The Conceptual Relationship Between Privacy and Data Protection

Aidan Forde[1]

1. Introduction

RECENT DECISIONS FROM the Court of Justice of the European Union ('CJEU') in *Google Spain*[2], *Digital Rights Ireland*[3] and *Schrems*[4] illustrate an increasingly emboldened stance towards informational privacy and data protection issues by the CJEU.[5] In order for the judicial adjudication of privacy before the CJEU to be effective, it is necessary to pinpoint the inherent value of privacy, its conceptual foundations, and any competing considerations. After the Lisbon Treaty, informational privacy is now recognised as having attained the status of a constitutional right across the EU landscape, finding its constitutional

[1] BCL (Int.), LL.M. (Cantab), Aidan.forde@cantab.net.

[2] C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] All ER (EC) 717.

[3] Joined Cases C-293 & 594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* [2014] All ER (D) 66 (Apr).

[4] C-362/14 *Maximillian Schrems v Data Protection Commissioner* (6 October 2015).

[5] Informational privacy is founded upon personal autonomy and involves protecting and controlling information relating to the individual. It surrounds 'The freedom of the individual to decide on himself is at stake when the individual is uncertain about what is known about him, particularly where what society might view as deviant behaviour is at stake (the chilling effect). The individual therefore has the right to know and to decide on the information being processed about him. At the same time, as a social being, the individual cannot avoid becoming the object of information processing. However, limitations to his basic right are to be accepted only when there is an overriding general interest and where that interest is molded into a law that follows the basic requirements of clarity and proportionality. To protect these principles, a number of safeguards are required: the safeguards consist of data protection principles (correctness, timeliness, purpose limitation, fairly and lawfully obtained), derived rights (access, correction), and organisational safeguards (independent institutions).' BVerfGE 65, 1 ff (1983). Lynskey notes that ' ' Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (2015) 63 International & Comparative Law Quarterly 569, 590.

basis in article 8 of the Charter of the European Union ('EU Charter'). Under the framework of the European Convention of Human Rights ('ECHR'), informational privacy has been considered under Article 8 of the Convention.[6] The trouble arises, however, in identifying the conceptual foundations of the right to informational privacy under both the EU Charter and the ECHR. Though located in separate provisions of distinct instruments[7], there is, in recent times, an increasing convergence in the conceptual bases upon which the CJEU and European Court Human Rights ('ECtHR') have upheld informational privacy claims.

This article seeks to examine the relationship between the right to informational privacy and the right to data protection under both the EU Charter and the ECHR, utilising the perspectives offered by Paul de Hert and Serge Gutwirth, Lee Bygrave, and Orla Lynskey to critically analyse these two significant rights. Section 1 of this Article will outline the benefit of data protection. Section 2 will outline the perspectives offered by Paul de Hert and Serge Gutwirth, Lee Bygrave, and Orla Lynskey in turn. Section 3 will tie each of these theories together. I will conclude that, in light of the analysis of these theories, that data protection is located on the fringes of privacy and that many of the justifications for data protection overlap with the justifications for privacy.

2. The Benefit of Data Protection

It is an onerous task to identify a unified conceptual understanding of privacy. Controversy surrounds its relationship with data protection.[8] Notwithstanding the battle to identify such a unified conceptual understanding of privacy,[9] elucidating the relationship between privacy and data protection is something of clear benefit to democracy and society. Preventing disproportionate and unlawful intrusion into privacy serves as a shield to totalitarian states.[10] Totalitarianism flourishes when privacy rights are diminished. By contrast, a healthy democratic state will

[6] See 'Internet: Case-law of the European Court of Human Rights' (June 2015), 8 <http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf> Accessed 23 August 2016.

[7] TJ McIntyre, 'Implementing Information Privacy Rights in Ireland' in Suzanne Egan (ed) *International Human Rights: Perspectives from Ireland* (Dublin: Bloomsbury, 2015) 294.

[8] Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3(4) International Data Privacy Law 222–228; Raphael Gellert and Serge Gutwirth, 'The legal construction of privacy and data protection' (2013) 29(5) Computer Law & Security Review; Peter Blume, 'Data Protection and Privacy—Basic Concepts in a Changing World' (2010) 56 Scandanavian Studies in Law 297–318.

[9] ibid.

[10] Daniel J. Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 Stanford Law Review 1393; Neil M. Richards, 'The Dangers of Surveillance' 2013 126 Harvard Law Review 1934; Hina Sarfaraz, 'Surveillance, privacy and cyber law' (2014) 20 7 Computer and Telecommunications Law Review 189.

enable its citizens to live independent and informed lives.[11] When unlawful and disproportionate interference with the private zone occurs, the citizen should have an accessible and effective procedure to vindicate their rights. Establishing a functioning system where privacy and data protection are protected thus assists in achieving a free democratic communicative order.[12]

A culture concentrated on protecting privacy within Europe focuses on pluralism, democracy and autonomy. Autonomy is central to conceptualising both privacy and data protection. Differences are to be observed between substantive and informational privacy.[13] Substantive protection allows the individual to engage in daily affairs free from the threat of state coercion or harm. Privacy creates the environment through which informational autonomy can be exercised.[14] Data protection mechanisms such as data portability, rectification and erasure hand the individual greater control over content personal information. In the absence of such controls, human vulnerability increases. As Feldman notes, '[i]f people are able to release [private] information with impunity, it might have the effect of illegitimately constraining a person's choice as to his or her private behaviour, interfering in a major way with his or her autonomy.[15] Effective data protection provisions assist citizens to achieve human development and flourish within society. This ultimately contributes to the maintenance of healthy democracy and encourages civic engagement.[16] Data protection lessens surveillance woes and the feeling of living within a panoptical society.[17] Gutwirth notes that privacy forms a bedrock of democratic society 'because it affects individual self-determination; the autonomy of relationships; behavioural independence; existential choices and the development of one's self; spiritual peace of mind and the ability to resist power and behavioural manipulation'.[18] Data protection mechanisms lead citizens towards actualising greater personal freedom. Data protection tools such as right to be informed, access, rectification, erasure and object place constraints on information monopolists and states' storage of personal data. Such data protection

[11] Kirsty Hughes, 'The Social Value of Privacy' In Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015) 228.

[12] ibid.

[13] Helen Fenwick, *Civil Liberties and Human Rights* (Routledge 2009) 805.

[14] ibid.

[15] David Feldman 'Secrecy, dignity or autonomy? Views of privacy as a civil liberty' (1994) 47(2) Current Legal Problems 42, 54.

[16] Rachel L. Finn, David Wright and Michael Friedewald, 'Seven Types of Privacy' in Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet (eds) *European Data Protection: Coming of Age* (Springer Science and Business Media 2013) 9.

[17] John Edward Campbell and Matt Carlson, 'Panopticon.com: Online Surveillance and the Commodification of Privacy' (2002) 46(4) Journal of Broadcasting & Electronic Media 586; Malcolm White, 'Bentham and the panopticon: totalitarian or utilitarian?' (1995) 2 UCL Jurisprudence Review 67; David Lyon, 'Everyday surveillance: Personal data and social classifications' (2002) 5(2) Information, Communication & Society 242.

[18] Serge Gutwirth, *Privacy and the information age* (Rowman & Littlefield Publishers 2002) 30.

tools subject states and corporates to greater scrutiny, promote a culture focused on civil liberties and prevent the fuelling of 'surveillance focused' societies.[19] Data protection therefore has a positive effect on substantive privacy. Such mechanisms increase societal well-being overall and provide valuable tools through which the individual can remedy the asymmetric relationship between the citizen and state, where appropriate.

3. Discourse

As outlined, the concepts of privacy and data protection provide clear benefits to society. At a judicial level, these concepts have been conflated resulting in discordance in the adjudication of privacy issues. This Section shall accordingly proceed to consider this conceptual conflation in light of the perspectives of a) Paul de Hert and Serge Gutwirth, b) Lee Bygrave, and c) Orla Lynksey.

A. de Hert and Gutwirth

Paul de Hert and Serge Gutwirth's framework considers privacy to be a 'tool of opacity' and data protection a 'tool of transparency'.[20] This separatist model asserts that privacy and data protection undertake distinct, fundamental functions but, at the same time, remain complementary. Under this model, privacy serves an 'opacity function' by preventing interference into private life, limiting state power and disproportionate encroachment upon the private sphere. Data protection serves a 'transparency function' by defining the rules that make the processing of data permissible. Data protection channels and controls the processing of information, placing obligations on the controller and granting rights to the data subject.[21] This framework is placed against the backdrop of the democratic constitutional state. The complementary but distinct roles of privacy and data protection serve as constraints on state power.[22] According to de Hert and Gutwirth, data protection is a 'catch-all term' for a multiplicity of ideas relating to the processing of personal data.[23] It is through the application of these ideas that governments attempt to reconcile privacy with surveillance, taxation, and the free flow of information.[24]

[19] In exploring the benefits of privacy as a personality right and its contribution to human flourishing, see: Bart van der Stroot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"' (2015) 31(80) Utrecht Journal of International and European Law 25.

[20] Paul de Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in A. Duff and S. Gutwirth (eds), *Privacy and the criminal law*, (1st edn, Intersentia 2006).

[21] ibid at 4.2.

[22] ibid.

[23] Paul de Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxenbourg: Constitutionalisation in Action', *Reinventing Data Protection?* (Springer 2009).

[24] ibid.

Providing helpful analysis of de Hert and Gutwirth's framework, Noberto Nuno Gomez de Andrade notes that the tools of opacity and transparency do not exclude each other.[25] On the contrary, 'each tool supplements and pre-supposes the other'.[26] Privacy is a substantive right, while data protection is procedural.[27] Privacy serves as a normative tool, assisting in the realisation of individual freedoms—for example voting for local and national political representation or referendum by secret ballot. The substantive nature of privacy is observed in the judicial exercise of shielding the individual from disproportionate intrusion into one's private life by private and state entities.[28] Procedural rights appear at a later stage, once substantive rights have been weighed, and are formal in design.[29] Procedural rights (such as a right to rectification) aim to hold those who possess power to account. These 'transparency tools' assist in realising the substantive rights environment. Procedural rights formulate the legal conditions and procedures through which substantive rights are expanded.[30] Effective realisation and enforcement of privacy rights are supplemented by data protection rules. The rights which the General Data Protection Regulation creates assist in bolstering privacy rights across the Union. Under this scheme, data protection ranks below privacy and serves a supportive and ancillary function. It places a structure through which the processing of information concerning the individual is respected. As a procedural 'tool of transparency', data protection has no real value; it merely serves as a facilitator of privacy.

De Hert and Gutwirth's analysis is helpful in its simplicity and coherence. The theory properly locates the function of data protection within the democratic constitutional order. Privacy and data protection assist in permitting the individual to maintain control over individuality. Data protection is not a later 'spin off' of privacy, but clarifies the conditions through which processing of information concerning the individual becomes legitimate.[31] This theory illustrates that, given their diverging functions; privacy and data protection are best not placed within the same bottle.[32] De Hert and Gutwirth conclude that 'data protection principles might seem less substantive and more procedural compared to other rights… they are in reality closely tied to substantive values and protect a broad scale of fundamental values'.[33]

[25] Norberto Nuno Gomes de Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer-Hübner and others (eds), *Privacy and Identity Management for Life*, (1st edn, Springer Berlin Heidelberg 2011) 96.

[26] ibid.

[27] ibid.

[28] ibid.

[29] ibid.

[30] ibid.

[31] ibid 96.

[32] ibid 97.

[33] Federico Ferretti, *EU Competition Law, the Consumer Interest and Data Protection: The Exchange of Consumer Information in the Retail Financial Sector* (Springer 2014) 105.

Despite the apparent clarity of de Hert and Gutwirth's theory, criticisms emerge. Tzanou points out this separation attempts to show the independent value of data protection.[34] However, under this framework, data protection will always be dependent upon and ultimately collapse into privacy. Data protection is denigrated to rules detailing requirements for consent and legitimate processing of information. As a 'transparency tool', data protection rules serve to assist in the realisation of privacy. Even though de Hert and Gutwirth note the benefits of Article 8 of the EU Charter conferring independent constitutional status upon data protection, their formulation requires personal data breaches to be adjudicated with privacy, as opposed to a distinct consideration of data protection, taking precedence. The formulation undermines developing data protection as a distinct fundamental right. It dilutes the significance of informational privacy and data protection rights. Contemporary threats to informational privacy, such as those illustrated by the Edward Snowden revelations, highlight the importance of developing effective legal frameworks. Ensuring data protection and informational privacy are distinct fundamental rights increases protection against such threats.

The authors conclude '[o]pacity and transparency each have their own role to play. They are not communicating vessels.'[35] De Hert and Gutwirth fail to clarify the exact scope of 'opacity'.[36] There are clear benefits to a structure that separates privacy and data protection through the prisms of 'opacity' and 'transparency'. It creates a welcomed separation of the two tools' contrasting core roles. A problem with the theory is its failure to expand upon situations where tools of transparency fall upon opacity to justify their execution and existence. There is a failure to properly consider the opacity dimensions of data protection. This formulation envisages two lines that fail to communicate effectively. A failure to examine the opacity dimensions similar to both, risks the development and value of data protection as a distinct fundamental right. Since there will be areas of overlap and similarity, such a separatist formula raises concern. De Hert and Gutwirth

[34] Maria Tzanou, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 International Data Privacy Law 88.

[35] ibid.

[36] In particular, the authors do not define why 'opacity' as a key term is used: 'Opacity tools set limits to the interference of the power with the individuals' autonomy and as such, they have a strong normative nature. The regime they install is that of a principled prescription: they foresee 'no but…' law. Through these tools, the (constitutional) legislator takes the place of the individual as the prime arbiter of desirable or undesirable acts that infringe on liberty, autonomy and identity-building: some actors are considered unlawful even if the individual consents.' Serge Gutwirth and Paul de Hert, 'Regulating profiling in a democratic constitutional state' in Mireille Hildebrandt and Serge Gutwirth (eds), 'Profiling the European Citizen' (Springer 2009).

state that transparency and opacity will blend, but fail to comprehensively work through the opacity/transparency divide, stating:

> [D]ata protection principles might seem less substantive and more procedural compared to other rights norms but they are in reality closely tied to substantial values and protect a broad scale of fundamental values other than privacy. [37]

De Hert and Gutwirth recognise that placing data protection under the ambit of privacy could inhibit the societal benefits of data protection rights. By placing data protection under a purist transparency formula, it neglects the overall value and societal impact of data protection. By failing to effectively outline the relationship of opacity within data protection, it views data protection as an overly procedural mechanism. This results in its ultimate societal value being lost. It places data protection within an unrealistic cocoon. Privacy and data protection in the majority run in different directions. A complete conflation of the two risks conflicts but a complete separation also raises concerns.

1. The Danger of Proceduralisation

De Hert and Gutwirth discuss the 'danger of proceduralisation' in relation to the ECtHR's expansion of the right to respect for private life as encompassing data protection.[38] According to de Hert and Gutwirth, Article 8 ECHR jurisprudence has gone too far in expanding privacy to encompass data protection. Their theory illustrates the problems that can arise when privacy and data protection converge, without any sustained discussion as to their inherent differences. De Hert and Gutwirth believe that Article 8 is no place for procedural developments.[39] Procedural requirements are best located within the Article 13 right to an effective remedy for violations of Convention rights.[40] De Hert and Gutwirth contend that the ECtHR has utilised procedural rights to construe substantive norms. This has led to interpreting 'procedural rights narrowly'.[41] The benefits of proceduralisation include objectivity and impartiality. However, risks include 'the formalization, bureaucratization and de-politicisation of human rights questions'[42] In the well-known phone-tapping case of *Klass v Germany*, for example, the ECtHR outlined in detail the procedural constraints to be complied with for tapping to be legitimate.[43] De Hert and Gutwirth believe the 'necessary in a democratic society' element is

[37] De Hert and Gutwirth (n 23) 44.
[38] De Hert and Gutwirth (n 20) 87.
[39] ibid.
[40] ibid 88.
[41] ibid.
[42] ibid.
[43] *Klass v Germany* (1978) 2 EHRR 214.

neglected. In somewhat extreme sentiment, they assert proceduralisation 'might well bring the erosion of recognized rights'.[44]

If we envisage Article 8 as primarily dealing with protecting zones of opacity, bringing data protection elements under its remit is beyond its scope. Following this reasoning, questions surface concerning the ECtHR's future legitimacy in dealing with privacy claims. If the Court wished to develop data protection freedoms under Article 8, it needs to be clear as to the exact value of privacy in its foundation. Kirsty Hughes has recently outlined the societal values inherent to privacy within the ECHR and the ECtHR's overall principles.[45] Hughes submits that there is a failure of the ECtHR to articulate the societal value of privacy. To bolster the intellectual consistency of the Court, it should recognize that the value of privacy is essential to the democratic state and 'is crucial to facilitating harmonious social interaction'.[46] The ECtHR concentrates on the legality requirement and limits the 'necessary in a democratic society' discussion. Once the Court addresses if there is a legal basis for the infringement and finds a breach, it does not address the issue as to whether it the measure is 'necessary in a democratic society'. There is no sustained discussion as to how data protection freedoms contribute toward and are necessary to democratic society. In setting the foundation from which the ECtHR draws inspiration and adjudicates cases, it would require more from the state to justify proportionate interference.[47] An effective data protection framework should strive to locate the value and inspiration of data protection. As the ECHR remains ambiguous as to the central value of privacy, the Court has incorporated procedural elements. By failing to properly locate the conceptual foundations of privacy, confusion is increased when the Court strays into areas not traditionally envisaged by the Convention, like data protection. If the Court wishes to work through data protection through the ambit of Article 8, it should be clear from first principles as to the exact relationship between the two. Problems inherent to internal expansion notwithstanding, given that the Convention is a 'living instrument',[48] one can see a need to interpret Article 8 expansively to bring informational privacy under its ambit and Article 8 is arguably broad enough to found such development. Even though it may be misplaced, such development is necessary.

[44] De Hert and Gutwirth (n 20) 89. The authors ultimately feel that transparency mechanisms have no place within Article 8, concluding that the drafters of the Convention could not have envisaged the development of Article 8 as a source of procedural conditions and rights. This forms a view that Article 8 jurisprudence on this issue is misplaced and not currently fit for purpose.

[45] Kirsty Hughes, 'The Social Value of Privacy' (n 11) 228.

[46] ibid 238.

[47] ibid 240.

[48] George Letsas, 'Strasbourg's Interpretive Ethic: Lessons for the International Lawyer' (2010) European Journal of International Law 509.

2. The Charter

We observe De Hert and Gutwirth's opacity/transparency divide clearly within Article 7 and Article 8 of the EU Charter. Article 7 of the EU Charter unimaginatively recites Article 8 ECHR stating that 'Everyone has the right to respect for his or her private and family life, home and communications'.[49] Article 7 of the EU Charter falls under the 'opacity' formulation, preventing unwarranted intrusion by the state within the private sphere. Article 8 of the EU Charter outlines the 'transparency' elements supporting the realisation of Article 7's substantive formulation, guaranteeing the 'right to protection of personal data concerning him or her'[50] and requiring data be processed fairly and on the basis of consent or some other legitimate basis laid down by the law.[51]

While Article 7 EU Charter has its influence in Article 8 ECHR, given there is no distinct right to data protection under the ECHR and the piecemeal fashion through which the ECtHR has developed data protection freedoms, Article 7 EU Charter may be problematic when assessing its precise relationship to Article 8. The manner in which the CJEU adjudicates Article 8 data protection claims illustrates a continued reliance on the Article 7 right to privacy.[52] Currently, the two rights continue to be conflated with no clear conceptual footing. De Hert and Gutwirth's theory nonetheless illustrates the difference in logic between Articles 7 and 8 of the EU Charter. The underlying rationale for the separation of the two within the Charter remains unclear, perhaps purposely so. Their framework helps inform a broader picture, yet fundamentally neglects how the two should effectively communicate with and complement each other.

B. Lee Bygrave

In response to de Hert and Gutwirth's failure to locate the place of 'opacity' within data protection, Lee Bygrave's work contributes to examining this perceive gap. Bygrave expands upon the 'opacity' nature of data protection.[53] Bygrave asserts that it is not effective for data protection to be characterised or centrally concerned with privacy. It is under this construction that data protection is about the reconciliation of the interests of the data subjects with the legitimate interests of data controllers.[54]

[49] The wording of Article 8(1) is almost identical stating that 'Everyone has the right to respect for his private and family life, his home and correspondence'.

[50] Article 8(1), EU Charter.

[51] Article 8(2), EU Charter.

[52] Felix Bieker, 'The Court of Justice of the European Union, Data Retention and the Right to Data Protection and Privacy—Where Are We Now?' in Camenisch, Fischer-Hubner and Hansen (eds), *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (Springer 2015).

[53] Lee Bygrave, 'The place of privacy in data protection law' (2001) University of New South Wales Law Journal 241, 277–283.

[54] ibid.

Even though the evolution of data protection has been somewhat convoluted, Bygrave details nine elements of data protection: 'the fair and lawful processing principle, the transparency principle, the data subject participation and control principle, the purpose limitation principle, the data minimization principle, the information quality principle, the proportionality principle, the security principle, and the sensitivity principle.'[55] A failure to characterise privacy in terms of data protection is reflected in the difficulties in attempting 'to give privacy a precise, analytically serviceable and generally accepted meaning.'[56] The law's guidance and development is affected by the current dysfunctional relationship between the two. Bygrave is correct that the expansive nature of privacy forms part of the rationale for data protection. [57]

In line with the increased emphasis within the Article 8 ECHR jurisprudence considering the of benefits privacy for society and democracy, the values of personal identity that data protection helps to realise 'have a broader societal significance.'[58] In bridging the gap between privacy and data protection, Bygrave is correct in asserting that the general societal values common to both must be recognised when forming effective legal policy on data protection issues. De Hert and Gutwirth's theory neglects the impact that procedural data protection structures can have in modern constitutional democracy. It does so by failing to acknowledge the opacity and substantive benefits data protection has to the citizen and society. Second, data protection is concerned with 'setting standards for the quality of personal information' which has 'little direct connection' to privacy values.[59] Third, data protection rules are concerned with the legitimate processing of information, taking on a management quality.[60] In this sense, data protection orbits privacy, but never seeks to be attached. Both concepts coexist to prevent conflict by putting in place appropriate management strategies.[61] Bygrave concludes that while privacy occupies a place within data protection, viewing data protection as serving and securing privacy is problematic; data protection serves a multitude of interests that extend beyond privacy.

The focus of data protection laws shifts with technological developments. Attempts to create a 'right to be forgotten' illustrate an example of recent policy adapting to behavioural change.[62] The emergence of European data protection is observed within Convention 108, the 1995 Directive, and, most recently, the Regulation. The Regulation, due to come into effect in the spring of 2018, is a

[55] Frederik Zuiderveen Borgesius 'Privacy on the Internet' in Alberto Alemanno and Anne-Lise Sibony (eds) *Nudge and the Law: A European Perspective* (Bloomsbury Publishing 2015) 183.
[56] Bygrave (n 53) 278.
[57] ibid 281.
[58] ibid.
[59] ibid.
[60] ibid 282.
[61] ibid.
[62] C-131/12 *Google Spain* (n 2).

significant step in the evolution of European data protection policy. It contains a number of innovations, such as introducing a right to data portability and a right of erasure. As privacy concerns continue to increase with changes in human behaviour, so too does the focus of data protection laws and regulation. Yet we should still strive to locate the guiding principles and conceptual structures of informational privacy in order to bolster the intellectual consistency and future of this area. Collapsing data protection into privacy effectively renders the essential societal and democratic benefits of such rights incoherent and haphazard. The risk of the Article 8 ECHR approach where the ECtHR views data protection as a mere subset of privacy, risks diluting the constitutional value of data protection to 'soft law'.[63]

C. Orla Lynskey

Lynskey believes while data protection and privacy overlap, data protection offers individuals more rights than privacy. Data protection more effectively ensures 'selective presentation' of individual identity than the right to privacy, 'thereby promoting self-development and the personality rights of the individual.'[64] It assists in identity construction. By providing individuals with greater control over their personal data, the individual can 'reveal different elements of their personality.'[65] Effective data protection frameworks thus focus more on controlling disclosure of information. Privacy is not as focused in its informational management function. Data protection tools are concentrated on removing power and information asymmetries in the relationship between the individual and the data controller/processor.[66] Power asymmetries impact the ability of the individual to make an informed choice about whether to allow their information to be processed or not.[67] The right to data protection goes further than the right to privacy as it envisages that 'individuals . . . have difficulty asserting their preferences for privacy protection'.[68] Effective rules help to empower citizens and reduce power asymmetries. The right to data protection thus hands the individual more control than the right to privacy. Lynskey advises that the continued conflation of the right to privacy and the right to data protection is best avoided. Recognising the right to data protection as a right distinct from the right to privacy re-balances the asymmetric relationship between the individual and state or private entities. As the 'cascade of decaying information'[69] concerning the individuals online information only sets to increase, such protections have clear significance.

[63] De Hert and Gutwirth (n 23) 44.

[64] Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (2015) 63 International & Comparative Law Quarterly 590.

[65] ibid 591.

[66] ibid 592.

[67] ibid.

[68] ibid 594.

[69] Oskar Josef Gstrein, 'The Cascade of Decaying Information: Putting the "Right to Be Forgotten" in Perspective' (2015) 21 Computer and Telecommunications Law Review 40.

Lynskey's work is helpful in detailing the value of having a clear distinct right to data protection within the EU constitutional order. Lynskey explains that the CJEU continues to conflate the two rights in its adjudication after the Lisbon Treaty.[70] The discourse should focus on how best to ensure that the right data protection and the right to privacy should complement and inform, rather than converge. This approach will assist in further bolstering data protection rights for EU citizens. The earlier discussion about the 'dangers of proceduralisation' illustrates that a continued reliance by the CJEU on Article 8 ECHR to interpret the Data Protection Directive may be problematic. To ensure data is processed lawfully, the CJEU can rely solely on Article 8 of the EU Charter without resorting to reliance on Article 8 ECHR. Nonetheless, it is questionable whether strict reliance on Article EU Charter alone will be effective.

4. Comment

This brief review and assessment of the theories of de Hert and Gutwirth, Bygrave, and Lynskey illustrates the ambiguity surrounding the conceptual bases of privacy and data protection under the EU Charter and ECHR. Such ambiguity impacts upon adjudication of these issues within the Courts. This ultimately amounts to a disservice to expanding EU privacy rights. The three theories discussed each complement one another in informing a broader perspective. De Hert and Gutwirth's opacity-transparency formulation provides a clear framework for understanding the functional differences between the privacy and data protection. The theory fails, however, to discuss areas of overlap between privacy and data protection and fails to encourage effective dialogue between the two. It fails to discuss the 'opacity' nature of data protection and how it should engage with competing rights. Lee Bygrave's theory assists in these communication failures in correctly identifying that data protection assists the actualisation of privacy rights. Data protections aims and values go beyond privacy, however. Orla Lynskey finally places this continued conflation within its current context within the CJEU. Lynskey correctly identifies the importance in recognising data protection as a distinct right in increasing access to informational self-determination and preventing power asymmetries. In order for this potential tension between privacy and data protection to ease, we need to be clear about the exact values of data protection to society and democracy. Similar to the manner in which the ECtHR has failed to expand upon the benefits of privacy for societal well-being, failing to concentrate on the overall value of data protection mechanisms for the individual's benefit within democracy will decrease rather than bolster data protection rights.

Data protection is located on the fringes of privacy and many of the values and justifications for data protection overlap with those for privacy. Data protection

[70] Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (2015) 63 International & Comparative Law Quarterly 569, 579–581.

deduces its foundational inspirations from privacy, but remains distinct. Emphasis should be placed on data protection beyond a purely procedural or mechanical function. Effective data protection rules empower citizens and hand citizens greater control over personal information. This assists in achieving a free democratic order that values the individual's private sphere. Data protection is not of solely structural significance; it provides the structures through which the private sphere is respected. Whilst data protection rules outline principles that result in the proper processing of information, such structures have significant impact to the individual and democratic society. The two rights are reciprocal.

The current judicial approaches to Articles 7 and 8 of the EU Charter and Article 8 ECHR are inconsistent. Such inconsistency stems in part from a reluctance of the courts to clearly articulate the value of privacy to society. There is limited intellectual stability from the ECtHR in its development of the right to informational privacy. This flows from the ECtHR's inability to locate its intellectual footing in relation to the Article 8 ECtHR's substantive right to privacy. The CJEU's development of data protection freedoms under Article 8 of the EU Charter is similarly unstable. We remain unclear about the relationship between the Article 7 EU Charter right to privacy and the Article 8 EU Charter right to data protection, its impact upon private entities, and the place of Article 8 ECHR jurisprudence within the EU Charter framework. Increased discussion at a judicial level in locating the conceptual place of informational privacy assists in increasing legitimacy of the CJEU's recent emboldened approach. de Hert and Gutwirth's 'danger of proceduralisation' comment illustrates the problems of failing to give data protection independent constitutional status. It demonstrates the failure of the ECtHR to satisfactorily locate the intellectual routes of privacy.

In *Digital Rights Ireland*,[71] the CJEU utilised its own cases and Article 7 of the EU Charter to find the retention of data was unlawful.[72] It then referred to ECtHR cases to find that access to the data was a separate interference.[73] In seeking to outline the differences between data protection and privacy under Article 7 and Article 8 of the EU Charter, it ultimately enunciated identical versions.[74] *Google Spain*[75] epitomises the minimalist nature of the CJEU's reasoning and the problems this creates for the actualisation of the CJEU's judicial innovations. The CJEU gave no detailed assessment of the right to privacy or the competing considerations at play. In stark contrast to *Schrems,* there was a lack of engagement

[71] *Digital Rights Ireland* Joined Cases C-293/12 C-594/12 8 April 2014 (n 3).

[72] ibid paras. 33–34.

[73] ibid para. 35.

[74] Felix Bieker, 'The Court of Justice of the European Union, Data Retention and the Right to Data Protection and Privacy—Where Are We Now?' in Camenisch, Fischer-Hubner and Hansen (eds), Privacy and Identity Management for the Future Internet in the Age of Globalisation (Springer 2015).

[75] *Google Spain* (n 2).

with ECtHR judgments considering the Internet archives.[76] In determining when the 'preponderant interest'[77] where public interest requires retention of the material online, reference to *Von Hannover (no. 2)*[78] which considered such considerations in detail, would have been welcomed. *Google Spain* illustrates a failure of the CJEU to clarify the opacity dimensions of data protection rights, looking beyond the delisting of the search result as a procedural tool but how actualized the privacy rights engaged. *Schrems* relied upon Article 7 EU Charter in holding the intrusion violated the 'essence of privacy'.[79] It was not satisfactorily expanded upon what constitutes the 'essence of privacy', especially with reference to Article 7 EU Charter and what role (if any) Article 8 EU Charter plays within such adjudication.

In examining these judgments, it is difficult to gauge any broader or consistent reading as to the CJEU's conception of privacy and data protection. A contributory factor to this judicial inadequacy is a fundamental failure to articulate the foundations of data protection and privacy to the individual and society. The EU Charter paves the way forward at a European level for the protection of informational privacy. The CJEU's inability to effectively interpret and expand its provisions renders such judicial innovations haphazard and undermines the legitimacy of the CJEU in developing data protection rights. EU data protection can be viewed as both a sword and a shield. It protects individual's information in daily life from unlawful intrusion by states and private entities. Recent cases from the CJEU illustrate a judicial institution not afraid to utilise such provisions to hold both states and private entities to account for violations. This is so having little regard to possible political critique or economic considerations. On the other hand, within the ECHR, we may have to reassess whether Article 8 ECHR (in its current form) is the best place for expanding data protection freedoms. The Article 13 ECHR right to an effective remedy may be an appropriate alternative. It is not possible for data protection rights to be effectively actualised when the ECtHR remains unable to outline the intellectual stability of Article 8 ECHR right to privacy. Similarly, we remain unclear as to the foundations of the right to privacy and the right to data protection within the CJEU, the relationship between Article 7 and 8 of the EU Charter, and the place of Article 8 ECHR jurisprudence. In tackling these issues, both the ECtHR and the CJEU need to be clear from first principles about the relative significance of informational privacy. A failure to

[76] See *Case of Times Newspapers Ltd. (Nos. 1 and 2) v. The United Kingdom* Applications nos. 3002/03 and 23676/03, 10 March 2009; *Editorial Board of Pravoye Delo and Shtekel v. Ukraine* Application no. 33914/95, 5 May 2011; *Ahmet Yildirim v. Turkey* 18 December 2012, application No. 3111/10; *Wegrzynowski and Smolczewski v. Poland* Application No. 33846/07, 16 July 2013.

[77] *Google Spain* (n 2) para 98.

[78] Applications nos. 40660/08 and 60641/08, 7 February 2012.

[79] *Schrems* (n 4); see Martin Scheininm 'The Essence of Privacy, and Varying Degrees of Intrusion' *Verfassungsblog,* 18 November 2015 Available at: http://www.verfassungsblog.de/en/the-essence-of-privacy-and-varying-degrees-of-intrusion/#.Vkxi3nvFk14.

properly locate the place of data protection within Article 8 ECHR jurisprudence is problematic. Moreover, a systematic failure of the CJEU to work through the relationship between data protection and privacy and the possible competing considerations (most fundamentally, freedom of expression), raises questions as to the effectiveness of the Court's recent emboldened stance.

5. CONCLUSION

What role does the right to data protection play with regard to the right to privacy? Clearly the right to data protection and the right to privacy are interrelated and often overlap. Both add something of clear significance in providing for a free democratic communicative order. Data protection in the majority goes beyond privacy, but the two should communicate effectively. Recognising that data protection is a distinct right is necessary to ensure its continued expansion as 'hard law' at EU constitutional level. We must also recognise that from a conceptual perspective, a complete separation is not possible. This question comes at a time of increased discussions surrounding the Regulation. Whatever direction informational privacy may go, it should be guided with transparency in mind and preventing unnecessary tension within the two frameworks.

There are two principal conclusions. First, de Hert & Gutwirth's theory acts as a valued basis for assessing the relationship between the two. Their theory fails, however, to examine the 'opacity' dimensions of data protection and how it can effectively deal with competing rights. It does identify a procedural or 'transparency' line that mirrors the ECHR and EU Charter frameworks. Bygrave fills in some of the gaps in de Hert and Gutwirth's formulation. According to Bygrave, data protection orbits privacy, but ultimately remains a distinct right. Lynskey's work recognises the importance of viewing data protection as a distinct right in reducing power asymmetries and promoting informational self-determination. Moreover, she illustrates the importance of transferring discussion of this conceptual conflict to a judicial level. The ECtHR should reassess the exact place of data protection. The ECtHR should, to borrow a phrase from *Schrems*, reconsider what is the 'essence of privacy' and what role it plays within society. Only then can we assess the respective place of data protection.

Whatever problems the ECtHR has in terms of conceptualising privacy, the CJEU is a cause for greater concern. Fundamental rights may be viewed as a new area for the CJEU. If the CJEU continues its fervent expansion of privacy rights, it needs to be clear about its conception of privacy and the distinct but complementary roles of the EU Charter and ECHR. In order for such judicial growth to gather legitimacy, clarity concerning the conceptual roles of privacy and data protection is necessary. Otherwise, pivotal judicial developments created by litigants such as Max Schrems, Mario Costeja González, and Digital Rights Ireland could be futile.