DIGITAL MEMORY & INFORMATIONAL PRIVACY: REFLECTING ON THE EU's 'RIGHT TO BE FORGOTTEN'

Ujwala Uppaluri

Research Fellow

CCG Working Paper Series
(2014-15)

I. INTRODUCTION, OUTLINE & SCOPE

As part of a complete overhaul of European Union regulations concerning Internet information stored electronically, a proposal for a 'General Data Regulation'[1] (*hereinafter* "the Regulation") was been passed by the European Parliament.[2] The Regulation is intended to be read with the existing law as to data protection in the European Union, specifically the Data Protection Directive[3] (*hereinafter* "the 1995 Directive") and the E-Privacy Directive.[4] *Inter alia*, this legislative attempt made reference at its Article 17 to a data subject's right to be forgotten. The proposal sparked a staggering amount of debate[5] around the consequences of the grant of such a right, with particular resistance arising out of the potential burden that such a right could impose on intermediaries online.

Since that proposal was made, a 'right to be forgotten' has been articulated by the Court of Justice of the Eurpoean Union (CJEU).[6] It used existing data protection law, including portions

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012) 11 final.

[2] *See* Viviane Reding, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age* (January 24, 2012) (Transcript of Speech) *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26.

[3] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

[5] *See, for e.g.,* Claire Davenport, *'Right to be Forgotten': Online Privacy Legislation proposed by European Commission* (January 25, 2012) *available at* http://www.huffingtonpost.com/2012/01/25/right-to-be-forgotten-online-privacy_n_1230371.html; Peter Bright, *Europe proposes a "right to be forgotten"*, ARS TECHNICA *available at* http://arstechnica.com/tech-policy/news/2012/01/eu-proposes-a-right-to-be-forgotten.ars; Suzanne Daley, *On Its Own, Europe Backs Web Privacy Fights* (August 9, 2011), THE NEW YORK TIMES *available at* http://www.nytimes.com/2011/08/10/world/europe/10spain.html?pagewanted=all ; Jane Yakowitz, *More Bad Ideas from the EU* (January 25, 2012), FORBES MAGAZINE *available at* http://www.forbes.com/sites/kashmirhill/2012/01/25/more-bad-ideas-from-the-e-u/; John Hendel, *Why Journalists Shouldn't Fear Europe's 'Right to be Forgotten'* (January 25, 2012) *available at* http://www.theatlantic.com/technology/archive/2012/01/why-journalists-shouldnt-fear-europes-right-to-be-forgotten/251955/; Emma Barnet, *We must fight for a right to be forgotten online* (January 26, 2012) http://www.telegraph.co.uk/technology/social-media/9041302/We-must-fight-for-the-right-to-be-forgotten-online.html.

[6] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, Case No. C-131/12 (CJEU).

of the Data Protection Directive of 1995[7] to read in a right to be forgotten for data subjects, and a corresponding obligation to takedown for intermediaries, and search engines in particular. As with Article 17, *Costeja* has been the subject of a great deal of criticism.

This article will cursorily consider the history and nature of machine memory, make the case for digital forgetting, describe the legal and conceptual sources of the right to be forgotten, and evaluate Article 17 and the CJEU's iteration of the right, with the intention of contributing to this debate. Particular emphasis will be placed, in the process, on informational privacy on the fundamentals of data protection and on the many concerns that the present iteration of the right raises not only for Europe but for data protection law generally.

At the outset, the following normative assumptions will guide and constrain the scope of this article's appraisal of the right to be forgotten. *First*, it will take as given the need to regulate toward greater and more meaningful privacy for Internet users (in the sense of informational autonomy and informational control for data subjects, at least presumptively) as a favourable regulatory end. *Second*, it will endorse what has been termed the "dignity" model of regulating toward privacy that is prevalent in the EU, in contrast to the "liberty" model that is applied in the United States, although it will make reference to information practices in that jurisdiction.[8] *Third*, it will operate on the assumption that users of the Internet, rather than data controllers (especially given their commercial nature, but also otherwise), must be the ultimate beneficiaries of regulatory interventions, whether it is in respect of the assertion of their privacy rights or the enhancement of their speech capacities.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281 , 23/11/1995 P. 0031 – 0050*.

[8] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151 (2004).

II. (THE RIGHT TO) INFORMATIONAL PRIVACY: CONTENT & SCOPE

Some Theoretical Markers

Privacy has been a difficult notion to define with precision.[9] The right to privacy is understood to be fundamental to human dignity[10], notwithstanding the debates around the substantive content of the latter term.[11] For the purposes of this article's argument, it is of note that privacy does not mean the complete absence or unavailability of information about the rightsholder in the public domain, rather, it sees the data subject as an autonomous moral agent and requires that he or she be able to *control* in real and effective terms information that relates to her.[12] The right to privacy includes also the data subject's right to his or her identity, and specifically the rights to self-definition and presumptive control over personal information are intrinsic. Privacy for the present purposes must also be understood as contextual integrity.[13] In pragmatic terms, it is useful to view informational as an exercise in balancing power relations between data subject and data controller, and privacy protections as an attempt to prevent the latter class' "dehumanization"[14], to maximize their participation[15] and capacity for free choice.[16]

The need for specifically regulating how those transacting in information relating to natural persons is manifest: the power imbalance between large data processors, both governmental and commercial, and individual data subjects in an unregulated landscape would a wide margin for

---

[9] *See, e.g.,* LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 126 (2002); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1130 (2002); Ken Gormley, *One Hundred Years of Privacy*, WIS. L. REV. 1335 (1992); Raymond Wacks, *The Poverty of "Privacy"*, 96 L. Q. REV. 73, 76-77 (1980).

[10] *See, e.g.,*Edwatd J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964).

[11] *See* Tarunabh Khaitan, *Dignity as an Expressive Norm: Neither Vacuous Nor a Panacea*, 32 OXFORD JOURNAL OF LEGAL STUDIES 1 (2012); Christopher McCrudden, *Human Dignity and Judicial Interpretation of Human Rights*, 19 EUR. J. INT'L L. 655 (2008) .

[12] Charles Fried, *Privacy*, 77 YALE L. REV. 475, 482 (1968).

[13] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

[14] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1398 (2000).

[15] *Id.*

[16] PAUL M. SCHWARTZ AND JOEL R. REIDENBERG, DATA PRIVACY LAW 39 (1996).

unchecked harms to individuals' more broadly protected rights to privacy. Data protection law attempts to serve as this specific regulation.

Cornerstones of Data Protection Law

Data protection law is based in ensuring compliance with a core set of principles that govern the manner in which units of information ('data'), particularly personal and sensitive data, are treated at each stage of processing. There are several principles that have been identified in this context, with the OECD Guidelines[17], the United States' Federal Trade Commission's Fair Information Practices[18] and the 1995 Directive[19] containing lists of principles generally accepted as the standard. For the purposes of the argument in this article, the following principles are of particular relevance:

First, all inventories of data protection principles emphasize consent, and especially prior and informed consent. For instance, it is recognized as a necessary element at each of Solove's[20] stages of data processing. This principle makes it the duty of potential data processors to obtain users' consent and so acknowledges informational autonomy as an element of data subjects' right of privacy. It is also a recognition that control of personal information, understood in the reductionist sense (of information actually associated with the individual) as in the United States if not in the expansionist sense as in the EU (*i.e.*, information which can be linked to an individual, in addition to information that has already been linked to her),[21] must vest in the subject of the information.

The consent principle can be read along with the principle of openness, which requires data controllers to be transparent and consistent in their practices and policies relating to the treatment of personal data. Ideally, all technologies having the potential to affect the privacy of the

[17] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. *See also* UN General Assembly, *Guidelines for the regulation of computerized personal data files*, UN Doc. No. A/RES/45/95 *available at* http://daccess-ods.un.org/TMP/4703397.45283127.html.

[18] Federal Trade Commisssion, *Fair Information Practice Principles available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[19] *Supra*, n.3.

[20] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2005-2006).

[21] *See* Paul M. Schwartz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N. Y. U. L. REV. 1814 (2011).

individuals to whom the information relates must be architected so that privacy is the default and consent is required to process, use or disclose of any of the data concerning them. In other words, consent must be explicitly obtained, and users must choose to opt-in to technologies which may have privacy-invasive consequences for their information after being informed in accessible terms of the nature of the technology or service. In addition, where practices as to privacy change, as when social networking services alter their privacy policies, consent cannot be deemed to exist and should have to be obtained afresh. The argument, overall, is that the consent principle is best actualized in systems in which privacy is the default and users must opt-in to privacy-invasive services or elements, rather than opt-out.[22]

Second, the principle of purpose specification is an important cornerstone, and also one that will bear on the how a 'right to be forgotten' would be constructed.[23] This principle requires that data be collected and used only for the purposes that have been specified prior to the collection or use, as the case may be. This must be read with the use limitation principle which provides that personal data cannot be processed, disclosed or otherwise used for purposes unspecified at the time that the data was collected, with the exceptions that where the explicit and informed consent of the data subject has been obtained or where the use is in accordance with and under the authority of law, the use will be lawful.

Third, there is the security safeguards principle, which requires *inter alia* that all reasonable measures be taken to ensure that personal data, once collected, is secured, and that the risk of unauthorized access, use or disclosure of the data is minimized. *Finally*, data protection law is based on the accountability principle, *i.e.*, that the data controller must be held accountable for ensuring that all of the other principles are satisfactorily operationalised.

Several further principles flow as corollaries to the above. The rule as to purpose specification can be extrapolated to yield the principle that only as much data as is necessary for the purpose be collected, used and retained (data minimization). Importantly, the rules as to purpose specification and consent also imply that data be retained for only as long as is strictly required

[22] *But see* Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 67-8; Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 SCRIPTed 155, 155 (2010), *available at* http://www.law.ed.ac.uk/ahrc/scripted/vol7-1/lundblad.asp .

[23] *See* n.13, *supra*. (Purpose specification is a clear codification of this element of privacy).

to achieve the specified purpose. Upon the fulfillment of the purpose, mandating that the data be securely disposed of, whether by deletion or erasure or by anonymizing or otherwise, is the logical *sequitur*, if informational control must continue to vest in the data subject and the hazards of data breaches and unauthorized aggregation and/or mining are to be prevent.

To the degree that the right to be forgotten is an embodiment of these principles (and the EC opines that it is)[24], one could argue that it is a necessary element of a holistic scheme of data protection.[25]

Informational Privacy in EU Law: Sources and Countervailing Interests

At the first level, constitutional guarantees of privacy exist. A broad right to privacy is guaranteed across the European Union at Article 8 of the European Convention of Human Rights, which provides that everyone has a right to respect for private and family life. The European Court of Human Rights has been able to read data protection principles into Article 8. Notably, it has recognized that the fact of storage of personal data can, on its own, raise privacy concerns in terms of Article 8, and that data subjects ordinarily have the right to access information held about them and request rectification of incorrect records.[26] It has also recognized that data aggregation would adversely affect privacy, and that the privacy concern could arise irrespective of whether the individual bits of information were public or voluntarily disclosed, because information once compiled was more than the sum of individual bits of information[27]

However, it is also of note that the Convention protects against *state* interferences with privacy, and envisions that the right be applied vertically, that is as against state action or inaction, as the case may be. It is possible for some third-party violations of the right to privacy to allow a complainant to raise a Convention issue under Article 8, as the state's obligations under Article 8

[24] EC Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM (2010) 609, 8.
[25] Benjamin J. Keele, *Privacy by Deletion: The Need for a Global Data Deletion Principle*, (2009) 16 IND. J. GLOBAL LEG. STUD. 363, 375-79.
[26] *Amann v. Switzerland*, Application no. 27798/95 (ECtHR, 16 February 2000); *Kopp v. Switzerland* Application no. 23224/94 (ECtHR, 25 March 1998).
[27] *Rotaru v. Romania*, Application no. 28341/95 (ECtHR, 4 May 2000).

has been read by the European Court of Human Rights as also including positive obligations,[28] that require the state to act to preserve privacy, in addition to its primary negative obligation to desist from interfering unlawfully with its citizens' private lives.

More specifically, with the coming into force of the Lisbon Treaty,[29] the EU has given full legal effect to statements of a right to data protection. Article 16 (1) of Treaty on the Functioning of the European Union[30] explicitly provides that everyone has a right to protection of personal data concerning them as does Article 8 (1) of the Charter of Fundamental Rights, in addition to a right to privacy.[31]

Even as the EU explicitly grants data subjects the right to data protection, the Convention clearly makes out that an Article 8 issue arises only when a given instance of an interference with privacy is unreasonable, while the European Court of Justice has recognized that the right to privacy is not absolute[32]. The new Regulation has itself recognized that regulating towards greater privacy for data subjects can implicate other rights.[33] It identifies these countervailing interests as being the freedom speech and expression, the freedom to conduct a business, the right to property (and especially to intellectual property) and the rights of the child, *inter alia*.[34]

All of the above interests are affected by a potential right to be forgotten.

III. MEMORY AND FORGETTING IN DIGITAL MEDIA

Mapping the Nature and Characteristics of Digital Memory: Two Seminal Ideas

The foremost instance of the idea of replicating and then augmenting human memory through machines came from Vannevar Bush, an American engineer, who posited the idea of the of the

[28] *Gaskin v. The United Kingdom*, (1989) 12 EHRR 36, §§ 42-49
[29] TREATY OF LISBON AMENDING THE TREATY ON EUROPEAN UNION AND THE TREATY ESTABLISHING THE EUROPEAN COMMUNITY.
[30] TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION (2010/C83/47).
[31] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2010/C 83/02).
[32] *Volker und Markus Schecke and Eifert*, Joined Cases C-92/09 and C-93/09, [2010] ECR I-0000 (ECJ, 9 November 2010).
[33] *Supra,* n.1 at ¶ 3.3, 7.
[34] *Id.*

first mechanized system of remembering in an influential article in *The Atlantic*[35] in 1945. In it, he described his "memex", a device to which the fundamentals of the present-day World Wide Web are broadly analogous, in the following terms: "*A memex is a device in which an individual stores all his books, records, and communications, and which is mechanized so that it may be consulted with exceeding speed and flexibility. It is an enlarged intimate supplement to [human] memory.*"[36] To these capabilities, he added the notion of "associative indexing",[37] to mimic the organic nature of human memory.

Bush's attraction to the idea of the memex is illustrative of the fundamental characteristics of machine memory that will bear on the argument here. Where human memory is transient and indeterminate, machined memories could achieve an unprecedented permanence. Digital memory goes even further than the analogue model that Bush posited: it does not decay with time or use, as human and analog memories would (the "noise problem")[38]. Even more importantly, machines have meant a convergence of mediums: records varying by size, format and medium (audio, video, text, images, or combinations of these) could be collected, stored, retrieved and processed by means of the same digital medium. In addition, information held extrinsically to human memory was potentially accessible, in the same objective terms and form, to more than one recipient. Further, where human memory is neither perfect nor infinite, machine memory is unlimited – data storage costs have made it possible for a potentially infinite amount of information to be held at once.

By 1960, the idea of supporting human intelligence with machine (artificial) intelligence had been articulated by J.C.R. Licklider in his seminal paper "Man-Machine Symbiosis" in the following terms:

"*The hope is that, in not too many years, human brains and computing machines will be coupled together very tightly, and that the resulting partnership will think as no human brain has ever*

---

[35] Vannevar Bush, *As We May Think*, THE ATLANTIC, July 1945 *available at* http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/3881/.
[36] *Id.,* at § 6.
[37] *Supra,* n. 35 at § 7.
[38] *See* n. 41, *infra* at 57.

thought and process data in a way not approached by the information-handling machines we know today."[39]

Licklider's work helped found the canon of theoretical work on which GUIs and the (remembering) Internet of today are based. He speculated, in essence, that machines would maximize efficiency in collecting and handling information and have, in the result, transformative and empowering consequences for data subjects. It is possible for proponents of the right to be forgotten to argue that the Internet in its current form has resulted in the disappointment of those hopes. In the context of personal information (broadly understood), it has had the effect of overtaking human memory and providing access to information in ways that distort the initial intent behind the disclosure by data subjects, such that the ultimate result is the dissolution of informational control and the disempowerment of the human *vis à vis* the digital information system, in terms entirely antithetical to Licklider's pardigm.

"Total Recall"[40] versus the "Virtues of Forgetting"[41]

Two more recent, and less theoretical, accounts of the benefits and concerns arising from digital remembering describe the benefits and problems that arise as a result of the embedding of the phenomenon. In his book by the same name, Gordon Bell describes his experiment in life-logging and advocates emphatically for the transformative potential of the capacity for "total recall". He characterizes this capacity for remembering as the "e-memory revolution", and details benefits to data subjects in several fields – the workplace,[42] healthcare,[43] leisure[44] and education – even as he commendably recognizes the problems of establishing a fair system of obtaining consent and of the problem of keeping data relating to separate contexts separate ("data entanglement"). However, he appears to dismiss the problem of surveillance that such data banks

---

[39] J.C.R. Licklider, *Man-Computer Symbiosis*, IRE Transactions on Human Factors in Electronics, Volume HFE-1, March 1960, p. 4-11 *available at* http://groups.csail.mit.edu/medg/people/psz/Licklider.html. *See also* Dr. Douglas C. Englebart, *Augmenting Human Intellect: A Conceptual Framework*, Summary Report AFOSR-3233, Stanford Research Institute, October 1962 *available at* http://www.dougengelbart.org/pubs/augment-3906.html,

[40] GORDON BELL AND JIM GEMMELL, TOTAL RECALL: HOW THE E-MEMORY REVOLUTION WILL CHANGE EVERYTHING (2009).

[41] VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2011).

[42] *Id.,* at 73, 90.

[43] *Supra*, n.41 at 94.

[44] *Supra*, n.41 at 142.

become amenable to on the grounds that the data is not being collected by or at the behest of the state.[45]

On the other hand, Viktor Mayer-Schönberger fears that the result of comprehensive and perfect remembering would create a digital version of the Benthamite and Foucauldian panopticons.[46] Mayer-Schönberger problematizes this phenomenon on two counts: power and time. Perfect remembering disempowers data subjects while simultaneously empowering data collectors. The fact that all information is comprehensive, durable and potentially universally accessible means that data subjects who apprehend this will harbor tendencies toward silence rather than speech. With regard to time, Mayer-Schönberger argues that the capacity of forgetting allows for individuals and collectives to overcome particularizations, and filter and sift information with the result of more effective decision-making. He sees memory and forgetting as complementary processes, and argues that it is intrinsic to allowing for one to freely shape identity and evolve. This notion of the value of forgetting, and of the need for digital forgetting has been echoed elsewhere as well.[47]

The two accounts present valuable counterpoints to each other, but it must be recognized that they are not inconsistent or incompatible. Both are predicated, explicitly in the case of Mayer-Schönberger and implicitly in the case of Bell, on the consent, active and informed, of the data subject to allow capture of information, at the threshold itself.

The Internet, being a network constituted of a machine memory that interfaces with humans, raises particularly important considerations, given its capacity for public, perfect and often unalterable remembering. It is apparent the new Regulation is an attempt to manage the consequences of this capacity. It is arguable that the right to be forgotten is an attempt to regulate away from the harms apprehended by Mayer-Schönberger.

---

[45] *Supra*, n. 41 at 14.

[46] *Supra*, n. 41 at 11.

[47] Jean-François Blanchette and Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 18 THE INFORMATION SOCIETY, 33 (2002); Martin Dodge and Rob Kitchin, *The Ethics of Forgetting in an Age of Pervasive Computing*, UCL CASA WORKING PAPER SERIES, *available at* http://www.casa.ucl.ac.uk/working_papers/paper92.pdf; Liam J. Bannon, *Forgetting as a Feature, Not a Bug: The Duality of Memory and Implications for Ubiquitous computing*, CODESIGN, VOL. 2, NO. 1, MARCH 2006, 3 – 15; The Economist, *Relearning to forget* (January 27, 2012) http://www.economist.com/node/21543561.

IV. ARTICLE 17

The right to be forgotten is not an unprecedented notion in the EU's scheme of data protection.[48] Article 12 (b) of the 1995 Directive already provides for a limited right to data erasure, where data is incomplete or inaccurate. Jurisdictions in the EU have more direct rights to "oblivion" (specifically the French "*droit à l'oubli*"[49] and the Italian "*diritto al' oblio*"[50]). These originated as rights to silence, particularly in criminal law where an accused was later exonerated, or where convicts who had served their time were rehabilitated.

The particular terms of Article 17 of the proposed law grant EU data subjects the right to demand of data controllers, on pain of penalties in fines, the deletion of all existing copies of any personal data that relates to them, notwithstanding that these facts were voluntarily and publically disclosed at the outset. The right extends *all* copies of the information that exist online, including copies available on websites other than those of the data controller and on search engines. The right accounts for countervailing interests, such as the right to free speech and expression, of other online entities and of the media in particular, at its sub-clause (3), and thus recognizes, atleast *prima facie* that it is not absolute.

V. THE GOOGLE SPAIN RULING

In *Google Spain S.L. and Google Inc. v Agencia Española de Protección de Datos*[51], the CJEU ruled that Google was a data controller, and that it was under an obligation to delist websites from its search results on complaints from data subjects. This case concerned publically available information that has been lawfully published in a newspaper and that was available on its online form as well.

---

[48] Rolf H. Weber, The Right to Be Forgotten: More Than a Pandora's Box?, 2 (2011) JIPITEC 120, ¶ 5-9.

[49] *See* Article 40, Loi nº 78-17 du janvier 1978 relative à l'informatique, aux fichiers et aux libertés; Charte du droit à l'oubli dans les sites collaboratifs et les mo-teurs de recherche, October 13, 2010 *available at* http://www.aidh.org/Actualite/Act_2010/Images/Charte_oubli_La_Charte.pdf. *See also* Hunton & Williams LLP, *French Government Secures "Right to Be Forgotten" on the Internet*, (October 21, 2010) http://www.huntonprivacyblog.com/2010/10/articles/french-government-secures-right-to-be-forgotten-on-the-internet/ (for reportage in English).

[50] *See* Judgment no. 5525 of the Third Civil Division, Italian Supreme Court.

[51] Case C-131/12 (CJEU).

What is significant is that while the the CJEU uses the language of a right to be forgotten, that is not in fact what the ruling establishes. There is no erasure of information from its source so that it no longer exists online. The ruling dealt only with search engines and found that they were under an obligation to delist a website on the receipt of a complaint. The Article 29 Working Party, which issued guidelines[52] on the application of the ruling also made clear that content at the source would remain unaffected. What this ruling does in effect is to make access to content more difficult. This is an unfortunate outcome that is neither able to protect individual privacy nor serve the ends of free and equal access to publically available information. Compromising the integrity of the catalogue of information online and obscuring data would logically lead to creating information elites and presumptively unreasonable reinforcements of existing power imbalances – those with greater resources would be able to access more information that those with fewer. So for example, a large business checking the background of a potential employee would still be able to afford access to this information. The weight of this ruling falls disproportionately on the smaller, poorer and less powerful consumers of information.

The logics of the ruling also seem problematic – if the court saw the availability of this information as infringing Mr. Costeja's rights, the logical response would have been to require that the content no longer be available. That would, of course, raise its own set of concerns. There is a clear social value that *complete* archives, as historical record, and surely this should win in the balancing against one individuals concerns with regard to information which was made public in a wholly lawful manner.

The CJEU had every opportunity to engage with arguments from free speech, and it is unfortunate that it did not. The Advocate General's Opinion,[53] which was presented to the Court, clearly outlined these concerns.

---

[52] Press Release Communiqué de presse Mitteilung für die Presse Brussels, 26 November 2014 Issued by the Article 29 Data Protection Working Party http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf.

[53] Opinion of Advocate General Jääskinen delivered on 25 June 2013 (1) Case C□131/12, Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) & Mario Costeja González (Reference for a preliminary ruling from the Audiencia Nacional (Spain)) *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11341

VI. PRAGMATIC CONCERNS: UTILITY, REGULABILITY & BALANCING STAKEHOLDERS' INTERESTS

Merits & Demerits

It has already been established that digital memory is uniquely permanent and creates the potential for deeply pervasive incursions into private lives and personal data. It increases, in particular, the potential for surveillance by several stakeholders on the internet, the state, data controllers, search engines (and similar gateways) as well as other users. Informational privacy and the right to personal self-determination stand to be diluted by social networking coupled with comprehensive indexing on the World Wide Web. Instances of employer surveillance on social networking sites[54] are one example of the increasing application of data to uses unforeseen and potentially inimical to data subjects' interests. The right to be forgotten, if effective, will mitigate some of these concerns.

Commendably, Article 17's text places explicit emphasis on the rights of the child, given that comprehensive remembering is inconsistent with fluid and evolving identities, their legal incapacity to consent and the fact that, as "digital natives"[55], they normatively reveal rather than mask personal information. In addition, to some degree, it addresses the concern that it is no longer possible to have different projections of one's self for different contexts[56] and encourages contextual integrity and specificity

The countervailing interests to the provision of a right to be forgotten have already been inventoried.[57] However, the consequences of prioritizing privacy at their cost through Article 17 bears detailing:

---

[54] Dionne Searcey, *Employers Watching Workers Online Spurs Privacy Debate,* April 23, 2009, THE WALL STREET JOURNAL, *available at* http://online.wsj.com/article/SB124045009224646091.html.

[55] *See generally* JOHN PALFREY AND URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008).

[56] *See, for e.g.,* Curtis Sittenfeld, *I'm on Facebook. It's Over*, September 3, 2011, THE NEW YORK TIMES *available at* http://www.nytimes.com/2011/09/04/opinion/sunday/if-im-on-facebook-it-must-be-over.html?_r=2.

[57] *See* p.5, *supra*; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1217 (1998).

While the idea of a right to be forgotten is useful, Article 17 imposes burdens on intermediaries that may unreasonably intrude on their right to carry on business. Social networking sites have had trouble with ensuring deletion in the past,[58] and creating liability in revenue, as does the new Regulation, could mean that the balance is unjustifiably tilted away from any preservation of intermediaries' commercial interests.

There is a compelling set of arguments against the right, given its chilling effect. While the right to delete already applies to information posted by the data subject herself or himself, the chilling effect is implicated where information is posted by another, or copies (of either of these two types) exist. It is untenable to allow the information to be deleted simply because it relates to an individual. This realistically threatens journalistic endeavour and, therefore, legitimate speech. Further, Article 17 can also be criticized on the ground that it mandates private or commercial censorship by imposing liabilities on neutral intermediaries.[59] This can also create the propensity to over-censor to avoid liability and chill legitimate speech.

Unlike with defamation or libel, the right to be forgotten covers within its ambit information that is both true and voluntarily disclosed. There is a clear societal interest in the maintenance of comprehensive historical records. This raises the need to balance the right to curate one's identity to a reasonable degree against the general right to know and to receive information.

Regulatory Responses

Laissez-faire and self-regulation are inappropriate mechanisms by which to regulate toward privacy, whether it is offline or online.[60] An unregulated space for intermediaries online would mean minimal (if any) privacy safeguards. Privacy is, in the best case, not a fully monetizable

[58] *See, for e.g.,* Jacqui Cheng "Deleted" Facebook photos still not deleted: a followup, ARS TECHNICA, *available at* http://arstechnica.com/web/news/2010/10/facebook-may-be-making-strides.ars.

[59] *See* Seth F. Kreimer, *Censorship By Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 13-16 (2006); Jonathan Zittrain, *Internet Points of Control,* 44 B.C. L. REV. 653, 688 (2003); Jerry Brito, *What Europe's 'Right to Be Forgotten' Has in Common with SOPA, available at* http://techland.time.com/2012/01/30/what-europes-right-to-be-forgotten-has-in-common-with-sopa/; Adam Thierer, *Europe's 'Right to Be Forgotten': Privacy as Internet Censorship, available at* http://techliberation.com/2012/01/23/europes-right-to-be-forgotten-privacy-as-internet-censorship/ .

[60] Mike Feintuck, *Regulatory Rationales Beyond the Economic: In Search of the Public Interest* in THE OXFORD HANDBOOK OF REGULATION (2010) 39-60 (Public interest objectives must be delivered otherwise than by *purely* market-driven regulation.).

object, given the asymmetries in data subjects' understanding of privacy protections online[61], as well as bounded rationalities of minors which arise out of social norms on social networking sites, if nowhere else.[62] Consequently, the problem with self-regulation is that there is no compelling economic incentive that will lead to ideal degree of protection of informational privacy. Although industry responses do exist, these have proved largely unsatisfactory. One example is of the *robots.txt* standard, which allows for specific areas of websites to be excluded from indexing by search engines such as Google.[63] However, in addition to the fact that this standard is not intended to address the actual copies of the private information, compliance with this standard is purely voluntary. Another is ReputationDefender[64], a service offering "reputation management" services online. However, this is a third-party service available on the payment of a fee, and constitutes a reactionary and short-term response. Overall, the only effective alternative in such a system is "digital abstinence",[65] a self-explanatory term that is an unreasonable option because it places an inordinate burden on speech.

It is by now axiomatic that the Internet *can* be regulated by the state. Furthermore, given the failings of self-regulation, it can be argued that the state *must* intervene to preserve privacy in the case at hand, even if the regulation is only of Lessig's "some-regulation-better-than-none"[66] type. Innovation in legal regulation has already attempted to address the problems arising from perfect, permanent and public memory online. Zittrain proposes a paradigm of "reputation bankruptcy", based on the Fair Credit Reporting Act in the United States, to allow "fresh starts" online.[67] (This notion of second chances is already recognized in laws mandating sealing or disposal of records relating to personal bankruptcy and juvenile crime.) Another option would be to treat

---

[61] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 506, 509.

[62] Danah Boyd and Alice Marwick, *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies*, Paper presented at the Oxford Internet Institute Decade in Internet Time Symposium, September 22, 2011 *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.

[63] *See The Robots Exclusion Protocol, available at* http://www.robotstxt.org/ .

[64] Scott Gilbertson, *Delete Your Bad Web Rep*, July 11, 2006, WIRED MAGAZINE, *available at* http://www.wired.com/science/discoveries/news/2006/11/72063; *About us*, *available at* http://www.reputation.com/company.

[65] *Supra*, n. 41 at 128.

[66] *See* Lawrence Lessig, *Law Regulating Code Regulating Law*, 35 LOY. U. CHI. L.J. 1 (2003).

[67] JOHNATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 228-31 (2008). *See also* Johnathan L. Zittrain, *Reputation Bankruptcy*, CONCURRING OPINIONS *available at* http://www.concurringopinions.com/archives/2010/09/reputation-bankruptcy.html.

information as property.[68] Data is a valuable commodity, which subjects may be inclined to exchange as a cost for services. This could allow for some of the tensions that an expansionist paradigm of personal data could have with the right to free expression to be alleviated, by creating an informational "commons"[69] which all could freely exchange and use.

Finally, technological responses are also possible. Even where it is a satisfactory response, irrevocable anonymization of data is not yet a technical reality;[70] it is eliminated as an option at the threshold. Mayer-Schönberger's propositions, though largely untested, are possibilities: he suggests "perfect contextualization" through technical means, such that each bit of personal information would have to be located in its complete context and, more interestingly, auto-expiry: the notion that data should age and disappear over a given timespan, through a process of programming information systems to forget in a manner that is similar to human memory.[71] He proposes that the latter suggestion be operationalized by simply attaching an additional field of meta-data, to be specified by the generator of the content: a data retention period, at the end of which information will self-destruct.[72] Peter Fleischer has, however, recognized that this would do nothing for the problem of copies continuing to survive online. So, this would not be a *complete* answer to the problem. More broadly, Ann Cavoukian's privacy-by-design[73] offers a comprehensive and proactive system by which to ensure user privacy. However, while privileging and incentivizing privacy-enhancing technologies is a sustainable strategy, the provision of the right is indispensable with regard to information already disclosed.

VII. THE WAY FORWARD

The right to be forgotten is a valuable tool by which to operationalize online informational privacy for the vast majority of Internet users. Despite the failings of the CJEU's recent articulation of the right, it remains a useful way to encapsulate very real concerns about how

---

[68] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004).
[69] *Id.,*at 2088.
[70] *See* Paul Ohm, *Broken Promises of Privacy: Responding to The Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).
[71] *See supra,* n. 41.
[72] *See supra,* n. 41, at 185.
[73] Ann Cavoukian, *Privacy By Design: The Seven Foundational Principles, available at* http://privacybydesign.ca/about/principles/.

privacy concerns are shifting shape as the default moves from organic forgetting to digital remembering. However, Article 17 will realize this value only if it accounts for the concerns discussed above. Fundamentally, Article 17 is vague,[74] to the degree that some have suggested that it needs to be renamed as well as re-cast[75] and that it is in danger of being little more than a rhetorical device or placeholder term for political sloganeering.[76] Preliminarily, the following concrete changes would contribute to "lifting the fog" and articulating a reasoned balance between stakeholder interests:

First, Article 17 should be narrowed, so as to specify that the requirement to delete is a burden to be imposed on the publisher of the information, and to exclude the possibility of requiring information location tools such as search engines being required to de-list offending content, where it continues to exist.

Second, it must be made clear that Article 17 does not intend to create a right to re-write history. This can be done by more specifically delineating the rights in data posted by minors during the course of minority and data disclosed by the residuary class. The Regulation must also specify the conditions for informed consent, given that the right to delete will not be available where, for instance, legally fit adults disclose personal information in public spaces such as on social networking sites.

Third, sub-clause 3(a) must be made specific, to ensure clarity and disallow vexatious litigation, given that balancing with freedom of expression will involve expensive, time-consuming and case-by-case determinations in the absence of a specific and exhaustive list, covering all of the possible classes of exception.[77] The provision must also distinguish between the sources of (true and accurate) information, such that deletion can be requested only where the data subject published the information, in order to preserve journalistic rights.

---

[74] Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88.

[75] P.A. Bernal, *A Right to Delete?*, 2 EUR. J. L. & TECH. (2011) *available at* http://ejlt.org/article/view/75/144.

[76] Peter Fleischer, *The right to be forgotten, or how to edit your history* (January 29, 2012) *available at* http://peterfleischer.blogspot.in/2012/01/right-to-be-forgotten-or-how-to-edit.html

[77] P.A. Bernal, *A Right to Delete?*, 2 EUR. J. L. & TECH. (2011) *available at* http://ejlt.org/article/view/75/144, at § 3.2.