# Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order

## Article (Accepted version) (Refereed)

# DECONSTRUCTING DATA PROTECTION:

# THE 'ADDED-VALUE' OF A RIGHT TO DATA PROTECTION IN THE EU LEGAL ORDER

ORLA LYNSKEY

**ABSTRACT**

Article 8 of the EU Charter of Fundamental Rights sets out a right to data protection which sits alongside, and in addition to, the established right to privacy in the Charter. The Charter's inclusion of an independent right to data protection differentiates it from other key human rights documents which generally treat data protection as a subset of the right to privacy. Its introduction, and relationship with the established right to privacy, therefore merit an explanation.

This paper explores the relationship between the rights to data protection and privacy. It demonstrates that, to date, the Court of Justice of the European Union (CJEU) has consistently conflated the two rights. However, based on a comparison between the scope of the two rights as well as the protection they offer to individuals whose personal data are processed, it claims that the two rights are distinct. It argues that the right to data protection provides individuals with more rights over more types of data than the right to privacy. It suggests that the enhanced control over personal data provided by the right to data protection serves two purposes: first, it fosters the development of individual personality and, second, it reduces the power and information asymmetries between individuals and those who process their data. For these reasons, this paper suggests that there may be merit in explicitly recognising these additional dimensions of the right to data protection.

**KEYWORDS**

Data protection, privacy, EU Charter of Fundamental Rights, Court of Justice of the EU, informational self-determination, information and power asymmetries

## I. INTRODUCTION:

Article 8 of the EU Charter of Fundamental Rights[1] (EU Charter) sets out a right to data protection which sits alongside, and in addition to, the right to privacy set out in Article 7 of the Charter. This inclusion of a right to data protection in the EU Charter differentiates it from other key human rights documents[2], which tend to treat data protection as a subset of the right to privacy.[3] When the Charter was signed and proclaimed as a solemn political declaration in 2000, the Court of Justice of the EU (CJEU) had yet to recognise the existence of a right to data protection in the EU legal order.[4] Moreover, the European Data Protection Directive[5], enacted in 1995, makes no reference to the right to data protection. Its inclusion in the Charter therefore merits justification. Unfortunately, the Charter's explanatory memorandum[6] is of little actual explanatory value in this regard. It laconically states that the right to data protection is based on Article 286 EC[7], the Data Protection Directive[8], Article 8 ECHR[9] and the Council of Europe's Convention No 108.[10] It therefore does little to elucidate why such a new right was introduced, in addition to the pre-existing right to privacy, and how these two rights should interact.

---

* Assistant Professor of Law, LSE Law Department. My thanks to Dr Albertina Albors-Llorens, Dr Christopher Kuner, Mr Angus Johnston and Professor Andrew Murray who have contributed to the development of the thoughts expressed in this paper. All opinions expressed and errors remain my own.

[1] European Union, Charter of Fundamental Rights of the European Union [2000] OJ C364/01 and [2010] OJ C83/389.

[2] However, such an independent right exists at national level in many EU Member States. See further, JA Cannataci and JP Mifsud-Bonnici, 'Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty' (2005) 14 Information and Communications Technology Law 5, 8.

[3] For instance, data protection is treated as a subset of the right to privacy by national Constitutions in the Netherlands, Spain and Finland. Section 10 of the Finnish Constitution, entitled 'The right to privacy' states 'Everyone's private life, honour, and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act.'

[4] This right was recognised for the first time by the Court in *Promusicae* in 2008. Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España* [2008] ECR I-271, para 63.

[5] European Parliament and Council Directive 95/46/EC 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 [1995] OJ L281/23 (Directive 95/46 EC).

[6] Explanatory Memorandum, Convention document CHARTE 4473/00, 11 October 2000 <www.europarl.europa.eu/charter/pdf/04473_en.pdf>.

[7] Art 286 EC stated that 'Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty'.

[8] Directive 95/46 EC (n 5).

[9] This provision sets out the right to respect for private life and will be the subject of detailed consideration in section three.

[10] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108, 28.I.1981 <www.conventions.coe.int/Treaty/EN/Treaties/Html/108.htm>.

The failure to provide a convincing rationale for the inclusion of a right to data protection in the EU Charter prompted scholars to advance potential justifications. It has been suggested, for instance, that the Charter's right to data protection was introduced in order to bolster the legitimacy of EU data protection law by emphasising the fundamental rights dimension of the Data Protection Directive.[11] Indeed, although the Directive's stated objectives are to ensure the free flow of personal data in the EU internal market and to protect fundamental rights, the Directive was legally justified on the basis of internal market considerations alone as the EU lacks competence to enact fundamental rights legislation.[12] This potential justification is therefore plausible. Nevertheless, it seems unsatisfactory to accept that a new right has been recognised in the EU legal order to provide ex-post legitimacy to existing legislation. Moreover, if data protection is a subset of the right to privacy, why would the right to privacy, long recognised by the CJEU as a general principle of EU law[13] and set out in the EU Charter, not be sufficient to legitimise the fundamental rights dimension of the EU's data protection framework?

Other scholars suggest that the right to data protection was included in the Charter in order to extend the application of the data protection rules to personal data processing in areas which are explicitly excluded from the material scope of the Data Protection Directive (namely, personal data processing for Common Foreign and Security Policy purposes and for the purposes of Police and Judicial Cooperation in Criminal matters).[14] This view has received some implicit support from the Article 29 Working Party (A29WP), an advisory group on data protection matters composed of representatives of national data protection authorities.[15] Indeed, prior to the adoption of the Charter, the EU's Expert Group on Fundamental Rights highlighted data

[11] P De Hert and S Gutwirth, 'Data Protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in Action' in S Gutwirth, Y Poullet, P De Hert, S Nouwt and C De Terwangne (eds), *Reinventing Data Protection*? (Springer, 2009), 5.

[12] The legal basis of the Directive (ex art 95 EEC, now art 114 TFEU) allows for the enactment of legislation which will approximate the laws of the Member States to improve the functioning of the internal market.

[13] See, Case C- 137/79 *National Panasonic v Commission* [1980] ECR I-2033, paras 18-20.

[14] 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 et al (n 11). See also Cannataci and Mifsud-Bonnici, who recognise that arguably 'having data protection formally firmly entrenched at a constitutional level will put a stop to current "anti-data protection principles" positions taken by the Member States both at an EU level in the areas covered in the second and third pillars and at national levels' (n 2) 5-6.

[15] Article 29 Working Party (A29WP), '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', adopted on 1 December 2009 (WP168), 7.

protection as an area in which the EU's commitment to fundamental rights differed across the three pillars of EU activity.[16] However, a number of arguments militate against this rationale for the new right to data protection. First, at present there is less scope for such differentiation than was previously the case. Not only did the Lisbon Treaty (which gave the Charter its binding force) put an end to the former pillar structure, it also provides a legal basis for data protection legislation covering all aspects of Union law.[17] Secondly, and perhaps more significantly, the recognition of a right to data protection in the EU legal order has not in fact had the effect of putting an end to such differentiation. The European Commission's proposed reform package for data protection makes this abundantly clear: the Commission's Proposed Regulation[18] sets out the general rules applicable to personal data processing, while the Proposed Directive[19] sets out specific rules applicable to personal data processing for the purposes of law enforcement. Consequently, even if the right to data protection was introduced with the objective of ensuring that uniform data protection rules apply in all areas of EU law, it has not achieved this objective. What is apparent from this scholarly speculation is that the EU has neither adequately justified the introduction of the right to data protection in the EU legal order nor explained its content.

The objective of this paper is to examine whether there is, or could be, a credible rationale for introducing an independent right to data protection to the EU legal order. In particular, this paper seeks to ascertain whether data protection is merely a subset of the right to privacy or whether it should be treated as a self-standing right. At present, conceptions of the role data protection norms should play in society differ greatly between EU Member States. In the UK and Ireland, data protection is treated as a subset of the right to privacy with Courts refusing to apply data protection legislation in situations where the right to privacy is not

[16] See Report of the Expert Group on Fundamental Rights, 'Affirming Fundamental Rights in the EU: Time to Act', Brussels, February 1999, 8. <http://ftp.infoeuropa.eurocid.pt/database/000038001-000039000/000038827.pdf>.

[17] Art 16(2) TFEU provides that the EU legislature shall 'lay down the rules relating to the protection of individuals with regard to the processing of personal data by…the Member States when carrying out activities which fall within the scope of *Union* law' (emphasis added). Some differentiation nevertheless remains: see, for example, art 39 EU.

[18] European Commission, 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) COM (2012) 11 final.

[19] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM (2012) 10 final.

engaged.[20] However, there has been a recent notable exception as a judgment of the UK High Court highlighted the distinction between the two rights in order to limit the justiciability of the Charter right to data protection.[21] In contrast, several continental European jurisdictions refuse to systematically link the application of data protection rules to the right to privacy. For instance, in Germany, the Constitutional Court has held that data protection rights flow from the individual's right to 'informational self-determination'[22], a right which the Court had previously derived from the rights to human dignity[23] and free development of personality[24] in the German Basic Law.

This paper does not purport to take a comparative law approach to data protection. Rather, these differing conceptions of the roots and purposes of data protection are highlighted because of their practical consequences for the application of EU data protection law by Member States. The Commission's Proposed Regulation, the centrepiece of the EU data protection reform proposals, seeks to achieve further procedural and substantive harmonisation of national laws. This begs the question, is such substantive harmonisation possible when the central objectives of the right to data protection, which is given expression by EU data protection legislation, are disputed? For instance, would a court in the UK and a court in Germany reach the same conclusion when adopting a purposive approach to the interpretation the Proposed Data Protection Regulation? It seems unlikely. Perhaps more fundamentally however, this lack of clarity regarding the objectives of the right to data protection also detracts from the legitimacy of the EU data protection regime. How can the EU justify the de facto extraterritorial application of its regime or encourage the global application of its data protection standards when it cannot, or does not, articulate the precise purposes of such a regime? The question addressed in this paper

[20] For instance, in *Durant*, the Court of Appeal interpreted the notoriously broad concept of 'personal data' narrowly by finding that whether data constitutes personal data depends inter alia on whether the data is biographical in a significant sense or relates to 'a life event in respect of which his privacy could not be said to be compromised' and whether it is 'information that affects his privacy, whether in his personal or family life, business or professional capacity' (*Durant v Financial Services Authority* [2003] EWCA Civ 1746, Auld LJ at para 28).

[21] In *R (on the application of AB) v Secretary of State for the Home Department* [2013] EWHC 3453 Mostyn J was asked to consider a claim based, inter alia, on the claimant's right to data protection. He stated that the right to protection of personal data is not part of the ECHR and has therefore not been incorporated into domestic law by the Human Rights Act (para 16). He argued that Parliament had deliberately excluded aspects of the ECHR from the Human Rights Act and that the Charter contained 'all of those missing parts and more' (para 14), including the right to data protection.

[22] 'Population Census Decision', Judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65, 1.

[23] Art 1(1) German Basic Law (Deutscher Bundestag, Basic Law for the Federal Republic of Germany, <www.btg-bestellservice.de/pdf/80201000.pdf>).

[24] Ibid, art 2(1).

is therefore one which is integral to the coherence, proportionality and legitimacy of EU data protection law.

In order to expound a potential rationale for the right to data protection, this paper is structured as follows. In section two, the jurisprudence of the CJEU is analysed to see whether it sheds light on the meaning of an independent right to data protection or on the relationship between the rights to data protection and privacy. The analysis of this jurisprudence reveals that the CJEU consistently conflates the two rights which would indicate that the right to data protection is no more than a facet of the right to privacy. This finding is tested in section three by comparing the protection offered by the right to data protection, as given expression in EU data protection legislation, to that offered by the right to privacy, as interpreted by the European Court of Human Rights (ECtHR). A systematic analysis of the protection offered by the two rights reveals that although heavily overlapping, the rights to data protection and privacy are distinct. It is argued that data protection offers individuals more rights over more types of information than the right to privacy when applied in the context of personal data processing. Consequently, the 'added value' of data protection is that it offers individuals enhanced control over their personal data. Section four suggests that this enhanced control serves two primary functions: first, it strengthens the hand of the individual when faced with power and information asymmetries and, second, it proactively promotes the individuals' personality rights which are threatened by personal data processing. This paper therefore concludes that the content of the right to data protection overlaps with that of the right to privacy yet that data protection merits recognition as an independent right for these reasons.

## II. THE RIGHT TO DATA PROTECTION BEFORE THE CJEU

The explanation proffered by the EU for the inclusion of a right to data protection in the EU Charter is both vague and circular, as mentioned in section one. The jurisprudence of the CJEU, which will be examined in this section, constitutes one logical starting point for insights into the purpose of this right in the EU legal order and its relationship with the established right to privacy. This examination takes place in two stages. The EU Charter became binding on EU

Member States with the entry into force of the Treaty of Lisbon in December 2009.[25] The Court's case law from before this point shall firstly be examined before considering the case law following the Charter's acquisition of binding force.

The reason for this bifurcated examination of the case law is that it might be expected that the CJEU would be less forthright in its support of a self-standing right to data protection prior to the entry into force of the Treaty of Lisbon. This is because, unlike the right to privacy, the right to data protection is not a general principle of EU law recognised on the basis of the common constitutional traditions of Member States, nor is it a right which is explicitly mentioned in the ECHR. From the Court's perspective it would therefore appear more prudent to emphasize data protection's link to the established right to privacy in those early years rather than carving out an independent existence for this right. However, the introduction of an explicit legal basis for data protection in the Treaty of Lisbon, which coincided with the Charter acquiring binding force, arguably paved the way for the CJEU to clearly demarcate the distinctions, if any, between these two rights. As this section will demonstrate, the CJEU has not seized this opportunity to distinguish between the two rights. With one notable exception, the Court's jurisprudence has been characterised by its consistent conflation of the rights to data protection and privacy during the period prior to and after the entry into force of the Lisbon Treaty.

### *A. The Right to Data Protection in a Pre-Charter Era*

In *Rundfunk*[26], one of the earliest cases regarding the Data Protection Directive to appear before the Court of Justice, a national jurisdiction asked the Court to assess the compatibility of a

[25] The situation of the UK and Poland (and subsequently the Czech Republic) remains slightly differentiated to that of other Member States. These three Member States signed Protocol 30 to the Lisbon Treaty, which clarifies the effect of the Charter in domestic legal systems. Nevertheless, the precise effect of the Charter in domestic systems remains contested. The ECJ has held that the Protocol does not have the effect of exempting these countries 'from the obligation to comply with the provisions of the Charter or to prevent a court of one of those Member States from ensuring compliance with those provisions' (see Joined Cases C--411/10 *N.S. v Secretary of State for the Home Department* and C-493/10 *M.E. and Others v Refugee Applications Commissioner, Minister for Justice, Equality and Law Reform* [2011] ECR I-0000, 119). However, Mostyn J in the UK High Court in *R(AB)* (n 21) expressed his surprise at the claimant's reliance on EU Charter rights as he was 'sure that the British government … had secured at the negotiations of the Lisbon Treaty an opt-out from the incorporation of the Charter into EU law' (para 10).

[26] Case C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989.

national auditing requirement with the Directive. Austrian legislation stipulated that the salaries of senior public officials must be communicated to the national audit body, transmitted to the Parliament and later made publicly available. In reaching its conclusion, the Court emphasized that the provisions of the Directive must be interpreted in light of fundamental rights, in particular privacy. Therefore, 'for the purposes of applying the Directive', the Court systematically examined whether there had been an interference with the right to privacy contrary to Article 8 ECHR and, if so, whether it was justified. In so doing, the Court entirely overlooked the specific rules set out in the Data Protection Directive. In other words, the Court simply substituted privacy rules for data protection rules. As the interpretation of Article 8 ECHR alone was decisive in resolving the dispute, this led to concern regarding the future role and relevance of data protection rules.[27] Moreover, as *Rundfunk* treated data protection and privacy as interchangeable, it lent credence to the assertion that data protection is a subset of the right to privacy. Nevertheless, a strong argument could be made to limit the *Rundfunk* reasoning to its facts as the Court would have reached an identical outcome had it relied on the Directive rather than the right to privacy. Therefore, while the Court should have exercised more caution in substituting the application of secondary legislation with the application of a general principle of EU law, it could not be stated with certainty post-*Rundfunk* that data protection and privacy were substitutable rights in all circumstances.

In *Promusicae*[28] the Court considered whether EU law requires Member States to adopt national legislation placing an obligation on internet service providers (ISPs) to supply the personal data of alleged copyright infringers to copyright holders in order to facilitate civil proceedings. In particular, the Spanish referring court asked the Court of Justice whether a positive obligation to supply such personal data to copyright holders flowed from three EU Intellectual Property (IP) Directives.[29] The Court of Justice reformulated the questions asked by

[27] CD Classen, 'Case C-139/01 Österreichischer Rundfunk and Others: case-note' (2004) 41 CMLRev 1377, 1383.

[28] Case C-275/06 *Promusicae* (n 4).

[29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1 and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10.

the national court by firstly considering whether European Data Protection law, in particular the Data Protection Directive and the E-Privacy Directive[30], *precludes* a Member State from laying down such an obligation. It then addressed the question asked by the Spanish Court; whether the three IP Directives require a Member State to adopt legislation setting out such an obligation. Finally, the Court considered what impact the EU Charter, which was not yet binding on Member States, should have on the conclusions it had reached to the first two questions. It noted that the factual situation involved, on the one hand, the rights to property and to effective judicial protection, and, on the other hand, 'a further fundamental right, namely the right that guarantees protection of personal data and hence of private life'.[31] While the *Promusicae* judgment offered some initial promise as the Court raised data protection concerns of its own volition, this promise was short-lived given the Court's reference to the distinct rights to data protection and privacy as one right. Although the Court noted that the E-Privacy Directive 'seeks to ensure full respect for the rights set out in Articles 7 and 8 of the Charter'[32] it went on to state in the following paragraph that '[t]he present reference for a preliminary ruling thus raises the question of the need to reconcile the requirements of the protection of different fundamental rights, namely the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other'.[33] Therefore, to the Court data protection is synonymous with privacy.

In the later case of *Satamedia*[34], where the Court was asked to reconcile data protection legislation and the right to freedom of expression, the Court seemingly returned to its pre-*Promusicae* position. No reference was made to the right to data protection and the Directive was treated as a privacy protection tool. For instance, the Court noted that Article 9 of the Directive seeks to reconcile two fundamental rights: 'the protection of privacy and freedom of expression'.[35] Therefore, during the period prior to the entry into force of the Lisbon Treary, the

[30] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37. The second recital of the E-Privacy Directive states that it 'In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter'.

[31] Para 63.

[32] Para 64.

[33] Para 65.

[34] Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi OY, Satamedia* [2008] ECR I-09831.

[35] Ibid, para 54

right to data protection is considered by the Court of Justice as a subset of the right to privacy which does not merit independent consideration.

One judgment of the General Court, the lower instance of the CJEU, sits uneasily with this line of jurisprudence which treats data protection as a subset of the established right to privacy. In *Bavarian Lager*[36] the General Court was asked to reconcile the right to data protection with the right of access to documents (also enshrined in the EU Charter). The Bavarian Lager company made a request to the European Commission under EU access to documents legislation (Regulation 1049/2001[37]) for minutes to a particular meeting and the names of the meeting attendees. The Commission would only provide the data in anonymised form on the basis that the information requested contained personal data and the disclosure of the data would not be in compliance with the data protection rules applicable to the EU Institutions (Regulation 45/2001[38]). The General Court was asked to determine whether this Commission Decision to refuse the relevant data struck the correct balance between the freedom of information and data protection in the EU legal order.

Article 4(1)(b) of the access to documents regulation determines the relationship between these two rights. It provides that a request for access to a document shall be refused where the document's disclosure would undermine the protection of 'privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data'. Article 4(1)(b) therefore arguably contains two limbs: access to a document should be refused when 'disclosure would undermine the privacy and integrity of the individual' (first limb), 'in particular in accordance with Community legislation regarding the protection of personal data' (second limb). The dispute in *Bavarian Lager* centred upon the interaction between these two limbs. Indeed, Article 4(1)(b) could be read in a number of ways. On the one hand, it could be assumed that the second limb is merely expanding on the first and that the data protection rules should be applied to determine whether disclosure would undermine privacy.

[36] T-194/04 *Bavarian Lager v Commission* [2007] ECR II-3201.

[37] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents [OJ] L 145/43.

[38] Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1.

However, an alternative reading of these two limbs is possible, according to which it is only when the first limb is satisfied (i.e. privacy is undermined) that it is necessary, pursuant to the second limb, to apply the data protection rules. This is the interpretation preferred by the European Data Protection Supervisor (EDPS), who intervened before the Court in *Bavarian Lager*.[39] The General Court also seemingly preferred this interpretation as, when applying Article 4(1)(b), it began by examining whether the disclosure of the names of those attending the meeting would breach their Article 8 ECHR right to privacy. It concluded that the disclosure would not result in a violation of the right to privacy and therefore that the Article 4(1)(b) exception was not applicable.[40] As a result, the General Court held that the application to the request of the 'additional conditions' set out in the European data protection legislation, such as the need for consent of the data subject would be contrary to Regulation 1049/2001.[41] As a result, the General Court annulled the Commission decision.

The reasoning of the General Court in this case appears clear; in the absence of a violation of the right to privacy as a result of the disclosure of a document, the data protection rules do not apply. While at first glance this could be confused for another example of the conflation of the rights to data protection and privacy, it is in fact the opposite. The Court interpreted the wording of Article 4(1)(b) of Regulation 1049/2001 to mean that in cases of conflict between data protection and freedom of information, the data protection rules prevail only when privacy is undermined. When privacy is not undermined, the freedom of information rules prevail over the data protection rules. Therefore, the interpretation of Article 4(1)(b) advanced by the General Court and the EDPS acknowledges that not all data processing adversely affects the right to privacy and, consequently, that data protection applies to a wider variety of personal data than privacy law. In other words, the material scope of application of the two rights is distinct. Indeed, this was explicitly stated by both actors. In its pleading before the Court the EDPS stressed that the interest protected by Article 4(1)(b) is private life, and not the

[39] EDPS pleading in T-194/04 *Bavarian Lager v Commission*, section 8. Moreover, the EDPS argued that had the legislator intended to give art 4(1)(b) the meaning supported by the Commission's 'renvoi-theory' (according to which there is a direct referral to the data protection rules whenever a requested document contains personal data), 'the wording of the exception could and should have been far more explicit'.

[40] T-194/04 *Bavarian Lager* (n 36) paras 132-133.

[41] Ibid, para 137.

much broader concept of personal data[42] while in its judgment the General Court asserted that privacy and data protection are not synonymous.[43] While De Hert and Gutwirth suggest that the ease with which the General Court distinguished between two types of personal data – those that are protected by the right to privacy and those that are not – 'does not sit comfortably with the formal constitutional codification of data protection within EU law'[44], it is argued here that the opposite is in fact true. By recognising that data protection rules could apply even in the absence of an infringement of privacy, the General Court and the EDPS were liberating the data protection rules from the right to privacy and paving the way for the emergence of a truly independent right to data protection in the EU legal order. However, as will be demonstrated presently, the Court of Justice has steadfastly overlooked this distinction in its jurisprudence, even following the entry into force of the Treaty of Lisbon.

### *B. The Post-Lisbon Jurisprudence of the CJEU*

The binding force acquired by the EU Charter as well as the introduction of an explicit legal basis for data protection legislation in the Lisbon Treaty provided the CJEU with the necessary legal tools to elaborate on the content and meaning of an independent right to data protection. However, as this section will demonstrate, the Court has not taken this opportunity to expound a new vision for the right to data protection.

In her Opinion in *Volker*, delivered soon after the entry into force of the Lisbon Treaty, Advocate General Sharpston clearly distinguished between the rights to data protection and privacy stating that '[t]wo separate rights are here invoked: a classic right (the protection of privacy under Article 8 ECHR) and a more modern right (the data protection provisions of

[42] It, therefore, argued that, whilst a reference to the name of a participant in the minutes of a meeting constitutes personal data, the disclosure of a name in the context of professional activities does not normally have a link to private life. Ibid, para 67.

[43] It stated that 'not all personal data are by their nature capable of undermining the private life of the person concerned. In recital 33 of the General Directive, reference is made to data which are capable by their nature of infringing fundamental freedoms or privacy and which should not be processed unless the data subject gives his explicit consent, which implies that not all data are of that nature'. Ibid, para 119.

[44] P De Hert and S Gutwirth, 'Data Protection in the in the case law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth, Poullet, De Hert, Nouwt & De Terwangne (eds), *Reinventing Data Protection*? (Springer, 2009), 41.

Convention No 108)'.[45] While, unfortunately, the Advocate General did not elaborate on the meaning of this distinction or the content of this 'more modern right', her statement, coupled with the General Court's judgment in *Bavarian Lager*, should have provided the Court of Justice with food for thought on the differences between the two rights.

However, when the General Court's *Bavarian Lager* judgment was appealed to the Court of Justice[46], the Court of Justice held that the lower jurisdiction had erred in law. It found that by limiting the application of the Article 4(1)(b) exception to situations in which the privacy or integrity of the individual would be infringed under Article 8 ECHR, the General Court had disregarded the wording of Article 4(1)(b), which requires that this assessment should be made in conformity with the Union's data protection legislation.[47] Personal data processing cases could not, according to the Court, be separated into two categories: those examined in light of the ECHR right to privacy and those examined for compliance with European data protection legislation.[48] Therefore, the Court of Justice concluded that in all situations where access is sought to a document containing personal data EU data protection rules become applicable in their entirety.[49] The practical consequence of this finding is that EU data protection rules must systematically prevail over the EU rules on freedom of information.

The Court's judgment is noteworthy not only because it allows one fundamental right in the EU Charter to consistently trump another in this manner, but also because of what it reveals regarding the Court's view of the relationship between the rights to data protection and privacy. It follows implicitly from the judgment that even when there is no infringement of the individual's right to privacy (as was arguably the case in *Bavarian Lager*), the data protection rules trump the freedom of information rules. This begs the question, if the interest being protected by the Court in this instance is not privacy, what is the Court protecting? While the Court did not consider the matter explicitly, the Court may have assumed that a failure to comply with data protection legislation always undermines the right to privacy. In other words, despite

[45] C-92/09 and C-93/09 Volker und Markus Schecke and Hartmut Eifert [2010] ECR I-11063, Opinion of Advocate General Sharpston, para 71.
[46] C-28/08 *European Commission v Bavarian Lager* [2010] ECR I-6055.
[47] Ibid, paras 58-59.
[48] Ibid, 58-61.
[49] Ibid, 63.

the assertions of the EDPS and the findings of the General Court to the contrary[50], the Court treats data protection as a subset of the right to privacy. It is unclear whether this represents a conscious choice on the part of the Court or simply highlights that the Court has not given the distinction between the two rights adequate (or perhaps any) consideration. The subsequent *Volker* judgment seems to point to the latter conclusion. In *Volker* the Court firstly states that the two rights are 'closely connected'[51] before soon thereafter treating them as a hybrid species when it refers to 'the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter.'[52]

One explanation for the conflation of the two rights by the Court of Justice is that the Court has erroneously interpreted the ECtHR's Article 8 ECHR jurisprudence and applied this interpretation directly to the EU Charter articles. Indeed, in the *Volker* judgment the Court of Justice states that the Article 7 and 8 rights concern 'any information relating to an identified or identifiable individual'. It cites the ECtHR judgments in *Amann v Switzerland*[53] and *Rotaru v Romania*[54] as authority for this assertion.[55] However, the cited case law does not in fact support the proposition that Article 8 ECHR applies to 'any information relating to an identified or identifiable person'. Rather, this is how the Data Protection Directive defines 'personal data'.[56] Indeed, as will be seen in the follow section, despite the ECtHR's expansive interpretation of the right to privacy, it is frequently advocated that the right to privacy does not apply to the same wide range of data to which data protection rules apply.[57]

More recently in his Opinion in *Google Spain*[58], Advocate General Jääskinen argued that the scope of application of the EU data protection rules has become 'surprisingly wide' and highlighted that 'the wide interpretation given by the Court to the fundamental right to private

[50] Ibid, fn 41.
[51] C-92/09 and C-93/09 *Volker und Markus Schecke and Hartmut Eifert* [2010] ECR I-11063, para 47.
[52] Ibid, para 52.
[53] *Amann v Switzerland* (2000) 30 EHRR 843.
[54] *Rotaru v Romania* (App No 28341/95) (unreported) 4 May 2000.
[55] *Volker* (n 51) para 52.
[56] Directive 95/46 EC (n 5) art 2(a).
[57] See, for instance, Opinion of the A29WP, 'Opinion 4/2007 on the concept of personal data', 20 June 2007, 01248/07/EN WP 136, or H Kranenborg, 'Access to documents and data protection in the European Union: on the public nature of personal data' (2008) 45(4) CMLRev 1079, 1091.
[58] Opinion of Advocate General Jääskinen in Case C-131/12, *Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2013] ECR I-0000.

life in a data protection context seems to expose any human communication by electronic means to the scrutiny by reference to this right'.[59] As a result, the Advocate General called for what he termed a 'rule of reason' approach to the application of the data protection rules.[60] However, it is suggested that the conflation of the rights to privacy and data protection caused confusion in the Advocate General's Opinion. It is not 'the fundamental right to private life in a data protection context' which is given a wide interpretation. Rather, it is argued here that it is the fundamental right to data protection which is in fact more widely interpreted – and broader in scope – than the right to privacy. The Advocate General overlooks the fact that data protection rules were purposely designed to be broader in scope than the right to privacy by the EU legislature and seems to suggest that technological development is responsible for their wide application. As will be demonstrated in the next section this is a false assumption.

A clear picture emerges from the few data protection cases which have appeared before the CJEU both prior to and following the entry into force of the Treaty of Lisbon. Contrary to the instinct of the General Court, the Court of Justice deems the newly articulated right to data protection to be nothing more than a subset of the right to privacy thereby putting 'new wine in old bottles'.[61] However, this paper shall argue that, despite the Court of Justice's indications to the contrary, data protection and privacy are distinct rights, albeit heavily overlapping, and that there is adequate justification to treat them as such. However, at present, the conflation of these two rights by the Court of Justice risks subjecting the modern right of data protection to the limitations that have been imposed on the 'classic' right to privacy thereby stunting its development. It also precludes debate, both inside and outside the Court, of what independent objectives data protection pursues and how best to reconcile these objectives with competing rights and interests.

[59] Ibid, para 29.

[60] In fact it is submitted that what the Advocate General was asking for was the application of the principle of proportionality when interpreting the Directive (although, as a general principle of EU law, the principle of proportionality is applied at all times when interpreting EU law). He considered that such an approach was necessary in order to avoid 'unreasonable and excessive legal consequences'. Ibid, para 30.

[61] Similarly, Schwartz and Reidenberg have noted that calling data protection 'information privacy' is an attempt to 'put new wine in old bottles'. Paul M. Schwartz and Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (MICHIE Law Publishers, 1996), 102.

## III. DIFFERENTIATING DATA PROTECTION: LESSONS FROM THE EUROPEAN COURT OF HUMAN RIGHTS

In this section, the key distinctions between the protection offered by the right to data protection, as given expression in EU secondary legislation, and the right to privacy, set out in Article 8 ECHR, will be identified. This can be done by comparing the scope and safeguards offered by EU data protection law to the scope and safeguards offered by the right to privacy. The scope and safeguards of the latter can be deduced from the jurisprudence of the ECtHR.[62] It is argued in this section, that the right to data protection includes a broader range of data and data-related actions within its scope and guarantees more data-processing related rights to the individual than the right to privacy.[63] In other words, data protection offers individuals more control over more types of data than the right to privacy. Data protection should therefore be conceived as a right which heavily overlaps with the right to privacy yet offers additional, distinct benefits for individuals.

### *A. The Broader Range of Data and Data-Related Actions Covered by the Right to Data Protection*

In this part it shall be demonstrated that the scope of application of the data protection rules – determined by what constitutes 'personal data' and 'personal data processing' – is broader than the concept of 'privacy interference' which defines the scope of application of Article 8(1) ECHR.

#### *1. The Broader Range of Data*

[62] This issue has been considered by Brouwer in E Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff Publishers, 2008), 194-204 and more recently by Purtova (Nadezhda Purtova, *Property Rights in Personal Data: a European Perspective* (Kluwer Law International, 2011), 224-240). Due to space constraints, it is not possible to outline the relevant case law in this paper.

[63] In theory, the right to privacy is not applicable to private parties but this right places 'positive obligations' on States. It remains unclear whether the EU Charter can be directly invoked in proceedings between private parties. While the ECJ refused to give such horizontal direct effect to art 27 of the Charter in Case C-176/12 *AMS v Union locale des syndicats CGT and ors* [2014] ECR I-0000, it arguably left the door open to grant other rights such effect where the Charter article is 'sufficient in itself to confer on individuals an individual right which they may invoke as such.' (para 47).

The right to data protection, as given expression by EU data protection legislation, applies to personal data: that is, data relating to an 'identified' or 'identifiable' natural person.[64] The notion of 'personal data' was purposely defined as broadly as possible by the European legislature in order to include all data which might be linked to an individual.[65] Indeed, despite the ECtHR's expansive interpretation of the notion of privacy[66], it is argued that the right to privacy does not apply to the same wide range of data to which the data protection rules apply.[67] Two distinctions regarding the range of data falling within the scope of both rights can be observed: first, unlike the notion of 'privacy interference', the notion of 'personal data' is not context dependent[68] and, second, the notion of personal data includes data relating to unidentified yet identifiable individuals.

The jurisprudence of the ECtHR often conflates its analysis of, first, whether a prima facie privacy interest exists and, secondly, if so, whether there is an interference with this privacy interest. This makes it difficult to directly compare the notions of 'privacy interest' and 'personal data' although these notions determine the scope of the rights to privacy and data protection respectively. The ECtHR's conflated analysis also however demonstrates that the notion of 'privacy interest' is often circumstance-dependent and requires a contextual assessment. For instance, the assessment of whether an individual has a privacy interest in his name is context-dependent. The facts of the *Bavarian Lager* case illustrate this point well as it was questioned whether an individual has a privacy interest in his name when he is appearing before a public authority in a professional capacity. Advocate General Sharpston argued in her Opinion that names fall within the scope of Article 8 ECHR and therefore the disclosure of a name, even in a

[64] Art 2(a) Directive 95/46 EC (n 5); arts 4(1) and (2) Proposed Regulation (n 18).

[65] A29WP, 'Opinion 4/2007 on the concept of personal data', adopted on 20 June 2007 (WP 136).

[66] For instance, in *Amann* the Court noted that the applicant's file stated that he was a 'contact with the Russian embassy" and did "business of various kinds with the company [A.]', *Amann* (n 53) para 66. The Court found that those details undeniably amounted to data relating to the applicant's 'private life', para 67.

[67] As RAND Europe notes 'one of the crucial characteristics of the [Data Protection] Directive is that it is tied to the concept of personal data, and not to a notion of privacy. Indeed, the provisions of the Directive can apply to data processing acts which are not privacy sensitive' RAND Europe, 'Technical Report on the Review of the European Data Protection Directive', 27 <www.ico.govuk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf>. See also: Opinion of the A29WP, 'Opinion 4/2007 on the concept of personal data', 20 June 2007, 01248/07/EN WP 136, or Kranenborg (n 57) 1091.

[68] *Durant* (n 20).

business context, constitutes a potential interference contrary to the ECHR. The EDPS argued to the contrary that no such privacy interest existed in *Bavarian Lager* as 'the disclosure of a name in the context of professional activities does not normally have a link to private life'.[69] Similarly, the General Court inferred that there was not a privacy interest at stake in that case. Although the General Court merged its consideration of whether a privacy interest exists and whether it had been undermined, in so doing it highlighted that even though professional activities are not in principle excluded from the concept of private life under Article 8 ECHR, the mere fact that a document contains personal data does not mean that the privacy or integrity of the persons concerned is affected.[70] This, it is argued, is the preferred finding.[71] However, what is notable for present purposes is that there is a clear lack of consensus regarding whether, and if so in what circumstances, an individual has a privacy interest in his name. In contrast, as the EDPS highlighted, 'a reference to the name of a participant in the minutes of a meeting constitutes personal data'.[72] Thus, it can be seen that while the question of whether a 'privacy interest' exists in particular circumstances requires a context-dependent assessment, whether data constitutes personal data is generally an issues which is easier to assess.

Furthermore, as mentioned above, data protection rules apply to processing of data that relates to an identified or *identifiable* person.[73] In this regard, data protection rules apply where identification is possible, regardless of whether or not identification occurs. However, it appears that under Article 8 ECHR emphasis is placed on whether or not an individual is actually

[69] Case C-28/08 *Bavarian Lager* (n 46) para 167.

[70] Ibid, para 123.

[71] This is for three reasons. First, the jurisprudence of the ECtHR which finds that an individual has a privacy interest in his name concerns laws or administrative practices which prevent the applicant from being called by his correct or desired name and therefore has human dignity implications (see, Opinion of Advocate General Jacobs, delivered on 9 December 1992, in Case C-168/91 *Konstantinidis v Stadt Altensteig* [1993] ECR I-1191, para 40). In contrast, the disclosure of a name featured in a document has no impact on the individual's name or their rights over it and therefore does not have the same human dignity implications. Secondly, the ECtHR's rationale for extending privacy interests to the workplace and business activities of individuals, namely that 'private life' comprises 'the right to establish and develop relationships with other human beings' (*Niemietz v. Germany* 16 December 1992, appl. no. 13710/88, paras 29-30), cannot be applied in Bavarian Lager. On the contrary, one of the aims of the EU's transparency legislation is to enable EU citizen's to verify that EU measures, have been enacted in the absence of, and without any regard for, the personal relationships of those involved in the EU legislative or decision-making process. Finally, the meeting attendees had no reasonable expectation in Bavarian Lager that the public would not be privy to data concerning their involvement, in a professional capacity, in the processes of democratic, accountable Institutions (*PG and JH v United Kingdom* (2008) 46 EHRR 51, para 57).

[72] Case T-194/04 *Bavarian Lager* (n 36) para 67.

[73] Directive 95/46 EC (n 5) art 2(a).

identified when considering whether there is a breach. For instance, in *Friedl*[74] the applicant complained that there was an interference with his right to privacy when the police took a photograph of him participating in a public demonstration. The European Commission of Human Rights (ECommHR) – a predecessor of the ECtHR – struck the case off the list, explicitly attaching weight to the fact that no action was taken to identify the persons photographed by means of data processing.[75] Therefore, it is suggested that the notion of personal data is broader than the interest protected by the right to privacy. Moreover, as will now be demonstrated, the concept of 'personal data processing' which also helps delimit the scope of application of the right to data protection is clearly more expansive than that of 'privacy interference'[76], which determines what falls within the scope of the right to privacy.

### *2. The Broader Range of Data-Related Activities*

For the purposes of EU law, data processing is defined as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means' and could, therefore, encompass any form of data handling.[77] As Kuner highlights 'it is difficult to conceive of any operation performed on personal data in electronic commerce which would not be covered by it'.[78] While the ECtHR is willing to include even publicly available data within the scope of Article 8 ECHR provided it is systematically collected or stored, it is submitted that the notion of 'personal data processing' is nevertheless more inclusive than that of 'privacy interference'. Some examples will help to illustrate this point.

In the case of *Pierre Herbecq and the Association 'Ligue des droits de l'homme' v Belgium*[79], the ECommHR declared that an application made by the applicants was manifestly

[74] *Friedl v Austria* (1996) 21 EHRR 83.

[75] Ibid, para 50.

[76] It is often difficult to distinguish a 'privacy interest' from the 'interference'. The *Rotaru* judgment (n 54) is an excellent example of this point. In *Rotaru* the ECtHR held that publicly available data, which does not always benefit from privacy protection, fell within the material scope of the right to privacy as this data was treated in a particular way – it was systematically collected or stored.

[77] Directive 95/46 EC (n 5) art 2(b).

[78] C Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, OUP, 2007), 74.

[79] *Pierre Herbecq and the Association 'Ligue des droits de l'homme' v Belgium* (App Nos 32200/96 and 32201/96) 14 January 1998.

ill-founded and therefore inadmissible. In their application, the applicants challenged the Belgian government's failure to enact legislation concerning filming for surveillance purposes where the visual data obtained was not recorded. The ECommHR examined, inter alia, whether the visual data related to private matters or public incidents and whether it was likely to be made available to the general public. It held that, since nothing was recorded, it was difficult to see how the footage could be made available to the general public or used for alternative purposes. The ECommHR also noted that all that could be observed is 'essentially public behaviour'. Therefore this recording, which would constitute personal data processing and therefore fall within the scope of the right to data protection, was excluded from the scope of the right to privacy.

In the EU Court of Justice's *Rundfunk*[80] judgment it also implicitly acknowledges this distinction. The Court noted that 'the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life' under Article 8 ECHR.[81] However, such recording would constitute 'data processing' and thus fall within the scope of the right to data protection.

It is possible to think of numerous other day-to-day examples of data processing which falls within the scope of the right to data protection but arguably not privacy. For instance, if a student competes for her university athletics team, the name and age category of the student may be is published on the university webpage. This publication constitutes data processing within the meaning of EU data protection law. However, such an act would not fall within the scope of the right to privacy as the information concerned is publicly available data which is not systematically collected or stored. Moreover, it is arguable that the student should have reasonably expected her personal data to be processed in this way.[82] It can, therefore, be

[80] Case C-139/01 *Rundfunk* (n 26).

[81] Ibid, para 74.

[82] In *PG and JH* (n 71) the ECtHR noted that '[t]here are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises… a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor.' Para 57.

concluded that EU data protection regulation applies when data is manipulated in ways which would not be subject to privacy protection.[83]

### *B. The Limited Range of Information Rights Covered by Article 8 ECHR*

Not only is the scope of the right to data protection different to that of the right to privacy, the substantive protection offered by both rights also differs. Many of the rights provided for in the EU data protection regime have been encompassed in the ECtHR's Article 8 ECHR jurisprudence. When considering whether the collection or storage of data is in accordance with the law and is proportionate under Article 8(2) ECHR, the ECtHR has taken the opportunity to enumerate a number of requirements which must be respected. These requirements effectively mirror the principles relating to data quality set out in both the Data Protection Directive[84] and the Proposed Regulation[85] (for example, that data should be 'preserved in a form which permits identification of the data subject for no longer than is required for those purposes'[86]). Moreover, the jurisprudence of the ECtHR is constantly evolving and, in recent years, its evolution has encompassed rights offered by data protection law. For instance, although the ECtHR initially refused to acknowledge that a data subject had a general right of access to his personal data[87], in later judgments it went a long way towards introducing such a general right of access for individuals.[88]

There is therefore considerable, and growing, overlap in terms of the substantive protection offered to individuals by the EU right to data protection and the ECHR's right to privacy. Nevertheless, some rights granted by the EU data protection regime are not referred to in the Article 8 ECHR jurisprudence, for instance the individual's right not to be the subject of a

[83] See also De Hert and Gutwirth who state that privacy covers 'only flagrant abuse or risky use of data that can easily be used in a discriminatory way' while 'other kinds of data processing are left untouched "as long as there is no blood"' (De Hert and Gutwirth, n 11 23&25); Kranenborg (n 57) 1091.

[84] Directive 95/46 EC (n 5) art 6.

[85] Proposed Regulation (n 18) art 5.

[86] *S and Marper v United Kingdom* (2009) 48 EHRR 50 para 103; Directive 95/46 EC (n 5) art 6(1)(e) and art 5(e) Proposed Regulation (n 18).

[87] In *Gaskin* the ECtHR stated that 'a system…which makes access to records dependent on the consent of the contributor can, in principle, be considered compatible with Article 8 ECHR'. *Gaskin v United Kingdom* Series (1989) 12 EHRR 36, para 49.

[88] For instance, in *KH v Slovakia* the ECtHR held that data subjects should not be obliged to justify a request to be provided with their personal data files; it is for the authorities to provide compelling reasons why these files should not be provided. *KH v Slovakia* (2009) 49 EHRR 34, para 48.

decision which significantly affects him and is based on automatic processing.[89] It is submitted that this type of right is designed to tackle non-privacy related concerns, such as power asymmetry between individuals and those who process their data.[90] This differentiation in terms of substantive protection has been made more conspicuous by the Proposed Regulation. For example, although privacy law might recognise the right of the data subject to ensure the erasure of his personal data in certain instances, it does not recognise anything akin to the 'right to be forgotten' set out in the Proposed Regulation.[91] Moreover, the ECtHR case law does not recognise a right to data portability.[92] Indeed, this confirms that the objective of such a right is not to protect individual privacy; it must therefore serve a different, independent objective.

In conclusion, when determining whether the protection offered by Article 8 ECHR is coextensive to that offered by the right to data protection, it can be seen that the two differ in terms of scope and also the substantive protection they offer. Therefore, it is suggested that the rights to data protection and privacy are significantly overlapping yet distinct. In this regard, the Proposed Regulation is a timely reminder as it clearly illustrates that EU data protection law includes within its scope elements which do not fit easily under a privacy umbrella. These other elements are therefore what distinguish the right to data protection from the right to privacy. In the following section, a justification for the distinction between these two rights will be offered.

## IV. THE VALUE-ADDED OF A RIGHT TO DATA PROTECTION IN THE EU LEGAL ORDER

The rights to data protection and privacy serve many of the same objectives. For instance, both can protect psychological integrity[93] by preventing or mitigating embarrassment or distress caused as a result of the unwanted disclosure of personal facts.[94] Data protection and privacy

[89] Directive 95/46 EC (n 5) art 15; art 20(1) (n 18) Proposed Regulation.

[90] Another example of such a right might be the data subject's right to object to processing when personal data is disclosed to third parties for the first time or used for direct marketing (art. 14(b) Directive 95/46 EC n 5). While this right might attempt to tackle privacy concerns, it is also reflects an effort to empower individuals vis-à-vis data controllers and processors.

[91] Dominic McGoldrick, 'Developments in the Right to be Forgotten' (2013) 13(4) HRLR 761.

[92] Proposed Regulation (n 18) art 18.

[93] *Pretty v UK* (2002) 35 EHRR 1 35, para 61.

[94] *Campbell v MGM Limited* [2004] UKHL 22.

also, for instance, have a role to play in ensuring that State data processing remains within the limits of the law thereby reducing the risk or gravity of abuse of power by the State. Privacy violations, such as unauthorised surveillance, and personal data processing can also have a 'chilling effect' on individuals causing them to feel monitored and consequently modify their behaviour. The rights to data protection and privacy help to deter and regulate such unauthorised surveillance or dataveillance[95] allowing individuals to behave in an uninhibited manner and to exercise the rights guaranteed in democratic societies, such as freedom of expression and association, without fear of repercussion.[96] The fact that data protection and privacy promote many of the same goals is consistent with the finding in section three that the two rights are heavily overlapping. However, it was also established in section three that data protection grants individuals more rights over more personal data than the right to privacy. The aim of this section is to determine why this is so.

### *A. The Functions of an Independent Right to Data Protection*

According to the 1995 Data Protection Directive its aim is to 'protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data' and to ensure that states do not restrict or prohibit data flows for reasons connected with the protection offered to individuals. The Directive does not elaborate on these rather vague objectives. Nor, looking at this issue from an alternative angle, have the harms which EU data protection law seeks to prevent or mitigate been identified by the EU Institutions. This failure to identify the objectives of the law is remiss, particularly at a time when the legislative framework for data protection is in flux and there is increasing support for a 'risk-based' approach to data protection law. This part therefore seeks to identify the functions of an independent right to data protection.

[95] The term 'dataveillance' conveys the message that the systematic use of data systems to monitor the actions or communications of an individual can effectively amount to surveillance. This term was coined by RA Clarke, 'Information Technology and Dataveillance' (1988) 31 Communications of the ACM 498.

[96] The German Constitutional Court emphasized the societal importance of 'informational self-determination' as a precondition for citizens' free participation in the political processes of the democratic constitutional state in its famous 1983 'Population Census Decision' (judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65, 1). The societal costs of surveillance have also been emphasized in the academic literature: N Richards, 'The Dangers of Surveillance' Harvard Law Review (Symposium 2012: Privacy and Technology) 9 November 2012, 18-26 (<http://www.harvardlawreview.org/privacy-symposium.php>) and C Slobogin, 'Public privacy: camera surveillance of public places and the right to anonymity' (2002-2003) 72 Mississippi Law Journal 213.

The data protection rules, which give expression to the right to data protection, are arguably more effective than the right to privacy at minimising the risk for individuals of certain tangible harms caused by data processing.[97] Take the example of discrimination. Data protection reduces the risk of discrimination by decreasing the possibility that proxies or presumptions will be used to make decisions which negatively affect individuals. This is because data protection prohibits decision-makers from taking decisions which are likely to significantly affect the individual based solely on automated data processing.[98] Accordingly, human attention must be given to an individual's personal data before a decision can be made which may significantly affect that individual, arguably therefore making direct and indirect discrimination more difficult. For instance, an employer cannot automatically refuse to consider all applicants aged over 30 from a job selection process (direct discrimination) nor could the employer exclude all candidates whose University qualifications were acquired over ten years ago from the process (indirect discrimination).[99] Equally, it could be argued that the right to data protection is distinct from the right to privacy as it provides tools to minimise the risk of identity theft. As the European Commission has noted, 'the creation of centralised databases of identifying data...represents in principle a single point of vulnerability for large-scale identity theft and it would be reasonable, on these grounds alone, to try to minimise the number of such databases'.[100] While, perhaps paradoxically, data protection rules may on the whole facilitate the creation of such centralised databases, these data protection rules also reinforce the vulnerable architecture of such databases thereby reducing the risk of identity theft. For instance, pursuant to data protection rules there is an obligation on data controllers to 'implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss,

[97] The EU has not yet identified the intangible harm that EU data protection law seeks to prevent. Indeed, this dichotomy between tangible and intangible harm has received little, if any, attention in the EU context to date. Romanosky & Acquisti recognise this distinction in the context of US information privacy law; they state that 'both direct and indirect costs can be tangible and intangible: for example, the tangible monetary loss due to price discrimination and the intangible shame associated with having portions of one's life exposed to the public'. S Romanosky and A Acquisti, 'Privacy Costs and Personal Data Protection: Economic and Legal Perspectives' (2009) 24 Berkley Technology Law Journal 1060, 1094.

[98] Art 15.

[99] Some authors argue that the use of such proxies is an efficient way to make decisions. For instance, Posner argues that it is 'quite impossible to imagine how society would function without heavy reliance on proxies in lieu of full investigation of relevant facts'. R Posner, 'Privacy, Secrecy and Reputation', First Draft, 9 October 1978 (text accessed at Harvard Law Library), 46.

[100] N Mitchison et al, 'Identity Theft: A Discussion Paper' Technical Report EUR 21098, European Commission-Joint Research Centre, 2004, 29.

alteration, unauthorized disclosure or access'.[101] Equally, competent data protection authorities and the data subject must be informed when there is a data breach.[102] However, beyond the prevention or minimisation of such tangible risks, it is submitted that the right to data protection is distinct from, and adds value to, the right to privacy in two key ways.

### *1. Promoting Informational Self-Determination and Individual Personality Rights*

An individual may face multiple obstacles to his or her personal development. As previously mentioned, surveillance conducted via data processing can have a chilling effect on individual behaviour. Crucially, whether or not an individual is actually being monitored is not decisive in these circumstances: the mere perception of surveillance may be sufficient to inhibit individual behaviour. Indeed, this is the premise on which Jeremy Bentham's famous Panopticon architectural design is based: the potentially 'all-seeing' structure of the Panopticon assures the 'automatic functioning of power'.[103] Such surveillance, which both privacy and data protection seek to deter, can hinder individual development by leading to conformity and 'an unarmed occupation of individuals' lives'.[104] However, surveillance – acutal or perceived – is not the only such obstacle to personal development.

An individual may feel more or less inhibited in different circumstances. For instance, a student may feel comfortable discussing his thoughts on government immigration policy in a student bar with his friends but may feel less comfortable discussing the same topic in his local town or with his family. Stated otherwise, an individual's public persona may have mutliple facets. Consequently, individuals may want to engage in what this paper terms 'selective presentation': presenting to others only those parts of themselves which they want those others to see. Such selective presentation enables individuals to put forth different versions or aspects of

[101] Art 17 Directive 95/46 EC (n 5). Moreover, art 23 of the Directive obliges Member States to ensure that data controllers compensate individual data subjects for damages suffered as a result of unlawful processing or processing incompatible with the national implementation provisions. However, the Commission's report notes that there remain considerable difficulties in practice in demonstrating who was responsible for data release; hence there have been very few successful lawsuits to date. European Commission, 'Report on Identity Theft/Fraud', Fraud Prevention Expert Group, Brussels, 22 October, 2007, 27. <http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf>.

[102] Arts 31 and 32 of the Proposed Regulation (n 18).

[103] JH Reiman, 'Driving to the Panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future' (1995) 11 Santa Clara Computer & High Technology Law Journal 27, 35.

[104] Slobogin (n 96) 266.

themselves in different contexts. Consequently, those in work may see one side, those at home will see another while those at social events or competitions may see yet another side again.[105] This differentiation in terms of how people present themselves to others is an accepted part of daily life. For example, the possibility on social networking sites, such as Google+ and Facebook, to limit the availability of certain content to only specific contacts is a reflection of this fact. Equally, individuals frequently tailor the content of what they express to their target audience: few would speak as frankly to their boss about their work as they would to their spouse, for instance. The unauthorised merging of the various facets of an individual's persona can have serious tangible consequences. For example, anecdotal evidence would suggest that individuals have been denied employment or access to certain universities on the basis of the personal data they have made available on social networking sites. However, perhaps more significantly the unauthorised merging of personas can also have a censoring effect on individual behaviour and expression similar to that engendered by surveillance.[106] Indeed, it has been documented that individuals make less effort to tailor how they present themselves and have fewer inhibitions when fewer people are around.[107]

It is suggested that the right to data protection more effectively facilitates 'selective presentation' than the right to privacy thereby preventing tangible and intangible harms and promoting self-development and the personality rights of individuals. While the right to privacy is a broad notion which is 'not susceptible to exhaustive definition' and which lends support to the 'autonomous capacities of individuals to act and cooperate'[108], a right to self-determination has not yet been established in the ECtHR's Article 8 jurisprudence.[109] Similarly, informational self-determination is not explicitly mentioned in Article 8 of the EU Charter despite the fact that draft formulations of the right to data protection in the Charter had a greater emphasis on the notion of informational self-determination. For instance, the draft of the Charter dating from 5

[105] AE Taslitz, 'The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions' (2002) 65 Law and Contemporary Problems 125, 152.

[106] Josh Blackman, 'Omniveillance, Google, Privacy in Public, and the right to your digital identity: a tort for recording and disseminating an individual's image over the internet' (2009) 49 Santa Clara Law Review 313, 347. It can also have the effect of denying an individual of an opportunity which he might otherwise have benefited from. Had these individuals availed of the options for self-presentation available on these sites, these unfortunate consequences could have been avoided.

[107] NA Moreham, 'Privacy in Public Places' (2006) 65 Cambridge Law Journal 606, 622.

[108] Rouvroy and Poullet (n 14) 47.

[109] *Pretty* (n 93).

May 2000 provided that '[e]veryone has the right to determine for himself whether his personal data may be disclosed and how they may be used'.[110] A number of factors may explain the late change of wording of the right to data protection. For example, 'informational self-determination' may have been perceived by the drafters as more closely aligned to the German legal system[111] than was appropriate in the pluralistic EU legal order. Alternatively, the drafters may have recognised the limits of informational self-determination as these earlier formulations of the Charter expressed the individual's ability to make decisions regarding the disclosure and use of his personal data in absolute terms. However, such absolute terms do not reflect the reality that, for instance, in some circumstances the will of the individual will be prevailed over by the common interest.

Nevertheless, despite the departure in the EU Charter from the terminology of informational self-determination, it is argued that this concept remains a central tenet of the right to data protection and one which distinguishes it from the right to privacy. Data protection provides the individual with more informational rights than the right to privacy. For instance, the Proposed Regulation provides individuals with a right to data portability as well as a right to be forgotten. One explanation for these rights is that they allow individuals to better determine how their data is processed, by whom and for what purposes. In other words, they promote informational self-determination. This informational self-determination allows individuals to self-present: by providing individuals with more control over their personal data, they can reveal different elements of their personality to different audiences in contrast to the 'one size fits all' revelations which characterise a lack of control over personal information.

Moreover, the notion that informational self-determination is not an end in itself but rather it serves to promote the individual's right to personality (whether through freedom from unauthorised surveillance or by facilitating individual self-presentation) is one which has been

[110] Similarly, the 14 June 2000 version stipulated that 'Everyone has the right to determine for himself whether personal data concerning him may be collected and disclosed and how they may be used'. See CHARTRE 4284/00, 14 and CHARTRE 4360/00, 25 respectively. See Cannataci and Mifsud-Bonnici (n 2) 10.

[111] The German Constitutional Court held in its 1983 Population Census Decision that individuals must, in principle, be able to determine whether their data are disclosed and the use to which those data are put. These rights, which are stemmed from the individual's right to 'informational self-determination'.

endorsed by the German Constitutional Court. In its 1983 Population Census decision[112] the Court held that that the right to informational self-determination of individuals is itself based on the right to personality and human dignity.[113] This perspective has also been endorsed by data protection scholars such as Rodotà who observed that the EU had 'reinvented' data protection by turning it into 'an essential tool to freely develop one's personality'.[114]

### *2. Data Protection as a Positive Right to Reduce Information and Power Asymmetries*

The second major distinction which it is argued exists between the rights to data protection and privacy is that data protection is a proactive tool to reduce power and information asymmetries as it strengthens the hand of the individual vis-à-vis data controllers and processors. In this regard, the regulatory origins of the right to data protection become apparent: these power and information asymmetries are market failures which data protection legislation seeks to correct.[115] Power asymmetries are present when one party in a relationship is in a position of relative strength to the other while information asymmetries are present when one party in a relationship is in possession of more information than another.[116] Power and information asymmetries therefore lead to an unbalanced relationship between individuals (or data subjects) and other data processing actors. Information technology often serves to exacerbate the problem.[117]

---

[112] Judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65, 1. The text of this judgment is not available in English. This has been confirmed by Hornung and Schnabel who provide a detailed account of the judgment 'to help overcome the language barrier that has prevented much of the world from understanding the depth and value of German legal theory on data protection'. See G Hornung and C Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25 Computer, Law and Security Review 84.

[113] Art 2(1) and art 1(1) respectively. German Basic Law (Deutscher Bundestag, Basic Law for the Federal Republic of Germany, <www.btg-bestellservice.de/pdf/80201000.pdf>).

[114] S Rodotà, 'Data Protection as a Fundamental Right' in S Gutwirth, Y Poullet, P De Hert, S Nouwt and C De Terwangne (eds), *Reinventing Data Protection*? (Springer, 2009), 80.

[115] C Veljanovski, 'Economic Approaches to Regulation' in R Baldwin, M Cave and M Lodge (eds), *The Oxford Handbook of Regulation* (OUP, 2010), 18.

[116] For instance, the Electronic Privacy Information Centre (EPIC) argues, with regard to online behavioural advertising, that 'opaque industry practices result in consumers remaining largely unaware of the monitoring of their online behaviour, the security of this information and the extent to which this information is kept confidential'. See, EPIC, 'Search Engine Privacy', accessed 14 September 2012 <http://epic.org/privacy/search_engine/> .

[117] See, for instance, Purtova who argues that 'The vulnerability of the data subject stems from both the widely acknowledged inequality of resources of the individual and of the organisation and from the fact that, at present, most of the interactions between these two parties involve information technology, where the organisation has the benefit of professional expertise and the individual is but a layman': Purtova (n 59) 205.

As Purtova notes, as a result of such power asymmetries 'an individual is almost always a weaker party who is unable to protect his interests without state intervention'.[118] The individual's position of relative weakness is problematic for several reasons. First, information asymmetries make it more difficult for individuals to make an informed choice about how their personal data are processed, in particular because it is difficult for individuals to assess the likelihood that the use of their data will result in harm and the seriousness of this potential harm.[119] Secondly, information asymmetries can also constitute an obstacle which individuals must surmount in order to hold those who process their personal data accountable. This is because individuals are often unable to identify the responsible actors as a result of these information asymmetries.[120] Thirdly, information and power asymmetries also clearly disadvantage the bargaining position of an individual vis-a-vis a data processor or controller. For instance, Rotenberg has convincingly argued that the effect of data profiling is that 'consumers give up the privacy of their reservation price but the seller doesn't'. In this way, the balance of power in a transaction (for instance, the purchase of flights online) is tipped in favour of the profiler to the detriment of the consumer.[121]

Information and power asymmetries can also have less immediately discernible effects however. Broadly speaking, these asymmetries can have a negative impact on individual autonomy.[122] This is because individuals may feel helpless when faced with such asymmetries. As Dyson highlights, '[N]o one knows what is known and what isn't. It's the one-way mirror effect that makes people so uneasy'.[123] Indeed, Solove argues that it is incorrect to frame the

[118] Purtova notes that 'an individual's autonomy to make choices – even very simple ones like what book to read next – is questionable when the range of options and the context of the choice are being controlled by others'. Ibid 205.

[119] Prins argues that individuals may not always capture the value of privacy rights. She states that this 'relates to the larger problem of the information asymmetry that exists between companies and consumers. It seems very difficult for individuals to understand what is actually going on when online businesses collect and distribute their personal data and be sufficiently attentive to the implications of such use for their proprietary rights, let alone that they can verify what is really going on'. C Prins, 'When personal data, behaviour and virtual identities become a commodity: Would a property rights approach matter?' (2006) 3 SCRIPT-ed 270, 297.

[120] Berger makes this point in relation to online behavioural advertising: D Berger, 'Balancing Consumer Privacy with Behavioural Targeting' (2011) 27 Santa Clara Computer & High Technology Law Journal 3, 13.

[121] M Rotenberg, 'Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)' 2001 Stanford Technology Law Review 1, 31-32.

[122] Purtova (n 62) 47.

[123] For instance, Dyson notes that 'No one knows what is known and what isn't. It's the one-way mirror effect that makes people so uneasy'. E Dyson, 'Privacy Protection: Time to Think and Act Locally and Globally' (1998) 3 First Monday, 1 June 1998. Accessed 12 September 2012 <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/599/520>.

problems engendered by personal data processing in Orwellian 'Big Brother' terms on the basis of surveillance. Rather, he suggests that the harm which data processing causes relates to the sense of powerlessness felt by individuals in the face of personal data processing.[124] Solove therefore describes the problem as Kafkaesque: data processing alters the relationships that individuals have with those making decisions about their lives.[125] Similarly, Glancy notes that the movements of individuals can increasingly be tracked without their knowledge, and that 'the realisation that such centralised tracking is possible impresses a profound sense of powerlessness upon an individual and affects her choices about where, and where not, to go'.[126]

It is suggested that the right to data protection goes further than the right to privacy in rectifying and mitigating these power and information asymmetries by anticipating that 'individuals...have difficulty asserting their preferences for privacy protection' and consequently it consists of 'a set of legal norms that balance individual privacy interests against those of industry and bureaucracy'.[127] Indeed, the Dutch Government explicitly rejected the recognition of a constitutional right to informational self-determination 'fearing that such a right would tilt the balance between the individual and the state too far in favour of the data subject'.[128] How then does the right to data protection help mitigate and redress these power and information asymmetries? The right to data protection and data protection regulation help to readjust the balance of power between the data subject and those who process personal data primarily by ensuring that the latter 'adhere to established limits on the way they use personal information' without which individuals feel powerless.[129] One such obvious limitation is the principle of purpose limitation according to which personal data must be 'collected for specified, explicit and

[124] DJ Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745, 752.

[125] This is a reference to Franz Kafka's novel, *The Trial*, where a bureaucracy whose purposes are unknown uses people's information to make decisions about them while refusing to inform these people about how and why their information is being used. Ibid, 757.

[126] DJ Glancy, 'Privacy on the Open Road' (2004) 30 Ohio Northern University Law Review 295, 328. Similarly Calo describes the problem as 'less a function of top-down surveillance by a known entity for a reasonably clear if controversial purpose. It is characterized instead by an absence of understanding, a vague discomfort punctuated by the occasional act of disruption, unfairness, or violence': R Calo, 'The Boundaries of Privacy Harm' (2011) 86 Indiana Law Journal 1131, 1158.

[127] AL Newman, *Protectors of Privacy* (Cornell University Press, 2008), 24.

[128] Brouwer (n 62) 199

[129] Solove, 'Nothing to Hide' (n 121) 771.

legitimate purposes and not be further processed in a way incompatible with those purposes'.[130] Indeed, Article 8 of the EU Charter explicitly reiterates this principle when it states that data must be processed for specified purposes. This principle helps to create an 'informational division of powers'[131] as personal data cannot be freely exchanged in and between public and private bodies: it can only be processed and exchanged for specified purposes.[132]

The EU's Proposed Data Protection Regulation, which like the Directive gives expression to the right to data protection, also contains several provisions which seek to redress these power and information imbalances. Take the following examples. First, pursuant to the Proposed Regulation consent will not constitute a valid legal basis for data processing when there is a clear imbalance of power between the data subject and the data controller.[133] The Regulation states that this is 'especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context'.[134] The UK's regulator, the Information Commissioner's Office (ICO), has correctly highlighted that this broad claim – that consent should be invalid where there is a 'significant imbalance' between the data subject and the controller – requires qualification.[135] Indeed, it could be argued that this tips the balance of power too much in favour of the data subject: it is easy to think of examples where employer data processing is in fact data subject led, for instance when an employee consents to personal data processing to join a subsidised cycle-to-work scheme. Secondly, the Proposed Regulation now explicitly requires consent to be 'opt-in' in order to be valid.[136] This 'opt-in' default setting means that the data subject must indicate his or her agreement to the data processing 'either by a statement or by a clear affirmative action'.[137] Such an opt-in default setting can reduce information asymmetries as it is 'information-forcing' in so far as it places 'pressure on the

[130] Art 6(1)(b) Directive 95/46 EC (n 5).
[131] Brouwer (n 62) 201.
[132] Ibid, 202.
[133] Recital 34 Proposed Regulation (n 18).
[134] Ibid.
[135] Information Commissioner's Office, 'Initial analysis of the European Commission's proposals for a revised data protection legislative framework' <http://www.ico.gov.uk/news/current_topics.aspx> (27 February 2012), 7.
[136] Such a default setting is already found in the E-Privacy Directive for the collection of data using cookies.
[137] Art 4(8) Proposed Regulation (n 18).

better-informed party to disclose material information about how personal data will be used'.[138] Thirdly, the Proposed Regulation seeks to render the rights of data subjects more effective. For instance, it imposes an obligation on controllers to adopt procedures and mechanisms to respond to data subject access requests within set deadlines and to give reasons in the event that they refuse to take action.[139] These more effective rights strengthen the hand of the individual data subject vis-a-vis those who process personal data.

In this section, it has been argued that the right to data protection grants individuals more control over more data than the right to privacy for two primary reasons: first, to promote informational self-determination which itself flows from the individual's right to personality and second, to redress detrimental power and information asymmetries between data subjects and those that process their personal data. Indeed, De Hert and Gutwirth[140] argue that while privacy is a tool which facilitates individual opacity[141] as it protects individuals from intrusion, data protection promotes transparency and accountability.[142] While the distinction between privacy and data protection may be more nuanced – as the right to privacy has evolved beyond protecting intrusion into seclusion and data protection can also protect individuals from such intrusion – this distinction serves to highlight that data protection constitutes a positive instrument to equip the individual to cope with personal data processing.

Given the significant overlap between the rights, some may nevertheless seek to argue that this distinction is merely an academic one with little practical significance. Indeed, as was demonstrated in section two, the EU's highest jurisdiction, the Court of Justice, continues to

[138] PM Schwartz, 'Property, Privacy and Personal Data' (2004) 117 Harvard Law Review 2055, 2100.

[139] Art 12 Proposed Regulation (n 18)

[140] P De Hert and S Gutwirth 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence' in Institute for Prospective Technology Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview*, Technical Report EUR 20823 (European Commission-Joint Research Centre, 2003), 111-162.

[141] The term 'opacity' is not defined. However, the authors do state that '[t]he use of the word "opacity" designates a zone of non-interference which in our opinion must not be confused with a zone of invisibility: privacy for instance does not imply secrecy, it implies the possibility of being oneself openly without interference. However, 'opacity' contrasts nicely with 'transparency': ibid, 134.

[142] This distinction is also seemingly supported by Solove, who refers to privacy as the 'secrecy paradigm', noting that its predominant concern is to promote concealment and that it 'focuses on breached confidentiality, harmed reputation and unwanted publicity'. He argues that data protection differs from privacy in so far as 'the problem with databases pertains to the uses and practices associated with our information, not merely whether that information remains completely secret': D Solove, *The Digital Person: Technology and privacy in the information age* (New York University Press, 2004), 43.

conflate the two rights. However, it is argued that clarity on the distinction between the two rights is necessary for two reasons. Firstly, and perhaps most crucially, the continued conflation of these rights stunts the development of the right to data protection with the risk that its 'added values' – its potential to foster the individuals' right to personality and reduce information and power asymmetries – will be overlooked. Secondly, the current lack of consensus in EU jurisdictions regarding the relationship between these rights jeopardises the harmonised application of EU data protection rules. Take the following example. In the English case of *R v Brown (Gregory Michael)*[143] the defendant, a police officer, accessed the Police National Computer (PNC) database on two occasions to assist a friend who ran a debt-collection agency by checking vehicles owned by debtors from whom the agency had been employed to recover debts. No personal data was retrieved on the first occasion; on the second occasion, personal data was revealed but no subsequent use was made of that data. The defendant was charged with the criminal offence of 'use' of personal data for purposes other than those permitted, contrary to the UK's Data Protection Act. On appeal, the House of Lords rejected the prosecution's contention that the offence was committed as soon as personal data were retrieved from the computer with the intention of using the information for an unregistered purpose. The House of Lords held that something had to be done with the data beyond accessing them in order for criminal sanctions to ensue. Clearly, if a purposive approach to data protection was taken in this context, it could be argued that the access to the personal data on the PNC database for entirely unauthorised purposes exacerbated the power asymmetries between the police officers – the data controllers – and the individual and therefore the data protection rules should apply. However, in advocating a narrow definition of the term use, Lord Goff ignored these purposes of the Act by arguing that 'the statutory purpose of the Act is to protect personal data from improper use (or disclosure).[144] While the case could also be confined to its facts in so far as it involves the imposition of a criminal penalty[145], it nevertheless demonstrates the importance of clearly identifying the objectives of the right to data protection in the EU. A court in a different jurisdiction taking a different view of the purposes of the right to data protection (for instance, acknowledging that it seeks to promote informational self-determination) could easily have reached the opposite

[143] *R v Brown (Gregory Michael)* [1996] AC 543.

[144] Ibid, 550.

[145] Lord Hoffman emphasized that the Act treats 'processing' differently from 'using': while the retrieval of the data constituted improper processing, contrary to the data protection principles, it was not criminally punishable 'use', 562.

conclusion on the same facts. In this way, a lack of consensus regarding the role of intangible harm in the interpretation and application of EU data protection law also undermines data protection's market integration objective.

## V. Conclusion

The revelations of the Summer of 2013 that the US and UK government allegedly engaged in large scale individual surveillance based on data gathered by or transmitted on behalf of private entities had the positive effect of pushing personal data protection to the forefront of public consciousness. Data protection has occupied such a prominent position on the legislative agenda in the EU since the Commission published its proposed reform package in January 2012. This reform package is largely touted as the most contentious and lobbied piece of legislation to ever pass through the EU legislative process with over 4,000 amendments to its text proposed during its initial reading by the European Parliament. Data protection is beginning to take shape and gain importance in the eyes of the public as well as policymakers The aim of this paper was to explore the relationship between this key right in the EU legal order and the existing right to privacy. It demonstrates that, to date, the right to data protection has been treated as a subset of the right to privacy by the CJEU. However, it argues that this conflated vision of the two rights is misconeived and that the right to data protection provides individuals with more control over more personal data than the right to privacy. This enhanced control, it is submitted, serves two key purposes: first, it promotes the right to personality of individuals through informational self-determination and second, it reduces the information and power asymmetries which can have a negative impact on individual autonomy. At a time when personal data processing has reached an unprecedented scale, the benefits of this enhanced individual control should not be overlooked as readily as they have been to date by the CJEU. It is time to recognise a truly independent right to data protection.