July 2015, para. 30-31.; ECJ, Google Spain v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 13 May 2014, para. 69.

[17] ECJ, Digital Rights Ireland Ltd v Minister for Communications et al., Cases C-293/12 and C-594/12, 8 April 2014, para 65.

[18] See also: L. Costa and Y. Poullet, 'Privacy and the regulation of 2012' (2012) 28 no. 3 *Computer Law & Security Review*. Note that, often, still, the CJEU often discusses the right to privacy (Article 7) and the right to data protection (Article 8) together and in close connection.

[19] B. van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' 2017. In Leenes, R., Van Brakel, R., Gutwirth, S., & De Hert, P. (Eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures* (2017, Vol36, New York, Springer) 2.

[20] P.M. Schwartz, 'The EU-US privacy collision: a turn to institutions and procedures' (2013).

located outside the EU and fines for non-compliance with GDPR can amount up to four percent of global turnover.[21]

However, even a EU level Regulation imposing strict compliance is not enough to keep up with the many challenges that ever-evolving technology poses. The luring new possibilities that come with rapid technological advancement and their seemingly elusive susceptibility to regulation should not be allowed to compromise the protection of private data. Building trust and confidence among the public should defeat public skepticism and the rising tide of fatalism regarding the prospects for privacy protection. This also requires these concerns to be embedded in broader discussions on regulating technology within democratic societies, which prize the rule of law.

As argued in the next section, the GDPR provides a means towards the required trust-building: its basis if formed by a meaningful notion of individual consent under a strong accountability regime and due regard of ethical considerations. The GDPR intertwines legal regulation with ethics. Only by keeping these two inseparable, will its benefits materialize.

3. Guarding the fundamental right of data protection – from the notion of consent and accountability to moral responsibility

3.1. The sensitive notion of consent and accountability under GDPR

Often enough, studies reveal how the cessation in engaging Internet services by users is often correlated to their shared fear that their data is being collected and misused.[22] It is thus not uncommon that data protection is sometimes seen as simply an anachronistic concept, especially in a world where the most basic social and economic processes require easy flow of information.[23] The concerns are usually a result deriving from the misconception that privacy and the free flow of

[21] See Article 83 par. 6, General Data Protection Regulation.

[22] The GSMA Foundation. (2011). GSMA research shows mobile users rank privacy as an important concern when using applications and services. Privacy concerns can prevent consumers' engagement with mobile Internet services. For further information follow: http://www.gsma.com/newsroom/press- release/gsma-research-shows-mobile-users-rank-privacy-as-an-important-concern-when-using- applications-and-services/.

[23] J.M. Rule, *Privacy in peril: How we are sacrificing a fundamental right in exchange for security and convenience* (2007 Oxford University Press) 168.

data are contradictory rather than complementary concepts.[24] This misconception is not unjustified however.

Dating back to the Article 29 Working Party's[25] letter to WhatsApp regarding the terms of service and privacy policy, the former expressed serious concerns especially with regard to the validity of users' consent, specifically on the effectiveness of the mechanisms providing for the effective exercise of this right.[26] Yet, despite efforts to clarify such a notion, there is a growing uncertainty as to what extent proposals to strengthen consent – such as clearer privacy policies and fairer information practices – can actually and potentially overcome a fundamental flaw in this model: *namely the assumption that individuals can understand all facts relevant to true choice at the moment of pair-wise contracting between individuals and data gatherers.*[27]

Following this, Opinion 3/2010[28] suggested the insertion of a general provision in order to reaffirm and strengthen the responsibility of data controllers as well to include an obligation on the latters to take the appropriate measures to implement the principles of data protection.[29] Indeed under GDPR, accountability shifts towards the implementation of internal measures and procedures that put into effect the data protection principles and ensure their effectiveness.[30] Compliance is no longer a merely legal administrative issue, but is to become entrenched in any

---

[24] European Commission, 'Myth-Busting: what Commission proposals on data protection do and don't mean' (2012). For further information follow: <http://ec.europa.eu/justice/news-room/data- protection/news/121207_en.htm>

[25] The Article 29 Working Party is to be replaced by the European Data Protection Board. See Article 68-76 of the General Data Protection Regulation.

[26] Article 29 Working Party Letter to WhatsApp on the updated terms of service and privacy policy. (2016).; For more detailed information on the notion of consent see: Opinion 15/2011 of the Article 29 Working Party. (2011). WP187. This Opinion is partly issued in response to a request from the Commission in the context of the ongoing review of the Data Protection Directive. It therefore contains recommendations for consideration in the review.

[27] H. Nissenbaum, 'A contextual approach to privacy online' (2011) 140 no.4 *Daedalus*.

[28] Article 29 Data Protection Working Party. (2010). Opinion 3/2010 on the Principle of Accountability. WP173.

[29] A. Reghelin, 'The principle of accountability as anticipated by the article 29 Data Protection Working Party' (2017) E-Privacy. For further information follow: http://europrivacy.info/2017/01/09/the-principle-of-accountability-as-anticipated-by-the- article-29-data-protection-working-party/.

[30] Article 5 of GDPR thus introduces the notion of accountability such as "*the controller shall be responsible for and be able to demonstrate compliance with general principles*.

business practice. The new Regulation is replacing '*reporting*'[31] with development of comprehensive *in-house*[32] documentation where in case of an investigation, a company should be able to provide all the relevant information on their activities. WP173 considers transparency[33] and the ability to demonstrate that consent has been obtained[34] vis-à-vis data subjects and the general public as one of the main factors contributing to accountability of data controllers.[35]

However, accountability under the GDPR needs to be addressed realistically and tied to binding principles as technological advancement does not allow for it to remain a rigid concept. This concept helps to go from theory to practice with compliance being the cornerstone. A growing awareness hereof results in stronger determination of all the actors involved in the process of safeguarding the data as it freely flows between collectors on both sides of the Atlantic.

Contextual integrity, as coined by Nissenbaum, ties the adequate privacy protection to norms for specific context, demanding that information gathering and dissemination be appropriate to that context and obeys the governing norms of distribution within it.[36] Thus, consent as one of the legal grounds for processing personal data does not exclude the possibility of other grounds – which could perhaps be more appropriate from both the controller's and data subject's perspective.

However, there are aspects that law cannot always capture. When it comes to collection of data, consumers are considered vulnerable in their dealings with businesses due to a lack of information about and an inability to control the subsequent use of their personal information. Having said this, the data

---

[31] In the former regime, companies were subject to DPAs and provide files and updates on their activities.

[32] Information Commissioner's Office (ICO). Accountability and Governance. For more detailed information follow: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the- gdpr/accountability-and-governance/. See also Article 5(2) GDPR.

[33] See: Article 29 Data Protection Working Party. (2010). Opinion 3/2010 on the Principle of Accountability. WP173. par. 48.

[34] Article 29 Data Protection Working Party. (2011). Opinion 15/2011on the definition of consent. WP187.

[35] D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland, and H. Postigo 'Managing privacy through accountability' (Eds.) (2012, Springer). See also: D. Aspinall, J. Camenisch, M. Hansen, S. Fischer-Hübner and C. Raab, 'Privacy and Identity Management. Time for a Revolution?' (Eds.) *International Summer School, Edinburgh, UK, August 16-21, 2015, Revised Selected Papers*. (2016 Springer Vol. 476).

[36] H. Nissenbaum, 'A contextual approach to privacy online' (2011) 140 no.4 *Daedalus* 32.

gatherers are not only accountable but these organizations also have moral responsibility vis-à-vis consumers, to avoid causing harm while exercising reasonable precautions.[37]

3.2. From consent and organizational accountability to moral responsibility

The protection of data calls for an integrated ethical approach, which combines *'the concern for the law'* with a very strong emphasis on managerial responsibility for the firms' organizational privacy behaviors. Thus inserting ethical reasoning into the organizations privacy programs and more specifically, the moral responsibility to *do no harm*. Scholarly contributions suggest that, at least when compared to businesses, customers suffer to a certain extent from information and control deficits, thereby leaving the organizations with a lot of responsibility which goes beyond legal compliance, but also calls for a moral duty to take reasonable precaution and prevent harm in using this data.[38]

Taking into account the social impact of privacy problems and in particular data breaches, two aspects of morality stand at the center of the complex relationship between those who collect and use the personal data and the individuals who provide their information. These two aspects of morality as emphasized by literature are: *vulnerability* and *avoiding harm*.[39]

Firstly, *vulnerability*, as the term suggests, occurs in a relationship where one of the parties is at a disadvantage with regard to the other. Usually this situation arises when one of the parties suffers a lack of information and control.[40]

Solove in 'I've Got Nothing to Hide'[41] also mentions this type of power imbalance is the root of large-scale privacy harm resulting from the large amount of personal information gathered from the consumers.

Secondly, *'avoiding harm'* should be the guiding pattern for managers of personal data, which exemplifies a sort of minimum moral responsibility to

---

[37] M.J. Culnan and C.C. Williams, 'How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches' (2009) *Mis Quarterly* 673.

[38] *Ibid*.

[39] *Ibid*.

[40] R. Goodin, 'Protecting the vulnerable' (1985); A.M. Marcoux, 'A fiduciary argument against stakeholder theory' (2004) 13 no.1 *Business Ethics Quarterly* 1.

[41] |D.J. Solove, 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) 44: Fall San Diego Law Review 745.

cause no harm when they treat the information, especially when such a treatment unnecessarily fortifies customers' *vulnerable* status.[42]

To this end, privacy, as a legal right, should be conceived essentially as an instrument for fostering the specific yet changing autonomic capabilities of individuals.[43] An approach that aims toward reconstructing trust based on concepts such as fairness and respect goes beyond legal compliance and supports an ethical based approach. The Council of Europe Consultative Committee Convention 108 also emphasizes this approach, through the 'Guidelines on the Protection of Individuals with regard to processing of personal data in a world of Big Data' in January 2017.[44] The Guidelines support an ethical and socially aware use of the data in conformity with values and norms, including the protection of human rights. This principle stipulates that when processing personal data, controllers should adequately take into account the likely impact and the broader ethical and social implications.

As the world of technology becomes more complex, ethical problems associated with it also tend to increase.[45] Theories to address these challenges, however, remain underdeveloped.[46] What is ultimately required is a value-driven data protection approach, executed by privacy officers with due concern for the very real impact that data related practices may have on the lives of people.

4. An ethical approach to data protection

Internet as an ecosystem of different players interacting poses great concerns in relation to the protection of individuals' online identity. However, as legislators now struggle to give answers to questions before considered easy, such as how to define responsibility and the notion of consent; European Data Protection

[42] *Supra* note 37.

[43] See in the same sense C. R. Sunstein, '*Why societies need dissent*' (2005) Vol. 9. Harvard University Press 157; A. Rouvroy and Y. Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in: S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds) Reinventing Data Protection? (2009 Springer, Dordrecht) 46.

[44] Council of Europe Guidelines on the Protection of Individuals Data with regard to Processing of Personal Data In a World of Big Data (2017).

[45] J.H. Moor, 'Why we need better ethics for emerging technologies' (2005) 7 no.3 *Ethics and information technology* 111.

[46] Y.E. Chan and K.E. Greenaway, 'Theoretical explanations for firms' information privacy behaviors' (2005) 6 no.6 *Journal of the Association for Information Systems* 171.

Supervisor – Ethics Advisory Group (EAG), through workshops shows a common effort to consider the ethical impact of the digital era.[47]

The EAG reaffirms that compliance with GDPR is not enough.[48] Though the cliché of fast moving world rings true, that only means that we have to hold tight onto our values by adjusting at the same pace. Following this, consent as a notion is based on how things work in a simpler world making it unrealistic to apply such a notion at its full capacity. Henceforth, it is suggested that consent is more likely to be seen in the light of a broader principle of accountability and ethics should be seen and worshiped as standards that one can count and rely on as they create the base for life.

On this note, organizations should implement strong internal data governance framework, which facilitates the development of a strategic approach to data. Such an approach would ideally be capable of combining the value maximization of information deriving from the data, while minimizing the risks of non-compliance, especially with regard to a breach of trust. A data governance framework designed to overcome data governance failure points, will not only change and transform the way an organization manages the data.

The type of ethical based approach taken, be it an ethical value or policy statement, an ethics committee, or formal data impact assessments including an ethics assessment, should all aim towards reaching the same objective. Such approach would ensure that personal information must be processed in a fair, transparent, responsible and ethical manner.[49] This way, a possible ethical based approach and data impact assessments would show the ability to build trust and transparency with consumers, ultimately delivering long term benefits to both the consumer and the organization. Compliance would thus result in a competitive advantage while further advancing the citizens' fundamental right of data protection.

---

[47] EDPS Newsletter no.50, '*EDPS continues to support debate on ethics in the digital world*' (2016) *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Ne wsletters/Newsletter_50_EN.pdf.*

[48] The EAG continues to work on identifying the ethical responsibilities of online actors.

[49] See also the ICO Report 'Big data, artificial intelligence, machine learning and data protection' points out [par 176] that 'a large organization may have its own board of ethics, which could ensure that its ethical principles are applied, and could make assessments of difficult issues such as the balance between legitimate interests and privacy rights'.; See also the EU ' Guidelines on the protection of individuals with regard to processing of personal data in a world of Big Data' par. 1.3. The Guideline provides that an ethics committee should stand as an independent body with highly qualified selected members who perform their duties impartially and objectively.

To this end, technology cannot dictate our values and ethics at least can help to keep the concrete effect of the GDPR robust. Regardless of how strong the law is if not accompanied with the morality and ethics of every practitioner, can become a dangerous grace for every individual, in a society where even the most powerful is vulnerable.

This is the time when the individual and the processor institution both support a full legal framework where morality and ethics become more important than penalty implementation.

References

Brandford, A. 'The brussels effect' (2012) 107(1) Northwestern University Law Review.

Fried, C. 'Privacy' in Schoeman, F.D. (ed.), *Philosophical dimensions of privacy* (1984, Cambridge University Press) 209.

Chan, Y.E. and Greenaway, K.E. 'Theoretical explanations for firms' information privacy behaviors' (2005) 6 no.6 *Journal of the Association for Information Systems* 171.

Costa, L. and Poullet, Y. 'Privacy and the regulation of 2012' (2012) 28 no. 3 *Computer Law & Security Review*.

Culnan, M.J. and Williams, C.C.'How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches' (2009) *Mis Quarterly* 673

Dammann, U., Mallmann, O. and Simitis, S. '*Data Protection Legislation: An International Documentation' Engl.–German: 'Eine internationale Dokumentation: Die Gesetzgebung zum Datenschutz'* (Frankfurt am Main: Metzner 1977)

González, G. '*The emergence of personal data protection as a fundamental right of the EU*' (2014) Vol. 16 Springer Science & Business chapter 5

Goodin, R. 'Protecting the vulnerable' (1985); A.M. Marcoux, 'A fiduciary argument against stakeholder theory' (2004) 13 no.1 *Business Ethics Quarterly* 1.

Guagnin, G., Hempel, L., Ilten, C., Kroener, I., Neyland, D., and Postigo, H. 'Managing privacy through accountability' (Eds.) (2012, Springer). See also: D. Aspinall, J. Camenisch, M. Hansen, S. Fischer-Hübner and C. Raab, 'Privacy and Identity Management. Time for a Revolution?' (Eds.) *International Summer School, Edinburgh, UK, August 16-21, 2015, Revised Selected Papers*. (2016 Springer Vol. 476).

Hijmans, H. 'The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU' Vol31 (2016) Springer.

Hondius, F. W. '*Emerging Data Protection in Europe*' (Amsterdam North-Holland 1975); H. Burkert, '*Freedom of Information and Data Protection*' (Bonn: Gesellschaft für Mathematik und Datenverarbeitung 1983).

Moor, J.H. 'Why we need better ethics for emerging technologies' (2005) 7 no. 3 *Ethics and information technology* 111.

Nissenbaum, H. 'A contextual approach to privacy online' (2011) 140 no. 4 *Daedalus*

Reghelin, A. 'The principle of accountability as anticipated by the article 29 Data Protection Working Party' (2017) E-Privacy

Rouvroy, A. and Poullet, Y. 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in: S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds) Reinventing Data Protection? (2009 Springer, Dordrecht) 46

van der Sloot, B. 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' 2017. In Leenes, R., Van Brakel, R., Gutwirth, S., & De Hert, P. (Eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures* (2017, Vol 36, New York, Springer).

van der Sloot, B. 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4 no.4 *International Data Privacy Law* 307.

van der Sloot, B. 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' 2017. In Leenes, R., Van Brakel, R., Gutwirth, S., & De Hert, P. (Eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures* (2017, Vol 36, New York, Springer) 2.

Solove, D.J. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) 44 :Fall San Diego Law Review 745.

Sunstein, C. R. '*Why societies need dissent*' (2005) Vol. 9. Harvard University Press 157

Schwartz, P.M. 'The EU-US privacy collision: a turn to institutions and procedures' (2013).

Rule, J.M. *Privacy in peril: How we are sacrificing a fundamental right in exchange for security and convenience* (2007 Oxford University Press) 168.