



## Remembering and Forgetting - Protecting Privacy Rights in the Digital Age

ALLEN, SR

“The final publication is available at <http://edpl.lexxion.eu/article/edpl/2015/3/4>”

For additional information about this publication click this link.

<http://qmro.qmul.ac.uk/xmlui/handle/123456789/13675>

Information about this research object was correct at the time of download; we occasionally make corrections to records, please therefore check the published record when citing. For more information contact [scholarlycommunications@qmul.ac.uk](mailto:scholarlycommunications@qmul.ac.uk)

## ‘Remembering and Forgetting – Protecting Privacy Rights in the Digital Age’

Stephen Allen\*

Unedited Version of Article published in (2015) 1(3) *European Data Protection Review* pp.164-177: Lexxion, Berlin.

### Abstract

This article interrogates the nature and scope of the right to erasure through the lens of the CJEU’s decision in *Google Spain/Google Inc v AEPD/González*. It examines the reasoning adopted by the Advocate-General and the CJEU in this case as a means of assessing the interpretative techniques used by lawyers and decision-makers to resolve the normative conflicts that arise in privacy/expression disputes. It harnesses Koskenniemi’s work on the structure of legal argumentation for the purpose of analysing rights reasoning in the context of EU Data Protection law. It also explores the significance of the symbiotic relationship between privacy rights and expression rights with a view to providing the basis for achieving meaningful normative co-ordination in concrete cases.

### I. Introduction

This article examines the reasoning adopted in *Google Spain/Google Inc v AEPD/González* with a view to establishing the interpretative techniques used by lawyers and decision-makers to resolve the normative conflicts which arise when the fundamental rights to privacy and expression/information are engaged.<sup>1</sup> It harnesses Koskenniemi’s work on the structure of international legal argumentation for the purpose of analysing the grammar of fundamental rights reasoning with specific reference to EU Data Protection law.<sup>2</sup> Koskenniemi observes that law aspires to realise ideal behavioural standards for its subjects but it must also reflect social reality to ensure that law’s standards are achievable.<sup>3</sup> However, if legal standards are set

---

\* Senior Lecturer (Associate Professor) in Law, Queen Mary, University of London: [s.r.allen@qmul.ac.uk](mailto:s.r.allen@qmul.ac.uk).

<sup>1</sup> Case 131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos and Mario Costeja González* [1984] OJ 2014 C212/4. Specific references to this case will appear in square brackets in the text of the article.

<sup>2</sup> Martti Koskenniemi, *From Apology to Utopia: The Structure of International Legal Argument* (CUP, 2005).

<sup>3</sup> See section 2 below.

that are too high then law's normative demands cannot be met. Conversely, if law mirrors social facts it has no independent purposive function (it simply justifies established socio-political practices). Consequently, Koskenniemi claims that every legal argument must combine both normative and factual components for its validity to be assured. Situated lawyers switch between these countervailing elements in a manner that is both professionally-credible and consistent with their substantive aims. However, if their arguments veer too far to the extremes of 'normativity' or 'concreteness', they will lack plausibility. Moreover, Koskenniemi believes that these structural requirements render all substantive arguments indeterminate. Accordingly, he contends that decisions are not produced by the legal arguments invoked in particular cases. For him, they are determined by external factors in keeping with the preferences of decision-makers, preferences which reflect the institutional biases of the legal regime engaged by the dispute.

In this article, Koskenniemi's structural thesis is applied to the *Google Case*. Specifically, it is used to show how Advocate-General Jaaskinen's Opinion satisfied the credibility requirements of fundamental rights reasoning and it highlights the shortcomings of the Court's judgment in this regard. Further, it endeavours to account for the manner in which expression rights always seem to trump privacy rights in concrete cases. To this end, the article not only offers an understanding of the impulses that underpinned the Court's controversial judgment in the *Google Case* it also seeks to improve upon its reasoning in ways that should enhance the plausibility of institutional decisions reached in cases involving normative clashes between privacy rights and expression rights in the future.

The article is divided into six parts. The next section sets out Koskenniemi's structural thesis and assesses its resonance for fundamental rights reasoning. The

third section offers an overview of the salient legal issues arising in the *Google Case* before analysing the Advocate-General's Opinion and the CJEU's judgment by reference to Koskenniemi's thesis. The fourth section explores, more generally, the ways in which lawyers and decision-makers seek to resolve normative conflicts by means of rights-balancing. In particular, it examines the problem of determining the plausibility of legal arguments in ground-breaking cases. The penultimate section investigates the existence of a symbiotic relationship between privacy rights and expression rights – claims that the former are prerequisites for the exercise of the latter – with a view to providing the basis for achieving normative co-ordination in concrete cases. It harnesses the interpretative device of *lex specialis* as a credible means by which to address the problems of normative co-ordination in a contextually-sensitive, transparent and systematic manner. It also suggests that the use of this technique should be accompanied by the adoption of a more nuanced approach to the resolution of such disputes in digital settings along the lines suggested by Hartzog and Stutzman, in their seminal work on a nascent entitlement to data obscurity.<sup>4</sup> The final part offers some concluding remarks.

## II. The Structure of Legal Argumentation

In *From Apology to Utopia: The Structure of International Legal Argument*, Koskenniemi outlines the argumentative structure of international law. He claims that every credible international legal argument contains both utopian (normative) and realist (concrete) components.<sup>5</sup> He contends that law aspires to achieve ideal

---

<sup>4</sup> Woodrow Hartzog and Frederic Stutzman, 'The Case for Online Obscurity' (2013) 101 *California Law Review* 1.

<sup>5</sup> *supra* note 2, pp. 17, 59, and 573.

behavioural standards for its subjects. But, at the same time, it must reflect existing social reality in order to ensure that its standards remain achievable in practice. However, these twin requirements are problematic. On the one hand, if legal standards are set that are too far removed from social reality then the applicable law becomes vulnerable to the charge of being utopia because its normative demands cannot be met in practice. But, on the other hand, if law simply mirrors established social facts then it cannot achieve those purposes which law considers to be beneficial to the wider political community. Instead, it becomes a device that apologises for (or legitimises) the privileged socio-political forces at work in a given social setting.<sup>6</sup>

So, in order to avoid the charge of being either utopian or apologist, the deep structure of any valid legal argument must exhibit both normative and concrete aspects. Further, Koskenniemi claims that all legal arguments are sustained by lawyers switching between the normative and concrete components with regard to any substantive (international) law argument in a manner that is both professionally credible and consistent with the substantive outcome which they are seeking to advance.<sup>7</sup> However, in order to make credible legal arguments (international) lawyers must inhabit the centre ground of plausibility:<sup>8</sup> if their arguments veer too far to the extremes of normativity or concreteness then, professionally speaking, their arguments will lack validity and will be open to criticism.<sup>9</sup>

It follows that, as any plausible (international) legal argument involves an appeal to both normative and concrete aspects, no substantive argument has a greater claim to be valid than any other. Consequently, Koskenniemi asserts that the argumentative structure of international law renders all substantive arguments

---

<sup>6</sup> *ibid*, p. 60.

<sup>7</sup> *ibid*, pp. 570 and 572.

<sup>8</sup> *ibid*, p. 59.

<sup>9</sup> *ibid*, p. 589.

indeterminate.<sup>10</sup> In his view, international law merely validates the plausibility of the structure of legal argument used within an institutional setting. Moreover, as a decision-maker has to make a choice between competing (professionally-credible) legal arguments – a choice that is, invariably, consistent with the established institutional structural bias of the legal regime engaged by the dispute –<sup>11</sup> the actual reasons for the decision must be found elsewhere.<sup>12</sup>

Koskenniemi indicates that the argumentative structure of international law is most obvious in situations where claim-rights visibly conflict because such situations require an institutional decision-maker to engage in the conscious exercise of rights 'balancing'.<sup>13</sup> However, he maintains that rights clashes can never be resolved because any such conflict is fundamental in nature – priority must be given to one right or the other – there can be no accommodation:<sup>14</sup> only the appearance of resolution can be achieved via the articulation of the decision-maker's preference. But, as with the arguments advanced by lawyers, a decision-maker will also have to satisfy both normative and concrete aspects in order to reach a professionally-credible decision. In so doing, the decision-maker will have to harness those competing components to reach a decision which accords with the institutionally-preferred outcome. There can be no reconciliation between the normative and concrete aspects of the decision just as there can be no balancing or accommodation of clashing legal rights instead other reference points must be found in an effort to justify – ostensibly – the decision while at the same time hiding the choice that has been made by referring to other criteria

---

<sup>10</sup> *ibid*, pp. 62 and 566-573.

<sup>11</sup> *ibid*, pp. 600-615.

<sup>12</sup> *ibid*, pp. 570, 589, 591, 596 and 606-607.

<sup>13</sup> Martti Koskenniemi, 'The Effect of Rights on Political Culture' in Philip Alston (ed), *The EU and Human Rights* (OUP, 1999) pp. 107-110.

<sup>14</sup> *ibid*, p. 113.

that legitimise the outcome, such as an appeal to ‘reasonableness’, ‘equity’, or ‘proportionality’ or some other (external) consideration.<sup>15</sup>

Koskenniemi’s analysis of the structure of legal argumentation is not necessarily restricted to the discipline of international law. The structure of fundamental rights reasoning is similar to that found in international law in key respects. The rights and obligations engaged in both fields are relatively abstract in nature, and the jurisprudence of fundamental rights has become a phenomenon closely associated – but not exclusively – with supranational legal systems. More significantly, as no legal right possesses a fixed substantive content, Koskenniemi’s analysis of the structure of legal argumentation is relevant to any theoretically-informed discussion about legal rights. The next section will seek to apply Koskenniemi’s thesis to the ‘decisions’ reached in the Google Case: the Advocate-General’s Opinion and the CJEU’s judgment, in turn.

### **III. Analysing Google Spain/Google Inc., v AEPD/González**

#### **1. The Salient Legal Issues in the Google Case**

The EU Data Protection Directive requires data controllers to comply with certain fundamental principles of data protection in connection with the processing of personal data which belongs to a data subject.<sup>16</sup> In particular, Article 6 states that data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purpose; (c) adequate, relevant and not excessive; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data

---

<sup>15</sup> *supra*, note 2, pp. 570 and 589.

<sup>16</sup> Directive 95/46/EC. Article 2 defines the concepts of ‘data controller’, ‘data processing’, ‘data subject’, and ‘personal data’. See below.

which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; and (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected/processed. Article 12 confers upon data subjects the right to obtain, from a data controller, the rectification, erasure or blocking of personal data in cases where it has not been processed in conformity with the Directive's provisions. Further, Article 14 gives a data subject the right to object to the processing of his or her personal data on more general grounds.

In *Google Spain/Google Inc. v AEPD/González*, the data subject initially complained to the Spanish Data Protection Agency (AEPD) that: (i) two notices, which revealed that he had been a defaulter, must be removed from the website of the newspaper that had printed them some years before; and (ii) the internet search engine (ISE) 'Google Search' must remove links to this information from its databanks so that it could no longer be retrieved by Internet users using this ISE, in response to a name search. The AEPD rejected the complaint against the newspaper on the ground that it was published lawfully and in accordance with the instructions of the Spanish authorities; consequently, it held that the newspaper was entitled to republish this information on its (source) website. However, the AEPD upheld the data subject's complaint against Google Search. It was this decision that led to a preliminary reference being made to the CJEU. The Court found that by operating a Google Search, Google Inc., was the controller of personal data that had been unlawfully processed within the context of the activities of Google Spain.<sup>17</sup>

---

<sup>17</sup> Article 4(1)(a) provides that a data controller will be responsible for the processing of personal data belonging to a data subject if the act of data-processing takes place in the context of the activities of the controller (if it has an establishment in the EU).



## 2. Analysing the Advocate-General's Opinion in the Google Case

The legal reasoning adopted by Advocate-General Jaaskinen in his Opinion in the Google Case was consistent with the argumentative structure elucidation by Koskenniemi. Specifically, the Opinion revealed the interplay between the normative and concrete components, which despite their mutual exclusivity, are both required to formulate plausible legal arguments. It began by emphasizing the social facts in issue – the concrete practices of Internet users in the digital age – we all use ISEs to access data on the Internet these days [27-29]. Consequently, it adopted the view that we cannot all be classified as 'data controllers' for the purposes of the EU Data Protection Directive [29]. In this respect, the Advocate-General claimed that EU Data Protection law must be grounded in social reality and it must keep pace with concrete social practices. From this standpoint, it follows that if the law is interpreted in a way which does not reflect the material social facts it is at risk of being ineffective (utopian).

The Opinion pointed to other social facts which show that ISE operators should not be treated as data controllers in accordance with Article 2(d) of the Directive.<sup>18</sup> In particular, it highlighted the fact that – in response to a name search involving data available on third party servers – ISE operators cannot control the content available on source websites because technological constraints mean that they have no prior knowledge of when they are processing personal data in accordance with the terms of Article 2(b).<sup>19</sup> Consequently, the Advocate-General asserted that ISE operators are incapable of satisfying the responsibilities of a data controller as set out in Articles 6,

---

<sup>18</sup> Article 2(d) provides: 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data [...].'

<sup>19</sup> Article 2(b) provides: 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'

7, 12 and 14 of the Directive even though, on a literal construction, they might be a 'body which alone or jointly with others determines the purposes and means of the processing of personal data' [77]. As ISE operators cannot satisfy the requirements imposed on data controllers in practice, they cannot render the Directive's provisions effective and, therefore, its normative aspiration of guaranteeing complete and effective protection for data subjects is out of step with social reality.

Nevertheless, Advocate-General Jaaskinen appreciated that law cannot be sustained by social practices alone, it also needs a normative dimension in order to retain its relative autonomy from the exercise of political, economic and social power. In order to satisfy the requirements of normativity within the argumentative structure of fundamental rights, the Advocate-General made an appeal to one of the EU's normative goals, namely to develop 'information society' [36] and, specifically, the aim of securing universal access to information via the Internet [45]. To this end, he claimed that ISEs perform a vital function in facilitating access to the global stock of data available on the Internet by connecting users to the content available on source websites, without which such information would remain largely inaccessible for most Internet users. The Advocate-General also acknowledged that the normative goal of promoting the free flow of personal data – as expressed in Article 1(2) of the Directive – was problematic from the perspective of the fundamental right to privacy, as enumerated in Article 1(1). Accordingly, he recognised the need to engage in the exercise of rights balancing in cases where these fundamental rights clashed. In this regard, he referenced the fundamental rights to expression/information, as enumerated in Article 11 of the EU Charter of Fundamental Rights,<sup>20</sup> and Article 16 of

---

<sup>20</sup> Article 11(1) of the EU Charter of Fundamental Rights provides: 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.

the Charter, which concerns the right to operate a business.<sup>21</sup> He observed that such rights must be weighed against the fundamental rights to privacy and data protection, as articulated in Articles 7 and 8 of the Charter.<sup>22</sup> However, the Advocate-General noted that interferences with the right to privacy may be justified by law and that the Article 7 of the Directive, which sets out the situations in which a data controller (or third parties) may have legitimate reasons for processing of personal data.<sup>23</sup>

But, as noted above, the Advocate-General reached the conclusion that ISE operators are not data controllers for the purposes of the operation of the Directive, in relation to the search results generated by a name search. Further, he argued that unless the data quality principles have been explicitly violated or the legitimising factors, contained in Article 7, are not established, then the right to rectification, erasure or blocking (Article 12(b)) or the right to object (Article 14), cannot be engaged. The Advocate-General also made a normative appeal to the fundamental rights of freedom of expression/information at the expense of rights to informational privacy. First, he decided that the right to search for information on the Internet, using ISEs, is one of the most important ways of exercising freedom to receive information [131]. Secondly, he concluded that the Internet is an important way of exercising the freedom of expression because it enables individuals to disseminate their views by publishing material on source websites, which thereby allows them to participate in legitimate

---

<sup>21</sup> Article 16 of the Charter provides: 'The freedom to conduct a business in accordance with Union law and national laws and practices is recognised'.

<sup>22</sup> Articles 7 of the Charter provides: 'Everyone has the right to respect for his or her private and family life, home and communications'. Article 8 provides: '(1) Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'.

<sup>23</sup> Art 7(f) of the Directive provides that: 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject...'

public debate; thus, by implication, ISEs facilitate the exercise of this fundamental right [122].

In an additional manoeuvre, the Advocate-General noted that the recognition of a 'right to be forgotten' would contradict the approach adopted by the Strasbourg Court in *The Times v UK Case* where it refused to allow the alteration of digitally published material on the grounds that it would amount to the falsification of history [129].<sup>24</sup> Moreover, he pointed out that, in that case, the European Court of Human Rights reaffirmed the importance of historical accuracy in relation to archive material above all other considerations. Finally, the Advocate-General drew attention to the Strasbourg Court's observation – again in *The Times Case* – that digital newspaper archives make a substantial contribution to the preservation and accessibility of news and information to the public and that this facilitates the exercise of the fundamental right to receive information [123].<sup>25</sup> Against this background, the Advocate-General articulated his preference:

'In my opinion the fundamental right to information merits particular protection in EU law, especially in view of the ever growing tendency of authoritarian regimes elsewhere to limit access to the Internet or to censure content made accessible by it.' [121].

The Advocate-General reinforced his normative preference by expressing the view that the 'right to be forgotten' would 'would entail sacrificing pivotal rights such as freedom of expression and information' in unacceptable ways [133].

---

<sup>24</sup> *The Times Newspapers Ltd v UK (Nos. 1 and 2)* App Nos 3002/03 and 23676/03 (ECtHR, 10 March 2009).

<sup>25</sup> *Ibid.*

The Opinions of Advocate-Generals do not have the status of judgments but they are sufficiently similar to judgments for the present purposes. Accordingly, the role of an Advocate-General is comparable to that of an institutional decision-maker. Therefore, in the *Google Case*, the Advocate-General Jaaskinen's Opinion had to satisfy the normative and concrete components required for the making of plausible arguments about fundamental legal rights – thereby rendering this (non-binding) decision professionally credible at a structural level. But, according to Koskenniemi, any such decision amounts to a choice between competing normative and concrete considerations, which will inevitably reflect the structural bias of the institutional decision-maker in question. And, invariably, the decision-maker will be compelled to justify that choice by reference to criteria, which legitimize the decision but which do not directly produce it.

In the *Google Case*, the Advocate-General endeavoured to hide his choice by invoking the principle of proportionality with a view to achieving an accommodation between satisfying the Directive's objectives, on the one hand, and the development of new technological phenomena, on the other hand, 'in order to achieve a balanced and reasonable outcome' [79]. This strategy was also apparent from his conclusion that ISE operators, 'cannot in law or in fact' fulfil the obligations placed on data controllers by the 1995 Directive in relation to personal data found on source websites hosted on third-party servers. And, in support of his conclusion (choice) the Advocate-General invoked the concept of reasonableness: in his view, 'a reasonable interpretation of the Directive requires that the service provider is not generally considered as having [the responsibilities of a data controller]' [89].

### **3. Analysing the CJEU's Judgment in the Google Case**

At the outset of its judgment the CJEU drew attention to what it considered to be the principal aim of the Directive – to protect fundamental rights and, in particular, a data subject’s right to privacy with respect to the processing of personal data.<sup>26</sup> The Court addressed the question of whether an ISE operator qualifies as a data controller for the Directive’s purposes, in accordance with Article 2(d), in relation to the results generated in response to a name search. It concluded that an ISE operator must be regarded as a controller in such situations as it determines the purposes and means of processing of personal data in the context of such a search [33]. This conclusion was in keeping with the Court’s normative preference – to ensure the complete and effective protection of the rights belonging to data subjects [34]. It held that to exempt ISE operators from the responsibilities imposed on controllers would prevent data subjects from exercising the rights conferred on them by the Directive, especially their fundamental right to informational privacy [38].

The Court observed that the Directive affords a high level of protection to fundamental rights, especially the right to privacy with regard to the processing of personal data. Moreover, it noted that this fundamental right has been strengthened by Article 7 and 8 of the EU Charter [69]. The Court also observed that a data subject has a right to obtain the rectification, blocking or erasure from a controller, in respect of personal data relating to him or her, which contravenes the data quality principles, set out in the Directive. Specifically, the Court concluded that the terms of Article 6(d) are illustrative rather than exhaustive in nature. As a result, it decided that processing of personal data, which was initially lawful, may become incompatible with the Directive. This could happen where the processing was ‘no longer necessary in the

---

<sup>26</sup> Article 1(1) provides: ‘In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data’.

light of the purposes for which they were collected or processed' and especially where the data becomes 'inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed' [93].

The Court acknowledged that the legitimate interests of the controller and/or third parties must be balanced with the rights belonging to data subjects and that the provisions of Articles 7 and 8 of the Charter must be taken into consideration for the purpose of such an exercise [74]. However, in response to claims that the processing of personal data by ISE operators may be rendered legitimate pursuant to Article 7(f) of the Directive, the Court pointed to the exception identified in that provision – where a data subject's fundamental right to privacy is engaged – and its applicability in the instant case [74]. In addition, it noted that while a data subject possessed a right of erasure in certain situations, in accordance with Article 12(b), he or she could also object to the processing of personal data relating to him or her on compelling grounds relating to his or her particular situation, under Article 14. As a result, the Court observed that the right to object enabled it to take into account the specific circumstances of the data subject's situation for the purpose of balancing the rights and interests identified in Article 7(f).

It is significant that, in articulating its normative preference, the Court made no attempt to rely upon relevant social facts for the purpose of grounding its preference in social reality in a way that would reflect the structural requirements of plausible legal arguments, as articulated by Koskenniemi. A clear example of the Court's failure to establish a concrete counterpoint as a means of rendering its normative preference plausible can be seen in its conclusion that ISE operators should be classified as data controllers pursuant to the 1995 Directive, despite the fact that operators cannot exercise control over personal data published on source websites [34]. The CJEU's

view that ISE operators must be controllers because data subjects fundamental right to informational privacy must be guaranteed does not address the obvious concerns about how the responsibilities of data controllers, as expressed in the Directive, can be satisfied by ISE operators in practice. Consequently, at a structural level, the Court's reasoning seems to be unconvincing.

Further, in its judgment, the CJEU characterised the competing stakes as being between the fundamental right to privacy belonging to data subjects in relation to the processing of their personal data, as articulated in Article 1(1) of the Directive, and reinforced by the fundamental rights enshrined in Article 7 and 8 of the Charter, and: (i) the economic *interests* that ISE operators have in the processing such data; and (ii) the *interests* that Internet users possess in having access to such personal data [81]. However, the Court's articulation of the need to achieve a balance between a data subject's fundamental rights to privacy, on the one hand, and the legitimate interests of ISE operators (and Internet users in general) on the other, meant that its decision was reached far more easily than if the clash had been expressed as a contest between the fundamental rights to privacy and the fundamental rights of expression/information.

Article 7(f) of the Directive expressly recognises that controllers, and third parties, have legitimate interests in the processing personal data in certain circumstances, and subject to particular conditions, but it refrains from using the language of rights. In sharp contrast, the provision states that data subjects possess fundamental rights in this context. Notwithstanding this observation, the Court failed to take into consideration the effect of the Charter's provisions on the interests and rights engaged in data protection disputes. Evidently, the Charter transformed the legitimate interests of Internet users and data controllers, as recognised in Article 7(f),



into fundamental rights in connection with the exercise of the freedoms of expression/information, at least where such rights claims can be substantiated.<sup>27</sup> Accordingly, the Court's lack of engagement with this issue rendered its decision vulnerable to the charge that its interpretation of the applicable fundamental rights in this case was, at best, selective.

Further, at paragraph 81, the Court recognised the need for a fair balance to be reached between the interests of Internet users in having access to information and a data subject's fundamental right to privacy in relation to the processing of his or her personal data. However, by this point in the judgment, it is notable that the Court had already disregarded the purely economic interest that ISE operators may have in the processing of such personal data without any explanation as to why their 'interests' should be disregarded. But, by paragraph 97 of the judgment, the CJEU's appreciation of the need to strike a balance between these opposing rights/interests had crystallised into a clear preference. Specifically, it stated that a data subject's fundamental right to privacy: 'override[s], as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information on a search relating to the data subject's name' [97]. This shift from the acknowledgement of the need for a balance to be struck to the making of a clear choice was effected without engaging in any reasoning as to why this should necessarily be the case.

In contrast, the Advocate-General's Opinion was much more balanced, at least at a structural level. His normative priorities; assessment of the applicable fundamental rights; and conclusions were markedly different from those arrived at by the Court. His

---

<sup>27</sup> See Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain, SL, Google Inc v AEPD*' (2014) 14 *HRLR* 761, p. 769.

Opinion reflected the orthodox structure of legal argument, as identified by Koskenniemi. As a result, the arguments marshalled by the Advocate-General were sufficiently plausible in relation to the fundamental rights engaged in case for his conclusions to be professionally credible and more convincing than that offered by the Court, at least according to legal commentators.<sup>28</sup> But while the CJEU did not show that its normative preference was grounded in social reality it did use social facts as a means of justifying its normative preference, at least in one respect. It reached the conclusion that, in response to a name search, ISEs enable internet users to obtain detailed profiles of targeted individuals which would otherwise be very difficult for most users to secure [36 and 37]. It used these facts to underpin its view that the risk of ISE operators behaving in a way that interferes with a data subject's fundamental rights to informational privacy is, in fact, significantly greater than the risk posed by publishing data on source webpages alone. The significance of this standpoint will be explored in the following sections.

#### **IV. Normative Co-ordination: Balancing Fundamental Rights**

As noted above, the Advocate-General alluded to the existence of a normative conflict within the Directive.<sup>29</sup> Article 1(1) sets out the aim of protecting the fundamental privacy rights of the data subjects in relation to their personal data while Article 1(2) identifies the free-flow of personal data within the EU as the Directive's other key objective. At one level, the two normative goals collide. The apparent oppositional nature of the rights to informational privacy and freedom of expression/information in

---

<sup>28</sup> See Dominic McGoldrick, 'Developments in the Right to be Forgotten' (2013) 13 *HRLR* 761 (the Advocate-General's approach regarding the liability of ISE operators was 'sensible, balanced and pragmatic', p. 768).

<sup>29</sup> This apparent clash was previously noted in Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, 2013), pp. 19-20.

this context has been reinforced by the EU Charter of the Fundamental Rights.<sup>30</sup> The same challenge exists in relation to Article 8 ECHR (privacy)<sup>31</sup> and Article 10 ECHR (expression/information).<sup>32</sup> The countervailing nature of the rights engaged at the regional level is replicated at the international level. Both Article 19 UDHR and Article 19 ICCPR endorse the freedom of expression and to impart and receive information and they adopt the view that such fundamental freedom can only be fully exercised if they are not restricted internationally.<sup>33</sup> But Article 12 UDHR and Article 17 ICCPR also recognise fundamental rights to privacy.<sup>34</sup> Consequently, EU law, the ECHR regime and International law all attribute equal status to both the right to privacy and the rights to freedom to expression/information. They do not, in principle, condone the normative priority of one set of fundamental rights over the other. As a result, in such situations, questions of normative priority must be resolved by the institutional decision-maker on an ad-hoc, and momentary, basis for the purpose of deciding the outcome of a concrete case.

In the Google Case, it is notable that the Advocate-General and the Court adopted very different positions regarding the role played by ISEs and their significance for the progressive development of 'informational society'. In his Opinion, the Advocate-General took the view that ISE operators perform a crucial role as the

---

<sup>30</sup> Articles 7/8 versus Articles 11/16.

<sup>31</sup> Article 8 ECHR provides: (1) Everyone has the right to respect for his private and family life, his home and his correspondence; (2) There shall be no interference by a public authority with the exercise of this right [...].'

<sup>32</sup> Article 10(1) ECHR provides: Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers [...].'

<sup>33</sup> Article 19 Universal Declaration on Human Rights (UDHR) and Article 19(2) International Covenant on Civil and Political Rights (ICCPR) both provide: 'Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers [...].'

<sup>34</sup> Article 12 UDHR and Article 17 ICCPR both provide: '(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks'.

'bridge-builders' between content-developers, who upload information onto source websites, and internet users who seek to obtain such data, which includes personal data [36]. He argued that, without ISEs, the ability of internet users to secure access to such data would be too complicated [45]. In sharp contrast, the Court adopted the standpoint that ISEs heighten the risk posed to personal data belonging to data subject and that their fundamental right to privacy must be protected under EU law [37 and 38]. Thus, while the Advocate-General thought that, without ISEs, data on the internet would be too difficult to find, for most internet users, the CJEU took the opposite view: it believed that ISEs made it too easy for internet users to acquire such personal information and that fundamental informational privacy rights had to be protected as a consequence.

It can be argued that the structure of legal argumentation depends on the frame of reference selected by lawyers and institutional decision-makers for the purpose of interpreting legal rights and obligations. The CJEU's decision in the Google Case has been strongly criticised for its apparent lack of legal reasoning and its minimalist style.<sup>35</sup> It has been claimed the professional audiences are required to take 'a leap of logic' in order to comprehend the basis for the decision.<sup>36</sup> Perhaps a more serious criticism has been that its approach is out of step with the Strasbourg Court's jurisprudence in the field of fundamental rights.<sup>37</sup> These two issues will be explored below.

---

<sup>35</sup> See Christopher Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines' (2015) LSE Legal Studies Working Papers 3/2015:

<<http://ssrn.com/abstract=2496060>> accessed 13 October 2015, pp. 3, 15, and 21. This has been a long-standing criticism of the Court's judicial style. See Vlad Perju, 'Reason and Authority in the European Court of Justice' (2009) 49 VJIL 307, pp. 322-327; and Grainne de Búrca, 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?' (2013) 20 *Maastricht Journal of European and Comparative Law* 168, pp. 176-178.

<sup>36</sup> Kuner, *ibid*, 35, p. 21.

<sup>37</sup> Frantziou, *supra* note 27, pp. 772-774.

In the Google Case, the Advocate-General conflated the exercise of the freedom of expression in connection with the activity of uploading data onto source websites with the freedom to obtain information from source websites via the use of ISEs [122]. More significant is the fine, but critical, distinction between ISEs and source websites in this context. It is suggested that both the Advocate-General and commentators have overlooked the importance of this distinction, as far as the rights of data subjects are concerned. As previously noted, the Advocate-General harnessed *The Times Case* to show that the Strasbourg Court fully endorsed the need to maintain the integrity and historical accuracy of newspaper digital archives on the basis that altering such information would be tantamount to re-writing history. He also drew attention to the Strasbourg Court's acknowledgement that digital newspaper archives generally make a substantial contribution to the preservation of information and, in turn, render it accessible to the public.

McGoldrick sought to draw an analogy between the approach adopted by the Advocate-General in the Google Case and the decision reached by the Strasbourg Court in *Węgrzynowski and Smolczewski v Poland*.<sup>38</sup> In 2002, the Applicants successfully brought cases against a Polish newspaper for libel. In 2004, they instituted further legal proceedings against the newspaper alleging that, as the newspaper's website was still hosting the offending material, violations of their legal rights were ongoing. The Polish courts, however, decided that the subsequent claims were unfounded because the information had been displayed on the newspaper's source website since 2000 and as the Applicants had not complained about the digital versions in their original cases it was not possible for them to make successful claims

---

<sup>38</sup> *Węgrzynowski and Smolczewski v Poland* App no 33846/07 (ECtHR 16 July, 2013). McGoldrick was writing before the CJEU delivered its judgment in the *Google Case*.

subsequently. The Strasbourg Court also rejected their cases. It observed that while the press had to be careful not to infringe the right to privacy as expressed in Article 8 ECHR, the removal of the information in question from the newspaper's website – and thus, *prima facie*, its deletion from the internet – amounted to a disproportionate interference with the right to freedom of expression, as enumerated in Article 10.

The Strasbourg Court observed that, in principle, the rights guaranteed by Articles 8 and 10 of the European Convention deserve equal protection [56]. Nevertheless, it noted that these rights would need to be balanced in accordance with the circumstances of a particular case. The Court noted that safeguarding the freedom of the press constitutes one of the essential foundations of a democratic society and a specific manifestation of the freedom of expression. Accordingly, in its view, observance of this fundamental right was particularly important in relation to debates that involved matters of legitimate public concern but which did not infringe upon the privacy rights guaranteed by the Convention. In reaching its decision in this case the Strasbourg Court was articulating a normative preference by prioritizing the right of freedom of expression over privacy rights. But would the Court have given priority to the freedom of expression on the facts of the Google Case? In the Polish cases, the Applicants were seeking the erasure of digital information from a source website. If that information had been deleted it would, in all probability, no longer be (digitally) available. In sharp contrast, in the Google Case, the disputed information is still available, via the newspaper's source website, even after the CJEU's decision. As noted previously, in the Google Case, the CJEU took the view that ISEs present a much greater risk to the privacy rights of data subjects than that posed by source websites alone because they make personal data much more readily available to internet users. It is suggested that the failure to differentiate between the different risks

presented by source websites and ISEs for the purpose of assessing infringements of fundamental privacy rights is central to misunderstandings about the approach adopted by the CJEU in the Google Case.

Nevertheless, according to Koskenniemi's thesis regarding the requirements of plausible legal arguments, the CJEU's reasoning was flawed. It was too idealistic because it did not pay sufficient attention to the limits of legal regulation in concrete settings, at least according to the combined judgement of the professional community concerned. But although Koskenniemi appreciates that plausible legal arguments must possess both normative and concrete components it is evident that the precise mix of these components depends on the circumstances and the preferences of the institutional decision-maker in question.<sup>39</sup> Accordingly, in some cases, a decision-maker might reach a decision that manifests a higher normative quotient and a correspondingly lower concrete component (or vice versa). As long as any such legal argument (or decision) exhibits both normative and concrete dimensions then its structural plausibility will be assured.<sup>40</sup> However, it must surely be the case that if an argument is judged to be plausible by a professional community of lawyers it is inevitable that the measure of credibility will gravitate to some kind of orthodoxy,<sup>41</sup> in recognition of the fact that lawyering and judging are inherently conservative activities and given that legal reasoning is grounded in a paradigm of authority and regulated by trends discernible from past decisions. Consequently, any assessment of what is deemed to be plausible – especially if the requirement of credibility depends on

---

<sup>39</sup> Martti Koskenniemi, 'Between Commitment and Cynicism: Outline for a Theory of International Law as Practice', in M. Koskenniemi (ed), *The Politics of International Law* (Hart Publishing, 2011) 271, p. 272.

<sup>40</sup> *supra* note 2, p. 589.

<sup>41</sup> Koskenniemi acknowledges the validating role of professional audiences both regarding the integrity of particular legal arguments and decisions, *ibid*, p. 571. Professional communities also play a key role in the development of legal intuition (pp. 566-569). For analysis of the relationship between mainstream and minority viewpoints see Koskenniemi, pp. 569-570.

professional determinations as to whether the applicable law can be rendered effective in concrete settings – will tend towards conservative estimates arrived at by the members of the professional community of lawyers in issue.

This seems to be a general weakness in Koskeniemi's thesis. It is apparent that assessments about normativity and concreteness – the structural requirements of 'valid' legal arguments are also manifestations of choice at a more general level – especially in relation to the issue of whether a particular argument is sufficiently concrete (i.e. that it is capable of being followed in practice). The extent to which a legal rule or principle is effective is also a question of judgement which depends on the expectations of the observer. Clearly, collective assessments regarding plausibility are preferable to the choices of individual decision-makers (or cabals of decision-makers) but we should not overlook the fact that such assessments are being made by narrow elites that have a direct stake in the outcome of decisions, as they are repeat-players in this form of professional activity.<sup>42</sup>

Viewpoints regarding practical issues, including the viability of notice and take-down procedures (e.g. the acceptable scale of requests made by aggrieved data subjects),<sup>43</sup> and whether ISE operators, as non-State actors, should bear the burden of assessments about fundamental human rights – will vary.<sup>44</sup> Some community members may privilege expression/information rights over privacy claims and some will adopt hard-nosed assessments about the extent to which personal data can ever

---

<sup>42</sup> The role of a community of professional interpreters is also central to Dworkin's scholarship. See Ronald Dworkin, *Law's Empire* (Hart Publishing, 1986). Also see Ian Johnstone, 'Security Council Deliberations: The Power of the Better Argument' (2003) 14 *European Journal of International Law* 437.

<sup>43</sup> For figures showing the challenge for ISE operators generated in the immediate aftermath of the Google decision see House of Lords European Union Committee, 'EU Data Protection Law: "A Right to be Forgotten"?' , Second Report of Session 2014-15, HL Paper 40, 30 July 2014 at pp. 14-15.

<sup>44</sup> See Bert-Japp Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice' (2011) 8(3) *Scripted* 229; and Frantziou, *supra* note 27, pp. 769-771.



be forgotten once it has been rendered accessible online,<sup>45</sup> while some will be attracted to the redemptive value of 'clean-slates'.<sup>46</sup> However, in the end, Koskenniemi's thesis assumes that plausibility will depend on the standpoint adopted by the critical mass of members of the professional community concerned.

But the question that must be asked is whether such matters should be determined by the professional sensibilities of (invested) lawyers at all? Perhaps we should think again about the structural requirements of legal arguments. Ground-breaking legal arguments – ones that are truly radical – would struggle to satisfy both normative and concrete requirements of plausible legal arguments. This observation follows from Koskenniemi's view that as legal rules and principles do not possess an inherent substantive content, the credibility of any legal arguments can only be assessed by reference to the way in which prior, analogous, arguments have been determined by professional communities of lawyers. However, while all radical legal arguments are at risk of being considered to be implausible (especially as far as the concrete axis is concerned) the rights clashes apparent in the Google case illuminate the challenges presented by structural implausibility brilliantly.

In any event, whether the concrete dimension can be satisfied might depend on the extent to which the decision-maker is aware of the structural requirements of legal reasoning. It has been observed that the CJEU is relatively inexperienced in dealing cases involving the balancing of fundamental human rights.<sup>47</sup> In this respect, it could be said that the approach the Court adopted in the Google Case is an example, par excellence, of its claimed inability to deliver plausible decisions in this field in sharp

---

<sup>45</sup> For a particularly negative assessment of the chances of privacy rights being successfully protected in digital setting see the 2014 House of Lords Report (above). Also see Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 250.

<sup>46</sup> See Koops, *supra* note 44, pp. 250-252 and 254-256.

<sup>47</sup> See de Búrca, *supra* note 35, p. 170.

contrast to the vastly more experienced (successful?) European Court of Human Rights. However, the danger with this criticism – the need to satisfy the expectations of observers with vested interests in the outcome – is that, in so doing, the Court may overlook the legitimate expectations of the wider political community in issue, which may differ from those of the professional audience concerned. Another risk is that requiring lawyers to undertake certain argumentative manoeuvres for the sake of credibility reduces legal reasoning to a hollow style.<sup>48</sup> What should the CJEU have done in order to satisfy the concrete requirements for its decision to be plausible in the Google decision? Would it have been sufficient if it had provided generic guidance on how data subjects could exercise their rights in appropriate cases and how ISE operators could satisfy their responsibilities as data controllers in such situations? If bland general advice was all that was required in order to make the decision legitimate then the CJEU could have adjusted its reasoning to satisfy the orthodox plausibility requirements, and thus the needs of its professional audience, without fundamentally changing the approach it adopted in the case.

## **V. Achieving Normative Co-ordination in Concrete Cases**

### **1. The Symbiotic Relationship between Privacy Rights and Expression Rights**

Kuner points to the existence of a distinction between the fields of privacy law and Data Protection law.<sup>49</sup> He indicates that privacy rights afford an individual protection against intrusions into his or her private sphere whereas Data Protection law regulates personal data belonging to identifiable natural persons, which may be accessible in

---

<sup>48</sup> Of course, this is the very point that Koskenniemi is trying to make.

<sup>49</sup> Kuner, *supra* note 29, pp. 18-20.

the public domain. The view that privacy rights are essentially negative and defensive in nature is a long-standing one. In contrast, the notion of informational privacy is broader in scope: it provides that 'an individual has the right to control the extent to which personal information is disseminated to other people'.<sup>50</sup> But while the idea of informational privacy is expressed in terms of control it does not find its normative origins in the proprietary paradigm (it is not sustained by the concept of ownership or use rights).<sup>51</sup> Instead, it is best captured by the fuzzy concept of informational self-determination. But although the notions of privacy and data protection are distinct they are not mutually exclusive.<sup>52</sup> As Kuner explains, in the digital age, personal data (i.e., data that renders a given individual identifiable) may be viewed as a proxy for the individual concerned in digital settings.<sup>53</sup> Therefore, an individual's personal data could be viewed as a manifestation of his or her personality in such situations. The implications concerning the possession and exercise of personality rights in the context of Data Protection law have not been fully worked out but this way of conceptualizing the nature and purpose of Data Protection law has the advantage of highlighting the close ties between privacy rights and data protection at a normative level.

It is also worth identifying the aims of privacy rights in an effort to make the shared normative framework more transparent for the purpose of analysis. As Cohen argues, negative conceptions of privacy ignore the extent to which identity is socially constructed and that a protected sphere provides the space for experimentation, the exchange of ideas and self-development.<sup>54</sup> The defining feature of the private sphere

---

<sup>50</sup> Ian Lloyd, *Informational Technology Law* (7<sup>th</sup> edn, OUP, 2014), p.17.

<sup>51</sup> See Koops, *supra* note 44, pp. 246-247.

<sup>52</sup> See Valsamis Mitsilegas, 'The Transformation of Privacy in an Era of Pre-emptive Surveillance' (2015) 20 *Tilburg Law Review* 35, pp. 52-3.

<sup>53</sup> Kuner, *supra* note 29, pp. 123-125.

<sup>54</sup> Julie Cohen 'What Privacy is For' (2013) 125 *HLR* 1904, pp.1910 and 1920.

is that it restricts – legitimately – the extent to which the State, and other actors, can interfere with processes of self-making.<sup>55</sup> Cohen asserts that such freedom is vital to the fostering of innovation which is a prerequisite for the achievement for progress and human flourishing at a societal level as well as being necessary for the maintenance of an informed and reflective citizenship.<sup>56</sup> In sharp contrast, by promoting techniques of mass surveillance, data interception, collection and retention, States and powerful private actors reduce the capacity for individuals to engage fully in those processes of self-development which sustain dynamic political and intellectual cultures.<sup>57</sup>

The idea that privacy rights create the conditions of possibility for the exercise of the freedom of expression has also been acknowledged by a number of institutional actors. For example, in a Report published in 2013, the Special Rapporteur on Opinion and Expression admitted that the right to privacy constitutes a prerequisite for the realisation of the right to freedom of expression. In particular, he endorsed the view that privacy incursions have the effect of limiting the scope for individual self-development and the exchange of ideas which are essential to the exercise of this fundamental right in meaningful ways.<sup>58</sup> Further, he stated that without the existence of a protected sphere in which individuals can engage in processes of autonomous development and social interaction, without interference, the freedom of expression would be significantly undermined, as the existence of such a fundamental freedom presupposes that individuals have the opportunity to develop themselves to the extent that they have opinions of their own.<sup>59</sup> The Special Rapporteur Report significantly informed the position adopted by the UN General Assembly with regard to its

---

<sup>55</sup> *ibid*, p. 1911.

<sup>56</sup> *ibid*, pp. 1905-1906, 1911-1912 and 1918-1927.

<sup>57</sup> *ibid*, at 1917.

<sup>58</sup> UN 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', 17 April, 2013, UN DOC A/HRC/23/40, [24].

<sup>59</sup> *ibid*, at [27].

resolution on the 'Right to Privacy in the Digital Age'<sup>60</sup>. Specifically, it harnessed Article 12 UDHR and Article 17 ICCPR, which together set out the parameters of the right to privacy in international law, before pointing out that: 'the exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and it is one of the foundations of a democratic society'.

## **2. Establishing Normative Priority: The Technique of Lex Specialis**

One plausible way of resolving the normative conflicts between privacy rights and expression/information rights in the light of their established interrelationship is to harness the interpretative technique of *lex specialis*. The relationship between *lex specialis* and *lex generalis* was considered in detail by the International Law Commission (ILC) in its 2006 Study on the Fragmentation of International Law.<sup>61</sup> The Study observed that where two norms are applicable in a particular case, and neither of which have formal hierarchical priority, the more specific norm should be applied. It concluded that the interpretative technique of giving greater weight to the more specific norm can be justified on the grounds that it is able to resolve the normative challenge in issue more effectively because its specificity means that it has a greater chance of anticipating the challenges encountered in a concrete dispute. The Report also indicated that the more specific norm acts as a better guide to the intentions of the parties (or a legislature) in such situations.<sup>62</sup> It should be noted that there may be no conflict between the two norms in question instead there may simply be one provision which is regarded as having a greater degree of applicability and that is the one which

---

<sup>60</sup> UN General Assembly Resolution 68/167, 18 December 2013.

<sup>61</sup> International Law Commission, 'Report on the Fragmentation of International Law' 13 April, 2006. UN DOC A/CN.4/L.682.

<sup>62</sup> *ibid*, at [59].

the Court deems to be applicable on the facts. This approach is not necessarily problematic for the *lex specialis* technique since it does not presuppose the existence of a genuine normative conflict rather it is an interpretative technique that is required to resolve questions of normative priority. It may well be that the more specific norms simply represents an elaboration of the more general norm in a given situation and that normative harmony exists rather than conflict. Nevertheless, the question of which norm constitutes the governing norm in relation to a concrete case must still be decided.

Further, the 2006 Report appreciated that the two norms in issue may be contained in a single instrument and it gives the ECHR as an example of such a phenomenon. For instance, in *Djavit An v Turkey*, the Strasbourg Court decided that Article 11 ECHR (freedom of assembly) could be considered to be the *lex specialis* while Article 10 (freedom of expression) constituted the *lex generalis* for the purpose of determining which of the Convention rights had normative priority in the context of the dispute in question.<sup>63</sup> In the Court's own words:

'[T]he issues of freedom of expression cannot in the present case be separated from that of freedom of assembly. The protection of personal opinions, secured by Article 10 of the Convention, is one of the objectives of the freedom of peaceful assembly as enshrined in Article 11 of the Convention [...] Thus [...] the Court considers that Article 11 of the Convention takes precedence as the *lex specialis* for assemblies, so that it is unnecessary to examine the issue

---

<sup>63</sup> *Djavit An v Turkey* App no 20652/92 (20 February 2003) also at [73] of the ILC Report, *ibid*.

under Article 10 separately. The Court will, however, have regard to Article 10 when examining and interpreting Article 11'.<sup>64</sup>

The ILC's Report endorsed the view that *lex specialis* amounts to an interpretative technique which is capable of resolving concrete disputes in a systematic manner.<sup>65</sup> It is suggested that harnessing such an interpretative mechanism would enhance the transparency of processes of legal reasoning undertaken by institutional decision-makers. Although this technique cannot transform the structure of legal argumentation at a fundamental level it could improve decision-making processes significantly. In particular, it should prompt decision-makers to articulate their understanding of the relationship between countervailing rights in ways that render their choices visible. In the present context, the *lex specialis* device could play an important role in recalibrating the relationship between privacy rights and expression rights in cases where the rights of data subjects are disproportionately affected in online situations by ensuring that decision-makers address the full implications of their choices for affected stakeholders in a transparent manner.

The use of such an interpretative technique could also facilitate the development of an entitlement to data obscurity. Hartzog and Stutzman have suggested that courts (and legislators) must do more to recognise the ways in which individuals harness obscurity in digital settings in order to gauge the applicability of privacy rights in such situations.<sup>66</sup> They have argued that courts should use contextually-sensitive means to restrict access to data (along a sliding-scale) where

---

<sup>64</sup> *Djavit An* *ibid*, at [39] (quoted in the ILC's Report, *ibid*, at [93]).

<sup>65</sup> However, Koskeniemi – who was responsible for finalizing the ILC's Report – used this opportunity to reiterate his structural thesis by observing that *lex specialis* provides an institutional decision-maker with the means to make an ostensibly legitimate choice between competing legal arguments (e.g. see ILC's Report, *ibid*, at [106]) .

<sup>66</sup> Hartzog and Stutzman, *supra* note 4.

individuals have a legitimate expectation that their personal data should be treated as obscure – and thus eligible for privacy protection – rather than be forced to make difficult (binary) decisions about whether information should be deemed either digitally accessible or inaccessible. It is clear that such a methodology would fit very well with the approach adopted by the CJEU in the Google Case although it would clearly require development and elaboration before it could become a pragmatic tool for resolving data protection disputes in concrete cases.

## **VI. Conclusion**

In the Google Case, the Advocate-General took the view that the accessibility of considerable sources of information to internet users, via ISEs, is vital to the success of the 'information society'. Consequently, he concluded that, if ISE operators did not perform this important connecting role, then information society would be impoverished. In articulating this standpoint the Advocate-General presented the goal of (near) full access to information available on the internet as a clear benefit to this 'society'. But if full access is perceived as a good, in and of itself, then virtually any restriction imposed on access to data on the internet would amount to a form of suppression and an unjustified restriction on internet users' freedom to receive information. From the Advocate-General's perspective, the freedom of information constitutes a broad right to be enjoyed by everyone, to the fullest extent possible. As ISEs render information published on source websites easily accessible the removal of links to sources websites is problematic as most internet users do not possess the research or technical skills to access data directly from the source websites. In contrast, the CJEU did not view the rights to information and expression in the same – maximalist – way. It was satisfied if the (offending) information is still accessible but



restricted to the source website in question – an approach which appears to support the idea of a right to obscurity.

Kuner claimed that the approach adopted by the Court, in the Google Case, indicates it thinks that the risks posed by the internet outweigh its benefits.<sup>67</sup> However, there is nothing in the CJEU's judgment which shows that it considers the internet to be problematic per se. Even if one could point to passages that could be interpreted as supporting the conclusion that the Court is of the view that different levels of legal protection are required in online and offline situations such an assessment is nothing new. For instance, in the Polish Cases, the Strasbourg Court showed some awareness of the additional risks posed by the internet for those fundamental rights guaranteed by the European Convention.<sup>68</sup> And even scholars who have expressed support for the approach adopted by the Advocate-General in the Google Case understand that developments regarding the so-called right to be forgotten, 'mark the not insignificant reassertion that privacy is seen as something having a continued societal and instrumental value that must be given a degree of protection'.<sup>69</sup> It is clear that, in the Google case, the Court was responding to a need to recalibrate the relationship between the fundamental privacy rights and expression/information rights in online settings. More theoretical work needs to be done in this area given the complex and problematic nature of the right to erasure. However, it is evident that the normative contours of some kind right to data obscurity are discernible and that the Court's (under-theorised) recognition of the significance of informational privacy rights in the digital age represents an important step in the right direction.

---

<sup>67</sup> Kuner, *supra* note 35, p. 21.

<sup>68</sup> See *Węgrzynowski and Smolczewski v Poland*, *supra* note 38, at [57].

<sup>69</sup> McGoldrick, *supra* note 28, at 775.