Corporate Social Responsibility, Shariah-Compliance, and Earnings Quality

Alsaadi, Abdullah; Ebrahim, M. Shahid; Jaafar, Aziz

Journal of Financial Services Research

DOI:
10.1007/s10693-016-0263-0

Published: 01/04/2017

Publisher's PDF, also known as Version of record

Commentary

BIG DATA & SOCIETY

Big Data & Society
January-June 2017: 1–7

DOI: 10.1177/2053951716686994
journals.sagepub.com/home/bds

SAGE

Conceptualising the right to data protection in an era of Big Data

Yvonne McDermott

Abstract

In 2009, with the enactment of the Lisbon Treaty, the Charter of Fundamental Rights of the European Union entered into force. Under Article 8 of the Charter, for the first time, a stand-alone fundamental right to data protection was declared. The creation of this right, standing as a distinct right to the right to privacy, is undoubtedly significant, and it is unique to the European legal order, being absent from other international human rights instruments. This commentary examines the parameters of this new right to data protection, asking what are the principles underpinning the right. It argues that the right reflects some key values inherent in the European legal order, namely: privacy, transparency, autonomy and nondiscrimination. It also analyses some of the challenges in implementing this right in an era of ubiquitous veillance practices and Big Data.

Keywords

Big Data, Global Data Protection Regulation, privacy, veillance, human rights, transparency

In 2009, with the enactment of the Lisbon Treaty, the Charter of Fundamental Rights of the European Union entered into force. Under Article 8 of the Charter, for the first time, a stand-alone fundamental right to data protection was declared. The creation of this right, standing as a distinct right to the right to privacy, is undoubtedly significant, and it is unique to the European legal order, being absent from other international human rights instruments, such as the International Covenant on Civil and Political Rights. However, the European Union 'has neither adequately justified the introduction of the right to data protection in the EU legal order nor explained its content.' (Lynskey, 2014: 572).

This commentary examines the parameters of this new right to data protection, asking what the values underpinning the right are. This piece also analyses some of the challenges in implementing this right in an era of ubiquitous 'dataveillance', or the systematic monitoring of citizen's communications or actions through the use of information technology (Clarke, 1988), and 'Big Data', or the collection of large datasets, which are capable of being searched, aggregated, and cross-referenced (Boyd and Crawford, 2012: 663).

Developing a fundamental right to data protection

The Data Protection Directive of 1995 made no mention to a human right to data protection. As Van der Sloot has argued, the original rules in the Data Protection Directive and related rules 'could best be regarded as principles of good governance', as they were not framed as relating to the human rights of the data subject, but rather focussed on the procedural obligations of controllers (Van der Sloot, 2014).

By contrast, the Global Data Protection Regulation (GDPR) is expressly framed in terms of rights, with Article 1 noting that the Regulation 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.' Given that a right to privacy was well-established in the European legal order for many years before the

Bangor University, UK

Corresponding author:
Yvonne McDermott, Bangor University, Bangor LL57 2DG, UK.
Email: y.mcdermott@bangor.ac.uk

drafting of the Charter, one might wonder what additional value or need was perceived to attach to a standalone right to data protection, especially given that the European Court of Human Rights had, in a number of cases, included data protection rights, including the principle that data should only be used for the limited purpose for which it was gathered, within the ambit of Article 8 of the European Convention on Human Rights on the right to privacy (*Peck*, 2003). Yet, while the right to data protection is closely related to the right to privacy, as well as the rights to freedom of thought, conscience and religion; freedom of expression; an effective remedy, and a fair trial, it has some distinct elements that justify its framing as a standalone right. These elements are: that data should be processed fairly, for specific purposes, and only on the basis of the consent of the person concerned or some other legitimate basis set down in law; the right of access and rectification of data collected, and control by an independent authority (Article 8, Charter of Fundamental Rights).

This new construction effectively elevates established principles of data protection to obligations incumbent on data processers in order to respect the rights of data subjects. In a Habermassian sense, this adds some normative force to the rights holder's claim, insofar as individuals' status is enhanced when they demand compliance with rights, as opposed to some moral obligation (Habermas, 2010: 349). Indeed, the framing of data protection as a right appears to have imposed much greater obligations on private actors than most other human rights – it is difficult, for example, to think of another human right that product designers must take into account when developing new products, as is required under the GDPR.

Therefore, the creation of data protection as a distinct right is both normatively and practically significant. The reasons for the creation of this right are somewhat unclear, however, and the explanations relating to the Charter provide little illustration in this regard. It could be said to have been a reflection of an increasing recognition of the right in domestic law across Europe – the German Constitutional Court had developed the notion of 'informational self-determination', stemming from the constitutional principle of dignity, whilst, in France, the courts had begun to apply data protection rights as a component of the right to liberty (De Hert and Gutwirth, 2009). Yet, this emergence of the right was far from universal across European legal systems, and was couched in rather different terms, being linked to distinct constitutional concepts in those states that had developed the right.

Another theory suggests that the purpose behind the development of the right to data protection in the Charter was to apply the principles of good data processing to those European Union activities that fell outside the Data Protection Directive's remit, namely police and security co-operation (Article 29 Working Party, 2009; Cannataci and Mifsud-Bonnici, 2005). That argument, while attractive, is not supported by the GDPR, which expressly excludes national security activities and the processing of personal data in relation to the Union's common foreign and security policy from the scope of the Regulation's application. I argue below that the creation of the right could be traced to a number of distinct values inherent in the pre-existing data protection framework – namely privacy, autonomy, transparency and non-discrimination – that were perhaps seen as not being fully protected in the pre-Charter fundamental rights framework, and that by placing data protection on an equal footing with existing rights, those values were sought to be protected.

Aside from the uncertain legislative basis for its incorporation, the nature of the right to data protection has sometimes been criticized as being necessarily of a procedural nature, insofar as it 'does not directly represent any value or interest *per se*; it prescribes the procedures and methods for pursuing the respect of values embodied in other rights' (de Andrade, 2012). Determann, for example, is critical of the *Schrems* judgment in pointing out that the claimant 'could hardly show any plausible harm or need of protection' (Determann, 2016: 246). This arguably misses the point of fundamental rights protection; the recognition of rights as fundamental reflect the norms underpinning a legal order (Palombella, 2007), and 'plausible' harm (whatever that might mean) need not be shown for a violation to be proven. This is illustrated by the extensive jurisprudence on the right to a fair trial, for example, where a violation can be found even where the failure to respect a component of the right to a fair trial (such as the right to examine witnesses, or access to a lawyer) has had no discernible impact on the outcome of the trial (Trechsel, 2005). Rights are recognised as such because they protect particular values of a polity, and whilst rights violations often result in serious harm to claimants, this is not a necessary component of a claim because a breach of those rights is an attack on the values underpinning the legal system, and that is the harm that human rights jurisprudence seeks to protect against. It is therefore apposite to examine what values underpin the right to data protection.

Values underpinning data protection as a fundamental right

Privacy

It is clear that privacy, itself a fundamental right, is a value that the right to data protection seeks to protect.

There are different formulations of what the right to privacy entails, spanning from the rather limited idea of privacy only attaching to those intimate matters to which a 'reasonable expectation of privacy' might attach (*Campbell*, 2004), to a wider notion of 'the right to be left alone' (*Von Hannover*, 2004), to an even broader, more recent, idea that the right to privacy is closely related to the protection of one's identity (Hildebrandt, 2006). Data protection clearly fits closest within this third sphere – while some data (such as medical information) might be of the sort to which a reasonable expectation of privacy attaches, other data (e.g. identifying data such as one's address and phone number) falls outside of that scope. Equally, the idea of the right to be left alone presupposes some intrusion into one's day-to-day life, yet the Snowden leaks showed that a great deal of surveillance happens in the background, unbeknownst to those whose data is being collected for those purposes (Lyon, 2014).

Autonomy

Another important value that the right to data protection protects is the autonomy of the individual – this is clear from the continued centrality of consent to the European data protection regime. Recital 7 of the GDPR notes that '[n]atural persons should have control of their own personal data.' The principle of autonomy and the related focus on consent is also clearly linked to the concept of dignity. When German courts developed the notion of 'informational self-determination', it was conceived as related to the constitutional right to dignity (1 BvR 209, 1983). The focus on consent in the right to data protection fits closest with the so-called 'will theory' of rights. The will theory sees the function of rights as being the granting of control to rights holders to subject others to a duty to respect those rights (Hart, 1955). The rights to remedies outlined in Chapter VIII of the GDPR enhance that view, insofar as they bolster that control (Lynskey, 2014).

Yet, the fact that a large degree of consent in this realm is uninformed has been well-documented (McStay, 2013), and some have questioned whether it is desirable to leave it to the individual data subject to improve the level of data protection (Matzner et al., 2016). As the European Commission's Impact Assessment noted, 'individuals are often neither aware nor in control of what happens to their personal data and therefore fail to exercise their rights effectively' (European Commission, 2012). To this end, the GDPR marries the emphasis on autonomy and consent with a parallel focus on the duties of data controllers, regardless of whether data subjects have taken positive steps to enforce those duties (Quelle, 2011). This aspect fits most closely with the 'interest theory' of rights, which sees the function of human rights as imposing a positive duty on actors to respect the interests of others, irrespective of whether the rights-holder claims that duty (Raz, 1984). Indeed, some have argued that the focus on data controllers in the GDPR is inherently paternalistic, insofar as it requires an assumption of the will of the rights holder that has not been expressly articulated (Quelle, 2011). However, given the degree to which research has shown people to be oblivious to the terms and conditions that they willingly sign up to, it would seem that placing some of those obligations on services to protect the data of individual users is both proportionate and necessary.

Transparency

Many authors have commented on the power asymmetries inherent in the area of data protection (Lynskey, 2014), given the issues surrounding consent and knowledge, as mentioned above. The GDPR attempts to address this fact, by defining 'consent' as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Article 4(11), GDPR). Pursuant to Article 7, any request for consent should be intelligible, accessible and in clear and plain language; Recital 58 of the GDPR explicitly links this requirement to 'the principle of transparency'. This formulation is 'information-forcing' and addresses the imbalance of power, insofar as it 'force[s] the disclosure of information about data transfer and use' (Schwartz, 2004: 2100). It is for this reason that De Hert and Gutwirth have argued that, while the right to privacy could be defined as a 'tool of opacity' that sets limits for the normative exercise of power, the right to data protection is a 'tool of transparency', which channels the exercise of that normatively accepted power (De Hert and Gutwirth, 2006).

Non-discrimination

Related to the principle of transparency underpinning the GDPR is a recognition that the collection and processing of data should be carried out in a manner that prevents discriminatory effects on persons 'on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation' (Recital 71, GDPR). To that end, the GDPR establishes a right not to be subject to a decision solely based on automated processing, including profiling, defined as the use of personal data to analyze or predict certain aspects of a person,

including their health, behaviour, movements and personal preferences (Article 9, GDPR). Further, the processing of personal, biometric or genetic data for the purposes of identifying an individual or revealing any their protected characteristics (Article 22, GDPR) is expressly prohibited, subject to a number of exceptions.

These prohibitions recognize that such processing can have an inherently discriminatory effect, and discrimination is one of the potential harms listed in Recital 75 of the GDPR. It could be argued that the right to data protection protects one's 'future life', insofar as the collection of data may not cause any harm at the time of its collection, but the potential that this data can be processed at a later date to profile or make assessments about the person or group of persons in question. The knowledge that data can be collected in bulk and stored for future processing may have a 'chilling effect' on society (Intelligence and Security Committee of Parliament, 2015).

The right to data protection and in an era of Big Data

The contemporary context of ubiquitous veillance practices and the increased focus on the collection and processing of Big Data poses some unique challenges to the right to data protection. Before turning to two specific challenges, it is important to clarify the meaning of both 'veillance' and 'Big Data'. Mann has distinguished between three types of veillance – the classic 'surveillance', when a person is being watched from above, 'sousveillance', when the person themselves is doing the watching, and co-veillance (or mutual watching) (Mann, 2016: 2). Owing to advances in technology, '(a) there is virtually no limit to the amount of information that can be recorded, (b) there is virtually no limit to the scope of analysis that can be done – bounded only by human ingenuity, and (c) the information may be stored virtually forever' (Rouvroy and Poullet, 2009). Bakir has referred to the new phenomenon of 'veillant panoptic assemblage', where data gathered through the ordinary citizen's veillance practices finds its way to state surveillance mechanisms, through the corporations that hold that data (Bakir, 2015). Big Data is a notoriously difficult concept to find a commonly accepted definition for (Ward and Barker, 2013), but a number of key features of Big Data have been identified, including: the huge volume of data, the speed at which it is collected, the variety of data, its relational nature (allowing linkages to be made to other data sets), and potentially exhaustive scope (Kitchin, 2013: 262).

The first challenge to protecting the right to data protection today is the ubiquity of 'volunteered' data, particularly through the rise in wearable devices and social media networks, although the users of such devices may not think of themselves as volunteering data to others (Lyon, 2014). The rise in the so-called 'quantified self', or the self-tracking of biological, environmental, physical, or behavioural information through tracking devices, Internet-of-things devices, social network data and other means (Swan, 2013) may result in information being gathered not just about the individual user, but about people around them as well. Thus, a solely consent-based model does not entirely ensure the protection of one's data, especially when data collected for one purpose can be repurposed for another.

Secondly, as revealed by the Snowden leaks, mass surveillance is seen as a means to prevent future crimes, such as terrorist attacks and cyber-attacks, and the 'watchers' are less visible than in the past, given that a great deal of their surveillance is by means of 'dataveillance', or surveilling online and communications data rather than physical movements. (Graham and Marvin, 2001; Richards and King, 2013) According to Waldron, any 'theory of rights will face difficulties about the interests it identifies as rights, and the terms in which it identifies them. Those disagreements will in turn be vehicles for controversies about the proper balance to be struck between some individual interest and some countervailing social considerations' (Waldron, 1993: 30). The correct balance to be struck between the interests protected by the right to data protection, as outlined above, and whether the curtailment of some aspects of that right constitutes as necessary and proportionate measure to protect national security will continue to be a subject of debate for many years to come.

In addition, the right to data protection comes into conflict with the interest of international co-operation in security matters and, more generally, companies' desire to allow the free transfer of data from its operations in an EU state to one of its operations in a third country. Much focus in the literature on transfer of data has been on the adequacy of protection with data transfers to the United States of America, which is unsurprising given the focus on the adequacy of the Safe Harbour Agreement in the *Schrems* decision (*Schrems*, 2015), and analysis of its successor, the EU-US Privacy Shield (see, e.g. Article 29 Working Party, 2016). However, the European Commission has also decided that data can be transferred to states that are not particularly renowned for their data protection regimes, including Argentina, Israel, Uruguay and New Zealand (European Commission, 2016), having deemed that those states offer an adequate level of protection of data (Determann, 2016). As regards the Privacy Shield, it remains to be seen how the results of the 2016 Presidential election in the United States

will impact upon the perceived sufficiency of data protection there. Hufbauer and Jung (2016) noted that the real test for US data protection would be the impact of the Trans-Pacific Partnership trade agreement, which had as one of its aims the free flow of data and an end to so-called 'data localization' (p. 2), but the President Elect has already signalled his opposition to the Trans-Pacific Partnership Agreement (TPP), which has not yet been ratified by the USA (Yuhas, 2016). From an EU point of view, there is reason to believe that surveillance activities will be even more enhanced and possibly more overt under the new President than his predecessor (Glaser, 2016); whether Privacy Shield will continue to satisfy citizens, companies, governments and intergovernmental organizations in this new political climate remains far from certain.

Lastly, a word of caution should be sounded on the increasing trend towards using algorithms to predict future crimes (de Goede, 2014). This form of 'social sorting' (Lyon, 2002) has the inherent danger of perpetuating discrimination and assumptions about certain strands of populations. The accuracy these Big Data methods to accurately predict potential future events might be called into question. We can point to a number of examples, including Google's unsuccessful attempts at health diagnostics (Lazer et al., 2014) and, most recently, the use of analytics to predict the US election results (Carter, 2016), to question the utility of Big Data to predict future events. This trend risks limiting individuals' human rights and freedoms, insofar as people self-regulate, being aware of 'a state of conscious and permanent visibility', in the sense of Foucault's Panopticism (Foucault, 1977: 201). Moreover, the use of Big Data as a profiling tool can have the impact of creating 'the very scenarios it seeks to prevent' (Carlson, 2016: 53) by turning an innocent citizen into a terrorist suspect through the collation and interpretation of pieces of their data; data, in this sense, becomes 'performative' (Raley, 2013: 128).

Conclusion

This piece examined the principles underpinning the human right to data protection and argued that this unique and newly created right reflects some key values inherent in the European legal order, namely privacy, transparency, autonomy and non-discrimination. The contemporary context of enhanced veillance (both by the state and fellow citizens), the repurposing of data, the globalization and international cooperation in data processing and collection, and the increased use of algorithms to predict future risks undoubtedly present challenges for the realization of the right to data protection. In a changing global order, there is a greater need than ever before to reflect on the importance of the principles underpinning that right to our society, and to strengthen the realization of the right to data protection as a fundamental human right owed to all individuals.

Cases and legislation

Cases

Judgment of 15 December 1983, Bundesverfassungsgericht, Germany 1 BvR 209/83, BVerfGE 65.

Campbell v. Mirror Group Newspapers Ltd, House of Lords, United Kingdom [2004] UKHL 22.

Peck v. United Kingdom, European Court of Human Rights (2003) 36 EHRR 41.

Schrems v. Data Protection Commissioner, Case C-362/14, Court of Justice of the European Union, 6 October 2015.

Von Hannover v. Germany, European Court of Human Rights (2005) 40 EHRR 1.

Treaties and Legislation

International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995.

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01.

Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

Explanations Relating to the Charter of Fundamental Rights, 14 December 2007, 2007/C 303/17.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 27 April 2016.

Acknowledgement

The author would like to thank the symposium editors for their comments on an earlier draft.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Article 29 Working Party (2009) The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (accessed 9 November 2016).

Article 29 Working Party (2016) Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (accessed 9 November 2016).

Bakir V (2015) ''Veillant panoptic assemblage'': Mutual watching and resistance to mass surveillance after Snowden. *Media and Communication* 3(3): 12–25.

Boyd D and Crawford K (2012) Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* 15(5): 662–679.

Cannataci JA and Mifsud-Bonnici JP (2005) Data protection comes of age: The data protection clauses in the European Constitutional Treaty. *Information & Communications Technology Law* 14(1): 5–15.

Carlson RJ (2016) Nietzsche's Snowden: Tightrope walking the posthuman dispositif. In: *Critical Posthumanism and Planetary Futures*. New Delhi, India: Springer, pp. 49–74.

Carter J (2016) Why couldn't tech predict the US election results? Available at: http://www.techradar.com/news/why-couldnt-tech-predict-the-us-election-results (accessed 12 November 2016).

Clarke R (1988) Information technology and dataveillance. *Communications of the ACM* 31(5): 498–512.

de Andrade N (2012) Oblivion: The right to be different . . . from oneself. Reproposing the right to be forgotten. *Revista de los Estudios de Derecho y Ciencia Política de la UOC* 13: 122–137.

de Goede M (2014) The politics of privacy in the age of preemptive security. *International Political Sociology* 8(1): 100–104.

De Hert & Gutwirth (2006) Privacy, data protection and law enforcement. In: Claes E, Duff A and Gutwirth S (eds) *Privacy and the Criminal Law*. Oxford, UK: Hart, pp. 61–104.

De Hert P and Gutwirth S (2009) Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. In: *Reinventing Data Protection?* The Netherlands: Springer, pp. 3–44.

Determann L (2016) Adequacy of data protection in the USA: Myths and facts. *International Data Privacy Law* 6(3): 244–250.

European Commission (2012) 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 on the free movement of such data (General Data Protection Regulation). Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011 (accessed 9 November 2016).

European Commission (2016) Commission decisions on the adequacy of the protection of personal data in third countries. Available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (accessed 9 November 2016).

Foucault M (1977) *Discipline and Punish: The Birth of the Prison*. New York, NY: Vintage.

Graham S and Marvin S (2001) *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*. London, UK: Routledge.

Glaser A (2016) Trump will be a disaster for online privacy. Here's how to protect yours before it's too late. Available at: http://www.recode.net/2016/11/10/13579280/trump-president-online-privacy-protect-surveillance-encryption-election (accessed 12 November 2016).

Habermas J (2010) Das Konzept der Menschenwürde und die realistische Utopie der Menschenrechte. *Deutsche Zeitschrift für Philosophie Zweimonatsschrift der internationalen philosophischen Forschung* 58(3): 343–357.

Hart HLA (1955) Are there any natural rights? *The Philosophical Review* 64(2): 175–191.

Hildebrandt M (2006) Privacy and Identity. In: Claes E, Duff A and Gutwirth S (eds) *Privacy and the Criminal Law*. Oxford, UK: Hart, pp. 43–60.

Hufbauer GC and Jung E (2016) The US-EU Privacy Shield Pact: A work in progress. *Privacy Briefing 16-12*. Available at: https://piie.com/system/files/documents/pb16-12.pdf.

Intelligence and Security Committee of Parliament (2015) *Privacy and Security: A Modern and Transparent Legal Framework*. Available at: http://isc.independent.gov.uk/committee-reports/special-reports (accessed 9 November 2016).

Kitchin R (2013) Big data and human geography: Opportunities, challenges and risks. *Dialogues in Human Geography* 3(3): 262–267.

Lazer D, Kennedy R, King G, et al. (2014) The parable of Google flu: Traps in big data analysis. *Science* 343(6176): 1203–1205.

Lynskey O (2014) Deconstructing data protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly* 63(3): 569–597.

Lyon D (2002) Everyday surveillance: Personal data and social classifications. *Information, Communication & Society* 5(2): 242–257.

Lyon D (2014) Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society* 1(2): 1–13. DOI: 10.1177/2053951714541861.

Mann S (2016) Surveillance (oversight), Sousveillance (undersight), and Metaveillance (seeing sight itself). *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*. Available at: http://www.cv-foundation.org//openaccess/content_cvpr_2016_workshops/w29/papers/Mann_Surveillance_Oversight_Sousveillance_CVPR_2016_paper.pdf (accessed 9 November 2016).

Matzner T, Masur PK, Ochs C, et al. (2016) Do-it-yourself data protection – Empowerment or burden? In: *Data Protection on the Move*. Dordrecht, Netherlands: Springer, pp. 277–305.

McStay A (2013) I consent: An analysis of the cookie directive and its implications for UK behavioural advertising. *New Media & Society* 15(4): 596–611.

Palombella G (2007) From Human Rights to Fundamental Rights Consequences of a conceptual distinction. *Archiv fuer Rechts-und Sozialphilosphie* 93(3): 396–426.

Quelle C (2011) Not just user control in the General Data Protection Regulation. On controller responsibility and how to evaluate its suitability to achieve fundamental rights protection. Available at: http://www.ifip-summerschool.org/wp-content/uploads/2016/08/IFIP-SC-2016_pre_paper_25.pdf (accessed 9 November 2016).

Raley R (2013) Dataveillance and counterveillance. In: *Raw Data is an Oxymoron*. Cambridge, MA: MIT Press, pp. 121–146.

Raz J (1984) Legal rights. *Oxford Journal of Legal Studies* 4(1): 1–21.

Richards NM and King JH (2013) Three paradoxes of big data. *Stanford Law Review Online* 66: 41–46.

Rouvroy A and Poullet Y (2009) The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In: *Reinventing Data Protection?* Dordrecht, Netherlands: Springer, pp. 45–76.

Schwartz PM (2004) Property, privacy, and personal data. *Harvard Law Review* 117: 2056–2128.

Swan M (2013) The quantified self: Fundamental disruption in big data science and biological discovery. *Big Data* 1(2): 85–99.

Trechsel S (2005) *Human Rights in Criminal Proceedings*. Oxford, UK: Oxford University Press.

Van der Sloot B (2014) Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law* 4(4): 307–325.

Waldron J (1993) A right-based critique of constitutional rights. *Oxford Journal of Legal Studies* 13(1): 18–51.

Ward JS and Barker A (2013) Undefined by data: A survey of big data definitions. *arXiv preprint arXiv:1309.5821*.

Yuhas A (2016) Congress will abandon Trans-Pacific Partnership deal, White House concedes. Available at: https://www.theguardian.com/business/2016/nov/12/tpp-trade-deal-congress-obama (accessed 13 November 2016).

This commentary is a part of special theme on Veillance and Transparency. To see a full list of all articles in this special theme, please click here: http://bds.sagepub.com/content/veillance-and-transparency.