Forthcoming Computer Law & Security Review (2012)

The 'Right to be Forgotten' - Worth Remembering?

By Jef Ausloos

ABSTRACT

In the last few years there has been a lot of buzz around a so-called 'right to be forgotten'. Especially in Europe, this catchphrase is heavily debated in the media, in court and by regulators. Since a clear definition has not emerged (yet), the following article will try to raise the veil on this vague concept. The first part will weigh the right's pros and cons against each other. It will appear that the 'right to be forgotten' clearly has merit, but needs better definition to avoid any negative consequences. As such, the right is nothing more than a way to give (back) individuals control over their personal data and make the consent regime more effective. The second part will then evaluate the potential implementation of the right. Measures are required at the normative, economical, technical, as well as legislative level. The article concludes by proposing a 'right to be forgotten' that is limited to data-processing situations where the individual has given his or her consent. Combined with a public-interest exception, this should (partially) restore the power balance and allow individuals a more effective control over their personal data.

KEYWORDS

Right to be forgotten; Right to oblivion; Privacy; Personal Data; Europe; EU

The 'Right to be Forgotten' - Worth Remembering?

By Jef Ausloos

1 Introduction 2
2 The Concept 3
2.1 Definition 3
2.2 *Ratio Legis* 4
2.3 Drawbacks 7
2.4 Conclusion 8
3 Implementation 9
3.1 Norms 9
3.2 Market 10
3.3 Code 11
3.4 Law 12
3.4.1 Current Framework 13
3.4.2 Future Perspective 14
4 Conclusion 17

1 Introduction

The Internet doesn't forget

OVERVIEW - Personal data has become *the* currency on the Internet. It is collected, stored and used in an ever-increasing variety of ways by a countless amount of different users, producing a "panopticon beyond anything Bentham ever imagined".[1] Cheap sensors[2], have made 'little big brothers' out of all of us,[3] producing a complex interaction between our different roles as data *controller* and data *subject*. In this 'global village'[4] where every piece of information can be remembered until eternity, the question of control over one's 'personal data' becomes the more important. The idea of a 'right to be

[1] LAWRENCE LESSIG, *Code: Version 2.0* (Perseus Books 2006) 208. The author also refers to disproportional monitoring of behaviour and the dangers of profiling (manipulation and discrimination).
[2] JONATHAN ZITTRAIN, *The Future of the Internet and How to Stop It* (Yale University Press 2008) 205 *et seq*.
[3] ALESSANDRO ACQUISTI at Carnegie Mellon talks about the 'democratisation of surveillance' in this context. Currently, he is conducting interesting research on face recognition and augmented reality, matching pictures taken with a cheap webcam on campus with publicly available online images (linking offline to online identity). See: <http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/>.
[4] MARSHAL MCLUHAN in: DANIEL J. SOLOVE, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press 2007) 33.

forgotten' - currently being pondered by the European Commission[5] - has been pushed forward as an important materialisation of this 'control-right'. Although many cases[6] seem to validate the introduction of this right, when thought through, there are many difficulties and conflicting values at stake. After a critical evaluation of its pros and cons, this article will examine the practicability of a 'right to be forgotten' following LESSIG's four principal 'regulators' (norms, market, code and law).

2 The Concept

2.1 Definition

> *"The right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes."*[7]

BACKGROUND - With the emergence of new technologies, the 'default of forgetting' has gradually shifted towards a 'default of remembering'.[8] This has incited many to reflect on the notion of a '*right* to be forgotten'. The European Commission has recently requested clarifications of the concept and has made an initial attempt to give its own (broad and vague) definition (*supra*). Arguably the right implies that the designated personal information has to be removed irrevocably. In 2008, JONATHAN ZITTRAIN also proposed a similar concept - 'reputation bankruptcy' - allowing people a 'fresh start' on the Net.[9] It might seem obvious that once an individual withdraws his/her consent or expresses his/her wish to stop the processing of personal data, the data should irrevocably be removed from the data processor's servers. But, as will become clear later on in this article, this assumption does not entirely fit legal, economical, nor technical reality.

CONTROL RIGHT - The 'right to be forgotten' clearly takes a proprietary approach to privacy protection.[10] Its scope, therefore, strongly depends on a clear and consistent

---

[5] European Commission, 'Review of the data protection legal framework' <ec.europa.eu/justice/policies/privacy/review/index_en.htm>. Proposals to reform will likely be announced early 2012.

[6] Drunken Pirate Case (First chapter in: VIKTOR MAYER-SCHÖNBERGER, *Delete: the Virtue of Forgetting in the Digital Age* (Princeton University Press 2009) and JEFFREY ROSEN, 'The Web Means the End of Forgetting' *NYTimes* (New York 21 July 2010) <http://nyti.ms/ftHuEt>); Korean Dog Poop Girl; Little Fatty; Star Wars Kid; the sexting-phenomenon (TAUNYA BANKS, 'Technology Musings' (*Concurring Opinions*, 3 April 2011) <concurringopinions.com/archives/2011/04/technology-musings>); etc.

[7] European Commission, 'A Comprehensive Approach On Personal Data Protection In The European Union' COM (2010) 609 final.

[8] MAYER-SCHÖNBERGER (n 6). According to the author, this shift began centuries (even millennia) ago, starting with language and scripture, but reached its final *coup de grâce* with today's Internet.

[9] ZITTRAIN, *The Future of the Internet and How to Stop It* (n 2) 228.

[10] Also referred to as 'informational privacy', focusing on personal data (as a commodity) to protect privacy (approach in the Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281 (DP Directive)). This differs from the 'personal privacy' approach (in the European Convention of Human Rights), which focuses on the legitimate expectation of privacy,

definition of 'personal data'.[11] The right – in its purest form – suggests 'ownership' over one's personal data and more importantly implies a certain 'control-right' of the data subject. The individual decides what happens with the information and maintains control even after it 'left his/her hands'. This approach to privacy protection was particularly popular in the early 2000's, especially at the other side of the Atlantic.[12] But interest gradually faded away this past decade, probably due to (valid) criticism[13]. Nevertheless, in several situations a proprietary approach to privacy protection definitely has some value[14] and the right to be forgotten (as proposed *infra*) is a clear example of this.

2.2 *Ratio Legis*

PROBLEMATIC NATURE OF PRIVACY ISSUES – Privacy issues often only become apparent when it is already too late. Especially in today's information society, it is practically impossible to predict (all) negative consequences of the use of personal data.[15] And even if one can foresee a few, they are very abstract, distant and uncertain.[16] They are abstract because privacy harms often only concern societal, psychological issues and the like.[17] They are distant as they do not present themselves right away. And they are uncertain because they might never occur, or at least not in a foreseeable way. So, even if an individual might know intellectually that the usage might have negative consequences, this is not going to change behaviour that much. Additionally, personal data is often collected and used outside the individual's control or without him/her even knowing. Our search-history[18], location-data[19], browsing-habits[20], reading-behaviour[21] and much more,

---

moral harm and psychological integrity of individuals (*Von Hannover v Germany* App no 59320/00 (ECtHR, 24 June 2004), 50 *et seq.*).

[11] Defined very broadly in Europe (DP Directive, art.2(a) *juncto* preamble (26)) and interpreted in: Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' WP 136.

[12] PAMELA SAMUELSON, 'Privacy as Intellectual Property?' (2000) 52 *Stan L Rev* 1125; LESSIG (n 1), 200 *et seq*; PAUL SCHWARTZ, 'Property, Privacy, and Personal Data' (2004) 117 *Harv L Rev* 2055.

[13] Such as its limited scope and inability/inadequacy to deal with broader forms of privacy harm. See: MARC ROTENBERG, 'Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)' (2001) 2001 *Stan Tech L Rev* 1, 34-35; 91 *et seq*.; YVES POULLET, 'Around the Concept of Privacy: Ethics and Human Rights in the Information Society?' (2008) 14 *The European Files*, 11.

[14] For a clear and concise analysis of property rights as regulatory framework to protect personal data, see: NADEZHDA PURTOVA, 'Property in personal data: Second life of an old idea in the age of cloud computing, chain informatisation, and ambient intelligence' (2010) TILT Law & Technology Working Paper 2010/017 <http://ssrn.com/abstract=1641027>, 16 *et seq*.

[15] A survey by Microsoft pointed out that 75% of U.S. recruiters and HR professionals are ordered to do online research about candidates. 70% reported having rejected candidates because of information that was found online. See: ROSEN (n 6).

[16] One could make a parallel with smoking or eating unhealthy food. Even if a person is well aware of the (potential) consequences, these products are still widely consumed.

[17] E.g.: The panopticon effect. See: OSCAR H. GANDY, *The Panoptic Sort: A Political Economy of Personal Information* (Westview 1993). Others claim that comprehensive and permanent digital 'remembering' can undermine human reasoning. It prevents people from generalising and conceptualise. In: MAYER-SCHÖNBERGER (n 6) 118-119. Put very briefly, MAYER-SCHÖNBERGER explains in his book that digital memory denies time (temporal aspect) and context (see idea of contextual integrity, proposed in: HELEN F. NISSENBAUM, *Privacy in context : technology, policy, and the integrity of social life* (Stanford Law Books 2009)).

[18] DANIEL C. HOWE & HELEN NISSENBAUM, 'Trackmenot: Resisting Surveillance In Web Search' in: IAN KERR and others (eds.), *Lessons From The Identity Trail - Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press 2009) 417-436. Beyond traditional web search

is collected and/or used to a degree we can barely imagine. Technology, nowadays, allows for unprecedented forms of data-matching[22], de-anonymisation[23] and data-mining[24], all contributing to extensive 'digital dossiers'.[25] Additionally, the few efforts people can make in order to 'protect their privacy' online, are often ignored or circumvented.[26] With all this in mind, it becomes clear that putting the *onus* to anticipate every possible privacy harm on the data subject is unfair. The often-repeated argument 'they had it coming', therefore, cannot be followed. Combined with awareness-raising, a 'right to be forgotten' could (arguably) contribute to solving the issue without disproportionately burdening one party.

INADEQUACY OF CURRENT FRAMEWORK - Most jurisdictions primarily rely on a consent regime (article 7(a) DP Directive) to enable control over one's personal data. In a

---

tracking, Apple's recently announced mobile 'personal assistant' - Siri - will be in direct connection to the company's servers.

[19] ZeitOnline, 'Verräterisches Handy', *Die Zeit* (2011) <zeit.de/datenschutz/malte-spitz-data-retention>.

[20] Often for behavioural advertising purposes, through the use of flash (or resurrecting) cookies or by using Deep Packet Inspection (RALF BENDRATH & MILTON MUELLER, 'The End of the Net as We Know it? Deep Packet Inspection and Internet Governance' (4 August 2010) <http://ssrn.com/abstract=1653259>. CHRIS WILLIAMS, ' ISP data deal with former 'spyware' boss triggers privacy fears' (*The Register*, 25 February 2008) <www.theregister.co.uk/2008/02/25/phorm_isp_advertising>. Two companies (NebuAd in the US and Phorm in the UK) who have tried to implement it on a large, commercial scale, have failed so far). Also see: 'Beware the cookie monster' *The Economist* (Seattle, 22 August 2011) <www.economist.com/node/21526571>. Tracking browsing behaviour can have other purposes too. Literally all of your Internet browsing on Amazon's new mobile browser 'Silk' on the Kindle Fire, will go through the company's servers to allow a faster and smoother web experience.

[21] Tracking people's reading behaviour on e-readers, companies argue, is justified as to keep different devices synchronised.

[22] JONATHAN MAYER, at the Stanford Center for Internet and Society recently discovered that dating-site *OkCupid* is sharing all kinds of (very) personal information with data providers such as BlueKai and Lotame. JONATHAN MAYER, 'Tracking the Trackers: Where Everybody Knows Your Username' (*CIS*, 11 October 2011) <http://cyberlaw.stanford.edu/node/6740>.

[23] Clearly demonstrated by the AOL and Netflix cases. In the first one, researchers quickly retrieved the real identity behind the unique numbers AOL had attributed to the published search queries of over half a million of its users. The same thing happened with movie ratings attached to unique numbers that Netflix had posted. PAUL OHM, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', (13 August 2009) University of Colorado Law Legal Studies Research Paper, <http://ssrn.com/abstract=1450006>, 15 *et seq*. Netflix even had to settle a legal challenge (R. SINGEL, 'NetFlix Cancels Recommendation Contest After Privacy Lawsuit' (*Wired*, 12 March 2010) <www.wired.com/threatlevel/2010/03/netflix-cancels-contest>).

[24] JASON MILLAR, 'Core Privacy - A Problem of Predictive Data Mining' in: IAN KERR and others (eds.), *Lessons From The Identity Trail - Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press 2009) 103-119.

[25] The combination of a variety of relatively innocuous data bits might have far-reaching privacy implications, as US Supreme Court Justice Scalia clearly experienced 2 years ago. See: DANIEL SOLOVE, 'Justice Scalia's Dossier: Interesting Issues about Privacy and Ethics' (*Concurring Opinions*, 29 April 2009) <http://www.concurringopinions.com/archives/2009/04/justice_scalias_2.html>. Also see: DANIEL SOLOVE, *Understanding Privacy* (Harvard University Press 2008), 70.

[26] The controversy surrounding so-called 'super-cookies' or 'respawning cookies' (*supra*) offers a great example in this regard. See: MIKA D. AYENSON and others, 'Flash Cookies And Privacy II: Now With HTML5 And Etag Respawning' (29 July 2011) <http://ssrn.com/abstract=1898390>. And the lack of companies' interest to protect their users' privacy was demonstrated once more in a recent study pointing out that most of the top 185 US websites are (un)intentionally leaking personal data to third parties, despite privacy policies claiming the opposite. In: MAYER (n 22).

free and democratic society, privacy is often considered to be sufficiently protected by giving individuals the 'power' to (dis)agree. Practice however, has clearly shown the shortcomings of this approach.[27] Privacy policies are written in vague legalese and people do not read them anyway. Network externalities,[28] lock-in[29] and the lack of valid alternatives often force people into consenting. And even a withdrawal of consent does not (necessarily) allow a person to have his or her data removed retroactively. An effective application of the purpose limitation principle – confining data processing to a previously defined scope – might seem to restrict the amount of potential harm in theory. But in an ever-increasing personalised web (where every piece of personal data can be considered as 'useful')[30], the value of this principle has become questionable too. A 'right to be forgotten' could bring back effective control over what happens to an individual's data.

PERMANENT RE-EVALUATION - The notion of 'personal data' has become very ambiguous and should not be seen as a static concept.[31] Information can be (un)linked to a person over time, vis-à-vis different actors and in different contexts. A flexible and casuistic approach is required, taking into account the constant transformation of 'data' as such. A 'right to be forgotten' would (arguably) offer people an effective opportunity to permanently (re-)evaluate the use of their data for ever-changing purposes in dynamic contexts[32]. Additionally, it would strengthen the individual's control over his/her identity[33], constitute some sort of 'check' on the purpose limitation principle and facilitate the accountability of data controllers[34]. These controllers might also become more lenient in their privacy policies, as the subject has the right to demand retro-active removal of all his/her data.

---

[27] More generally, the issues of a purely contractual approach to B2C relationships – largely due to the inequality of parties – has also resulted in stricter regulation to protect consumers.

[28] Or how the value of a service depends on the amount of users it has (e.g.: social networks).

[29] Investment in a service and lack of data-portability options decrease incentives for an individual to move to another provider (e.g.: Apple's iOS walled garden).

[30] For a recent evaluation of the impact of personalisation on individuals and society as a whole, see: ELI PARISER, *The Filter Bubble* (Penguin 2011).

[31] In a recent paper, P. SCHWARTZ AND D. SOLOVE make a distinction between data relating to an identif*ied* and an identif*iable* person. See: PAUL M. SCHWARTZ & DANIEL J. SOLOVE, 'The PII Problem: Privacy And A New Concept Of Personally Identifiable Information' (2011) NYU Law Review (forthcoming).

DAVID ARDIA describes identity as a continuum with on one end anonymity and fully disclosed personal identification at the other. Online, information is permanently moving (back and forth) on this line. See: DAVID S. ARDIA, 'Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law' (2010), *45 Harv. C.R.-C.L. L. Rev. 261*, 307.

[32] For more information on contextual privacy, see: NISSENBAUM (n 17).

Services like 123people.com or 'date check' (intelius.com/mobile) aggregate data from all over the web and form a great danger to proper contextualisation. Social Networks do not provide sufficient contextualisation tools either. See: DANIELLE CITRON, 'Aligning Privacy Expectations with Technical Tools' (*Concurring Opinions* 10 April 2011) <http://www.concurringopinions.com/archives/2011/04/aligning-privacy-expectations-with-technical-tools.html>.

JONATHAN ZITTRAIN speculates services might even be offered in the future that measure social desirability "based on minute social measurements — like how often he or she was approached or avoided by others at parties (a ranking that would be easy to calibrate under existing technology using cellphones and Bluetooth)." He also foresees the emergence of 'reputation brokers', providing advise on people's "sociability, trustworthiness and employability". See: ROSEN (n 6).

[33] On the importance of an individual's control over his/her reputation, see: SOLOVE, *The future of Reputation: Gossip, Rumor, and Privacy on the Internet* (n 4), 33.

[34] See: Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of Accountability' WP 173.

2.3 Drawbacks

LIMITED SCOPE - First of all, the 'right to be forgotten' seems to presuppose a contractual relationship. As will appear later in this article, it can/should only be applied in situations where the individual has consented to the processing of personal data. The concept is not suitable to cope with privacy issues where personal data is (legally) obtained without the individual's consent. Additionally, it is important to remember the right only provides an *ex post* solution to privacy issues.

'ANONYMISED DATA' - Many data controllers invoke the anonymisation-argument as their major line of defence.[35] Without going into the details about the value of this claim[36], it is clear that the right does not offer any solution in these (omnipresent) cases. Individuals may be profiled/targeted extensively and their data might (in)directly be used for comprehensive data-mining, but because no use is made of personal data *stricto sensu*[37], the individual cannot have a 'right to be forgotten' with regard to this information.

SUBTLE CENSORSHIP - One of the most repeated arguments against a 'right to be forgotten' is that it would constitute a concealed form of censorship.[38] By allowing people to remove their personal data at will, important information might become inaccessible, incomplete and/or misrepresentative of reality. There might be a great public interest in the remembrance of information.[39] One never knows what information might become useful in the future.[40] Culture is memory.[41] More specifically, the implementation of a fully-fledged 'right to be forgotten' might conflict with other fundamental rights such as freedom of expression and access to information.[42] Which right should prevail when and who should make this decision? Finally, defamation and privacy laws around the globe are already massively abused to censor legitimate speech. The introduction of a 'right to be forgotten', arguably, adds yet another censoring opportunity.

---

[35] Google recently introduced more privacy invasive practices in the mobile space. It's claim is that all personal data is made absolutely anonymous. GREG STERLING, 'Google Intros New Privacy Controls For Mobile Consumers' (*Search Engine Land*, 15 April 2011) <http://searchengineland.com/google-intros-new-privacy-controls-for-mobile-consumers-73156>.

[36] As mentioned above, though, de-anonymisation capabilities become increasingly powerful and the 'anonymisation-argument' has less and less value. For a thorough critical piece on anonymisation in a digital environment, see: OHM (n 23). For an interesting counter-argument, see: JANE YAKOWITZ, 'Tragedy of the Data Commons' (2011) <http://ssrn.com/abstract=1789749>.

[37] "The ability of behavioural targeting firms to pervasively track users without deciphering their specific identities seems to have made the 'identifiability' aspect of the definition of personal data obsolete." In: OMER TENE, 'Privacy: The New Generations' (2010) 1 International Data privacy Law 15, 25.

[38] PETER FLEISCHER, 'Foggy Thinking about the Right to Oblivion' (*Privacy...?*, 9 March 2011) <http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html>.

[39] E.g.: Google Flu Trends (http://www.google.org/flutrends/).

[40] VIKTOR MAYER-SCHÖNBERGER, 'Book Talk: Delete - The Virtue of Forgetting in the Digital Age' (*Berkman Center for Internet & Society* 2009) <http://cyber.law.harvard.edu/interactive/events/2009/10/schonberger>.

[41] FLEISCHER, 'Foggy Thinking about the Right to Oblivion' (n 38).

[42] For more information on the conflict between the wish of 'free flow of information' and the desire to maintain control over information relating to an individual, see: SOLOVE, *The future of Reputation: Gossip, Rumor, and Privacy on the Internet* (n 4), 33. In this book (92; 94 *et seq*.) the author explains that the posting of personal information of others online to *shame* may have benefits.

PRACTICAL DIFFICULTIES - How should the right deal with ubiquitous and opaque cross-platform data transfers? One could request 'personal data' to be deleted on one site, but meanwhile the information might have been copied and/or 'anonymised' already. All these potential third-party uses (and/or 'secondary uses') are practically untraceable and do not necessarily take into account deletion of the primary material.[43][44] Moreover, the right also raises some technical implementation issues (*infra*, 'Code'). In short, besides traditional jurisdictional issues, the actual implementation of an effective 'right to be forgotten' brings along many practical difficulties as well.

THE ILLUSION OF CHOICE - Just like the binary 'consent-framework' in most privacy-regulations nowadays[45], the 'right to be forgotten', arguably, is insufficient to deal with privacy issues on the Net. If a person does not agree with a privacy policy, he/she simply can not use the product or service.[46] Introducing a 'right to be forgotten' only postpones this illusion of choice. Additionally it burdens the individual even more and offers a wild card for more privacy-intrusive uses. The individual will often be frustrated by defences like "the subject had the right to delete".

2.4 Conclusion

BALANCED APPROACH - Although the proposed right might seem as a valuable right *a priori*, it raises both practical and policy-related questions when one takes a closer look. Before a potential implementation, a careful balance should be made between the individual's right to privacy and other (fundamental) rights.[47] It will therefore be important to clearly define the scope of application of the right. Furthermore, it will often be economically undesirable to put the burden of decision-making on the actual data controller (company). A clear set of rules should be put in place, on which erasure

---

[43] It might have been used, for example, for data-mining practices to adapt the individual's profile. The complexity of the situation is clearly illustrated by the recent sale of personal data by some major Facebook Apps to advertisers. Even if one expresses his/her will to be forgotten on a platform that provides such an option, there is absolutely no guarantee the individual's data is also 'forgotten' by the 'third' (App-providers) and even fourth (advertisers) parties. See: EMILY STEEL & GEOFFREY A. FLOWER, 'Facebook in Privacy Breach' (*Wall Street Journal*, 18 October 2010) <http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html>.

[44] Also see: ZITTRAIN, *The Future of the Internet and How to Stop It* (n 2), 229.

[45] Where privacy is considered to be sufficiently protected by allowing an individual to say either 'yes' or 'no' to personal data processing. For more on the issues surrounding consent, see: SOLON BAROCAS, 'On Notice: The Trouble with Notice and Consent' (*MITTechTV*, 2009) <http://techtv.mit.edu/videos/4535-session-ii-on-notice-the-trouble-with-notice-and-consent>.
Also see: RYAN CALO, 'Against Notice Skepticism in Privacy (And Elsewhere)' (2012) 87 Notre Dame Law Review (forthcoming) <http://ssrn.com/abstract=1790144>; DAVID LEVINE & RYAN CALO, 'Interview (#129) with Ryan Calo on Privacy Harms' (*Hearsay Culture*, 11 January 2011) <http://cyberlaw.stanford.edu/podcasts/20110111_Levine_129_Calo.mp3>.
On the inadequacy of the 'binary approach' more generally, see: ANNE CHEUNG, 'Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd' (2009) 1 Journal of Media Law 191; HELEN F. NISSENBAUM, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119.

[46] E.g.: individuals who do not want Apple to collect and use their data (anymore), would have to get rid of their iPhone because Apple collects and uses data 'to make its products and services better'. BRIAN X. CHEN, 'iPhone or iSpy? Feds, Lawyers Tackle Mobile Privacy' (*Wired*, 12 April 2011) <wired.com/gadgetlab/2011/04/iphone-ispy>. Companies may have a legitimate interest in requiring personal data. And a 'right to be forgotten' might be completely incompatible with delivering their service/product.

[47] See for example the tension between an individual's wish to delete information versus society's desire to 'remember' it. MAYER-SCHÖNBERGER (n 6), 190-191.

depends. With all of this in mind, the right merely enables the consent-regime to be more effective.

EX POST SOLUTION - It should be repeated however, that the right is nothing more than an *a posteriori* band-aid solution. The right only comes *after* the collection and can only prevent further (harmful) processing and dissemination. To really solve the issue, it is necessary to strike at the root. Many solutions have been proposed over the years. Worth mentioning in this context are: awareness-raising[48], transparency, clearer privacy notices[49], data-minimisation, stricter control on the purpose limitation principle, 'anonymisation'[50], transparency, encryption, etc. The goal of each of these measures is to prevent (potentially harmful) information to be shared in the first place. But, in an ever-increasing social Internet, where many features depend on disclosing personal data[51], *ex post* measures are needed as well. Enabling a more effective control by the individual, the introduction of a (well-defined) 'right to be forgotten', therefore, seems appropriate at first sight.[52] Only then will it be possible to take into account different preferences according to context and time.

3 Implementation

3.1 Norms

CONTROL - The 'right to be forgotten' is a mere crystallisation of the more fundamental wish for 'control' over one's personal data. Although norms with regard to protecting privacy vary among different countries and regions[53], the wish for more (effective) control seems to be a common denominator. Major privacy scandals in the last

---

[48] European Commission, 'A Comprehensive Approach On Personal Data Protection In The European Union' (n 6).
Also see: ROSEN (n 6); TENE, 'Privacy: The New Generations' (n 37), 12-13. According to the first author, research has demonstrated that the use of an anthropomorphic icon makes people more considerate about disclosing data.

[49] E.g. short layered notices, in: CALO, 'Against Notice Skepticism' (n 45),18 *et seq.*

[50] Although never perfect, anonymisation can definitely help to make access to and (mis)use of data a lot more burdensome. Google recently introduced some extended control-rights along with more privacy invasive practices on the mobile space, claiming that all personal data is made anonymous. STERLING (n 35).

[51] With Facebook as the most obvious example of ever-increasing data collection (https://f8.facebook.com).

[52] As an IT-investor recently put it: "Consumers must be able to protect their privacy by (1) Authorising companies to gather their information; (2) Understanding how the company will use their information; (3) Retaining the ability to opt out". In: HABIB KAIROUZ, 'How Worried Are Consumers About Privacy?' (*TechCrunch*, 10 April 2011) <techcrunch.com/2011/04/10/how-worried-are-consumers-about-privacy>. This can be enabled with more comprehensive privacy tools; universal (cross-platform) protocols; efficient security; etc.
European Studies too have pointed out the importance of empowering individuals in effective privacy regimes. See: LRDP Kantor Ltd. & Centre for Public Reform, 'Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments' (European Commission, 20 January 2010) <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf>.

[53] E.g.: Google street view and the so-called German '*Verpixelungsrecht*'. In: JEFF JARVIS, *Public Parts - How Sharing in the Digital Age Improves the Way We Work and Live* (Simon & Schuster 2011), 30 *et seq*. The author mentions the German *Freikörperkultur*, revealing criminals' identities in the US, and the publication of people's taxes and incomes in Norway and Finland.

few years[54] have clearly demonstrated the complete lack of control individuals have over their data in practice. And the massive public outcry as a result to these scandals suggests that absolute control is perceived as a general norm already.[55] People especially seem to expect they should be able to have their data removed at anytime and at any place.[56] One might ask however, if this perceived norm is not merely a remainder of the pre-internet era where the default was 'forgetting'.

3.2 Market

INSUFFICIENCY - The Internet is evolving from a practically entirely 'free' network to a primarily commercial environment. In this new setting, personal data has become the major currency. The greediness for this currency and the limitless data collection capacities of modern technology, have caused a major power shift between data *users* and data *subjects*. On the Internet, the latter are virtually powerless against the first. Even if an individual knows that his or her data is being collected/used, there is often not much that can be done in order to prevent this. Notice and takedown procedures might take content out of (public) sight, but do not normally result in removal from the data user's servers.[57] Public outcry and a lot of media coverage have not led to much improvement (yet). And the claim that competition is only 'one click away' has no value in this context. The free market argument depends on transparency[58] and does not take into account network externalities and lock-in issues (*supra*). Further, the few true efforts that are made by market players[59], necessarily lack in credibility as their business model generally depends on the collection and use of personal data. Finally, consumers are

---

[54] E.g.: Facebook's omnipresent 'Like Button' (RIVA RICHMOND, 'As 'Like' Buttons Spread, So Do Facebook's Tentacles' *NYTimes* (New York, 27 September 2011) <http://bits.blogs.nytimes.com/2011/09/27/as-like-buttons-spread-so-do-facebooks-tentacles>) and its storage of data that has been deleted by users (*infra*, n 57); the sale of personal data for unanticipated, commercial purposes (most recently illustrated on a massive scale in Hong Kong: 'Hong Kong banks sold personal data: watchdog' *TheChinaPost* (Hong Kong, 21 June 2011) < http://www.chinapost.com.tw/china/local-news/hong-kong/2011/06/21/307011/Hong-Kong.htm>); the discovery of concealed and unavoidable online tracking (R. SINGEL, 'Researchers Expose Cunning Online Tracking Service That Can't Be Dodged' (*Wired*, 29 July 2011) <www.wired.com/epicenter/2011/07/undeletable-cookie/>); cell-phone tracking (*supra*, n 19); Google Buzz ('New Google's Service Raises Privacy Concerns' (*EDRi-gram*, 24 February 2010) <www.edri.org/edrigram/number8.4/privacy-google-buzz-service>); Deep Packet Inspection for commercial purposes ('Third Phorm Trials Started, But Privacy Concerns Remained' (*EDRi-gram*, 8 October 2008) <www.edri.org/edrigram/number6.19/phorm-trial-privacy>); etc.

[55] CHRISTOPHER KUNER and others, 'Let's not kill all the privacy laws (and lawyers)' (2011) 1 *IDPL* 209. Also see: TENE, 'Privacy: The New Generations' (n 37), 11; ROSEN (n 6).

[56] See part 'Ratio Legis', *supra*.

[57] European citizens can request Facebook to send them all personal data in Facebook's possession: https://www.facebook.com/help/contact.php?show_form=data_requests. In these reports it becomes clear that Facebook keeps track of all your 'removed' data as well.

[58] Even when people know which company collects and/or uses their data, it is never clear to what extent this happens and under what conditions (privacy policies generally offer not much clarifications). The arguments become even more absurd when one takes into account the amount of data that is being collected by companies most users have never even heard of (e.g.: data brokers such as *Acxiom* and *ChoicePoint*).

[59] The ability to have pictures blurred or taken down from Google Streetview (*Verpixelungsrecht*), in: JARVIS (n 53), 27. Google, 'How many German households have opted-out of Street View?' (*European Public Policy Blog*, 21 October 2010) <http://googlepolicyeurope.blogspot.com/2010/10/how-many-german-households-have-opted.html>. Also see the 'ObscuraCam'-App in the Android Market.

showing a paradoxical demand for more data collection[60], which illustrates that they do not necessarily want more 'privacy' (oh, what a vague concept), but especially want more 'control'. Concluding, it has become clear over the last few years that it is impossible to rely on the market alone to give (back) control to individuals. Code and especially the law will be necessary to assure a healthy and balanced market.

3.3 Code

EXPIRY DATE - One of the most interesting ideas on how to implement the 'right to be forgotten' is that of an 'expiry date'.[61] It has the considerable advantage that an individual does not have to worry any longer after personal data is shared. But the practicability of this theoretical principle is far from evident. Personal data could, for example, be 'tagged' with an expiry date (adding so-called metadata).[62] This system relies on the willingness of data users to respect it and should probably be accompanied by a corresponding law forcing data users to comply. Alternatively a more profound technical protection could be inserted in the data, similar to DRM protection for intellectual property. In both cases, individuals should have a legal recourse against circumvention of these expiry dates.[63] Although interesting research is being done on the latter[64], the first (voluntary) system seems most technically feasible at this point in time.[65] Nonetheless, the idea that an individual will have to give an expiry date each time personal data is being collected seems unrealistic. Besides, it risks becoming a merely *pro forma* requirement that no one truly pays attention to, as is already the case in the current consent regime.[66] Additionally, nothing would prevent someone from copying and/or decrypting the data for as long as it is available.[67] A 'privacy agent', monitoring all personal data transfers and allowing people to manage their expiry preferences over time according to different types of data, controllers and contexts, could contribute to a more

---

[60] Clearly illustrated by the incredible amount of (smartphone) apps for monitoring and managing location data, fitness data, diet data, financial data, and so on.

[61] MAYER-SCHÖNBERGER (n 6).
A recent and interesting application of this principle is the 'TigerText-app' on smart phones. Messages sent through this app are automatically deleted after a predetermined time (tigertext.com).

[62] A similar example is the robots.txt file in which websites can 'opt-out' of search engine listings. Also see: JONATHAN ZITTRAIN, 'Privacy 2.0' (2008) *The University of Chicago Legal Forum* 65, 101 *et seq*.

[63] RYAN CALO at the Stanford Center for Internet and Society, has proposed a wider interpretation of anti-circumvention provisions in the DMCA (in Europe, Directive 2001/29/EC). These should not just be applied in intellectual property cases, but also when *any* 'technical measure' to protect (personal) data (blocking/deleting cookies, opting out, incognito modus, etc.) is circumvented or ignored. See: RYAN CALO, 'DRM for Privacy: Part 2' (*Concurring Opinions*, 14 August 2011) <www.concurringopinions.com/archives/2011/08/drm-for-privacy-part-2>.

[64] Researchers at the University of Washington are currently working on a technology called 'Vanish', which makes data 'auto-destruct' after a specified time period. "Instead of relying on Google, Facebook or Hotmail to delete the data that is stored 'in the cloud' — in other words, on their distributed servers — Vanish encrypts the data and then 'shatters' the encryption key. To read the data, your computer has to put the pieces of the key back together, but they 'erode' or 'rust' as time passes, and after a certain point the document can no longer be read." If successful, the technology could also be applied to any type of data stored in the cloud. In: ROSEN (n 6).

[65] MAYER-SCHÖNBERGER too criticises the implementation through DRMs. MAYER-SCHÖNBERGER (n 6), 144 *et seq*.

[66] SOLON BAROCAS & HELEN F. NISSENBAUM, 'On Notice: The Trouble with Notice and Consent' (2009) <http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf>.

[67] ROSEN (n 6).

effective 'user choice'[68]. Obviously, such centralised data-managing software raises many other privacy questions.[69] In short, although it could definitely contribute to shifting the balance, effective 'expiry date technology' will never allow an individual to be confident his/her data is entirely deleted.

REPUTATION MANAGERS - In addition to the vast increase in privacy enhancing browser-plugins[70], another interesting trend is the emergence of reputation managers on the Internet.[71] These websites offer to monitor all information circulating about an individual, defending reputation technically *and* legally (for instance by deleting harmful information or making it inaccessible)[72] and even "define your image". This clearly illustrates the potential threats of censorship and the embezzlement and distortion of information on the Internet.

ALTERNATIVES - Vague, ineffective top-down proposals[73] and the failure of the market to allow individuals to effectively control what happens to their personal data have led to an explosion of (mainly) grassroots initiatives to restore control. These projects are generally open source, allowing input from everyone. One of the most notable and recent examples in this regard is Diaspora.[74] It is a social network platform built from the ground up with privacy protection in mind and is entirely developed by a global community of volunteers. It even offers users the opportunity to host their own 'Diaspora server', so each individual can have its 'own cloud'. It will be interesting to see how successful the service will be in such a hard-to-penetrate-market. Its compatibility with commercial social networks will definitely help and other open-source examples such as Firefox, Linux and Wikipedia have clearly demonstrated already that these initiatives can work. The great amount of privacy and security plug-ins that are developed (mostly by volunteers) for web browsers also offer individuals a chance to have more control over their personal data. Robots.txt, finally, is another noteworthy example of a standard that is being established to communicate (privacy) preferences of a website to web robots (spiders or crawlers).[75] In the context of this article it is especially relevant to prevent data from being copied by third parties. The major hurdles these alternatives face are that they entirely depend on user adoption and the good will of data controllers (as mentioned *supra*, privacy preferences are often ignored or circumvented). Therefore, to give (back) individuals effective control and ensure data controller compliance a legal provision should be introduced.

3.4 Law

THE ISSUE OF EFFECTIVITY - As discussed *supra*, the existing consent regime has clearly failed to meet people's expectancy of privacy protection. The Article 29 Working

---

[68] MAYER-SCHÖNBERGER (n 6), 172-173.
[69] Especially regarding security and who has access to it.
[70] Check: https://addons.mozilla.org/en-US/firefox/extensions/privacy-security.
ERICA NEWLAND, 'CDT Releases Draft Definition of "Do Not Track"' (*Center for Democracy & Technology*, 31 January 2011) <http://cdt.org/blogs/erica-newland/cdt-releases-draft-definition-"do-not-track">.
[71] Reputation.com; reputationsquad.com; les-infostrateges.com; metalrabbitmedia.com; etc.
[72] ReputationSquad even partnered with an insurance company (Swiss Life) to offer financial, legal and technical help in case your e-reputation would be harmed, for €9.9/month (see: <www.reputationsquad.com/2011/06/reputation-squad-lance-en-partenariat-avec-swiss-life-la-premiere-offre-d'assurance-e-reputation>).
[73] E.g.: LRDP Kantor Ltd. & Centre for Public Reform (n 52), 46 *et seq*.
[74] Diasporafoundation.org.
[75] www.robotstxt.org.

Party's recent 'Opinion on Consent' has emphasised that individuals should always be allowed to withdraw their consent. But such a 'right of withdrawal' does not (necessarily) cover personal data to be removed retroactively.[7677] A conditional 'right to be forgotten', therefore, might seem a legitimate request in order to restore the power balance.

3.4.1 Current Framework

OVERVIEW - The EU legal framework does not provide for a general 'right to be forgotten'. Nevertheless, some existing provisions in the data protection framework[78] can be interpreted as diluted 'right to be forgotten' provisions. Article 6(1)(e) DP Directive, for example, declares that personal data can be kept "for no longer than is necessary for the purposes for which the data were collected or for which they are further processed." However, besides some exceptional cases[79], on the Internet personal data is permanently collected and used for never-ending purposes, rendering these provisions quite useless in practice. The consent requirement in art.7 remains silent on a potential withdrawal of consent. In its most recent opinion[80], the Art29 Working Party did stress that the right of withdrawal is implied in DP Directive but can only be exercised for the future.[81] In other words, the introduction of a potential 'right to be forgotten' cannot be legitimised by the existing consent regime. The most important provisions with regard to the 'right to be forgotten' in the DP Directive seem to be art.12 (b) and art.14. The first proclaims that each data subject has the right to "obtain from the controller (...) erasure or blocking of data". But the provision's scope of application is heavily limited, as it only applies "when the processing does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data". Art. 14, subsequently, provides the data subject with a general right to object to data processing, but also has a limited scope. The article only requires member states to provide a right to object in cases referred to in art. 7(e) and (f)[82] *and* if they are based on 'compelling and legitimate grounds'. This means that member states are not bound to introduce a 'right of objection' in cases where the data subject has given its unambiguous consent, where the processing is necessary to perform a contract, legal obligation or to protect a vital interest of the data subject (art.7 (a)-(d)). Nevertheless, if the data will be used for direct marketing purposes or will be shared with third parties, the individual always has the right to object without having to give any justification (art.14(b)). Further, article 6 of the (recently amended) ePrivacy Directive[83] introduces some sort of 'right to be forgotten' with regard to *traffic*

---

[76] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent' WP 187, 9; 32 *et seq*.

[77] On the lack of a provision allowing for retroactive removal, see for example: JEAN-FERDINAND PUYRAIMOND, 'La Protection des Données Personnelles: Nouveau Fondement du Droit à l'Image' (2008) 5 *Auteurs & Media* 364, 374-375.

[78] As opposed to the broader protection of privacy in article 8 of the ECHR. The right to be forgotten necessarily refers to specific data.

[79] Google deletes search history after 9 months. See: MIGUEL HELFT, 'Google Tightens Data Retention Policy - Again' (*NYTimes*, 9 September 2008) <http://bits.blogs.nytimes.com/2008/09/09/google-tightens-data-retention-policy-again/>.

[80] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent' (n 76).

[81] *Ibidem*, 9; 32 *et seq*.

[82] Processing for (e) 'tasks of public interest' or (f) 'necessary for the legitimate interests of the data controller'.

[83] Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201 (ePrivacy Directive). This Directive was amended by: Council Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users'

data.[84] But this article too, has some important exceptions and has a very limited scope (only traffic data, defined in art.2(b), is covered). At the other side of the spectrum, finally, the Data Retention Directive[85] seems to dilute these feeble 'right to be forgotten' attempts even more. According to this Directive, telecommunication service providers have to store traffic and location (non-content) data for up to two years.

3.4.2 Future Perspective

ONE AMONG MANY - The previous paragraph made clear that the European framework does not (yet) have a true 'right to be forgotten' in place. Some 'light' versions of the right can be found in a range of provisions in both the DP Directive and the ePrivacy Directive. In theory, the European framework offers quite a comprehensive protection already. Looking at the future, it is important to focus on enhancing the effectiveness of the existing framework in practice. The Commission properly stressed the importance of strengthening individuals' control over their data as a primary objective (with the 'right to be forgotten' as an example on how to achieve this).[86] Furthermore, the opt-in/opt-out debate too should be nuanced[87] and more efforts should be made to increase transparency and uniformity.[88] Proposals such as enhancing data controllers' accountability[89] (implying a more effective control of the purpose limitation principle)[90] should be encouraged. Finally, a comprehensive revision on the meaning and relevance of

---

rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337 (Cookie Directive).

[84] In the form of an *expiry term*: "traffic data ... must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication".

[85] Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105 (Data Retention Directive).

[86] European Commission, 'A Comprehensive Approach On Personal Data Protection In The European Union' (n 7).

[87] On the negative impacts of a strict opt-in regime: NICKLAS LUNDBLAD & BETSY MASIELLO, 'Opt-In Dystopia's' (2010) 7:1 *SCRIPTed* 155. Among the negative consequences of an opt-in regime: exclusion and brake on social welfare; excessiveness; desensitisation (the overload of opt-in requests would make people care even less, which could in turn lead to a widening of the scope (scope creep) without much awareness on the part of the user); and balkanisation (a mandatory opt-in regime would disproportionately benefit services requiring account registration, which would increase lock-in issues and decrease user mobility).
OMER TENE frames it very well: "Consider what is a better expression of individual autonomy – signing a 36 page contract printed in font 6 which includes a hidden paragraph on data usage (opt-in consent); or receiving conspicuous, clear notice and being offered a simple, no cost right to refuse (opt-out)?" In: OMER TENE, 'For Privacy, European Commission Must Be Innovative' (*Center for Democracy & Technology*, 28 February 2011) <http://www.cdt.org/blogs/privacy-european-commission-must-be-innovative>.

[88] E.g.: By introducing 'EU Standard Forms'. See: European Commission, 'A Comprehensive Approach On Personal Data Protection In The European Union' (n 7).

[89] Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability' WP 173; European Commission, 'A Comprehensive Approach On Personal Data Protection In The European Union' (n 7); TENE, 'Privacy: The New Generations' (n 37), 12-13.

[90] See Art.6 *juncto* recital (28) of the DP Directive.

the 'personal data'-concept is necessary as well (*supra*).[91] In short, to ensure more effective privacy protection in the digital society, there is a lot to be done on many different fronts.[92]

RIGHT TO BE FORGOTTEN - Notwithstanding all the improvements mentioned above, there is still a blind spot in the current framework to which a well-defined 'right to be forgotten' would be a perfect solution. The right's scope of application should be limited to situations in which the data subject provided his or her unambiguous consent (art.7(a) of the DP Directive). All the other situations legitimising data processing in article 7 of the Directive (and in the ePrivacy Directive *juncto* Data Retention Directive) imply 'necessity' and are outside the free will of the data subject. In these cases, the law – at least in theory – is already clear on what should and can happen to the data. The current consent regime, however, almost always fails to offer true choice and control to data subjects (*supra*). A restricted 'right to be forgotten' could restore the balance by taking into account the dynamic nature of 'personal data' and allowing the data subject to adapt its position over time.

PUBLIC INTEREST EXCEPTION - As a safeguard against censorship and unwanted erasure of data, the 'right to be forgotten' should be limited by a 'public interest' exception.[93] This exception would cover, but is not limited to, the free speech issues in article 9.[94] To decide on its applicability, one could rely on a 'substantial relevance' standard (with regard to the personal data) and a proportionality test (with regard to the request for deletion). Undoubtedly, an Article 29 Working Party opinion on the 'public interest exception', especially with regard to its compatibility with art.7(e) of the DP Directive, would bring more clarity and lead to cross-border efficiency. But ultimately, it will be national judges and data protection authorities that decide on the exact scope of the exception. The burden of proof, as EU Commissioner VIVIANE REDING hinted already[95], should be on the data *controller*. Finally, it should also be emphasised that the exception only applies to actual personal data, which might be separated from other content it is part of. Translated into practice, this results in the following:

- X is an HIV patient and regularly posts lengthy and informative posts on a social medical website that requires users to identify themselves. After a while, the website becomes very popular and X wishes not to be associated with it anymore. The website could rely on the public interest exception and refuse to delete the posts in their entirety. A more proportionate compromise might be to only erase all identifying information (if not relevant).

- An individual uploading pictures of him or herself to a social network will have the right to have them removed retro-actively. The social network will have to prove a public interest if it wants to keep using them. In these cases particularly, the right is of great importance. Besides the obvious processing by/for the user him

[91] TENE, 'For Privacy, European Commission Must Be Innovative' (n 87). The author explains the futility of the 'personal, non-personal' dichotomy, by referring to de-anonymisation issues and the profiling of individuals without necessarily knowing their 'real' identities.
[92] For an overview of the Commission's ambitious plan of action, see: European Commission, 'A Comprehensive Approach On Personal Data Protection In The European Union' (n 7).
[93] An often repeated notion, especially in the DP Directive.
[94] This 'public interest'-exception may still be too vague and other formulations might be more suitable. Alternatively, one could consider, for example, 'compelling and legitimate grounds' (as mentioned in art.14 of the Directive). Such wording, though, would burden the data subject more heavily and could lead to inefficiency of the provision in practice.
[95] Commission, 'Your data, your rights: Safeguarding your privacy in a connected world' (16 March 2011) SPEECH/11/183.

or herself, the pictures (and other personal data) will be processed in all kinds of different ways and for different purposes (commercial, creating links with other data, etc.). In practice social networks will almost always comply with removal requests with regard to data processing by/for the individual (in other words, they will remove the data from the public eye upon request). Nonetheless, in many cases they will not irrevocably remove the data from their servers and continue to use it for their own purposes (to which the individual might have consented indirectly in the general terms and conditions).[96]

- An Ad Network collects personal data through the use of cookies. In light of the latest changes to the ePrivacy Directive[97], this data controller will have to remove data irrevocably upon request, *unless* (which would be incredibly unlikely *in casu*) the Ad Network can prove some sort of public interest in not removing the personal data.

THIRD PARTY SHARING - To prevent data controllers from avoiding the right's application by transferring the data to a third entity (with whom the data subject has no direct consent-based relationship), the 'right to be forgotten' should follow the data when voluntarily (and legitimately) shared by the original data controller. It also allows individuals to request the erasure of their data in large data mining companies that purchase personal data from other companies (e.g.: Acxiom) and to which data subjects might not have consciously consented. The public interest exception stays applicable and might be relevant in cases where the data is shared with (inter)national intelligence services combatting crime. The right cannot be invoked against a third party that copied personal data from the initial data controller, without any pro-active (nor illegal) behaviour of the latter.[98] These situations are already covered by regulation and depending on the specific facts, the data subject will have several ways of defending his/her privacy. One last example to illustrate the above:

- X is interviewed by a local school-newspaper about her clothing preferences. Google's web-spiders find the data on the school's local website and the interview turns up in their search-results. X discovers this and wants her data removed. She will not be able to request erasure from Google directly. Instead she will have to ask the school's newspaper to remove the article. The newspaper will have to prove public interest in case it refuses to take down the interview. When the interview is taken down (either because the newspaper complied with X's request or because it did not manage to sufficiently prove public interest), Google might (under certain conditions) become liable if it does not remove it from its servers.

---

[96] As mentioned *supra*, a data request from Facebook makes clear that they keep track off all your deleted information as well.

[97] The whole 'cookie-debate' that emerged out of the modifications to the ePrivacy Directive (in the so-called Cookie Directive) largely goes beyond the scope of this paper. For more information and to know the position of the Working Party, see: Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising ' WP 171, 13 *et seq*.

[98] Consequently, the 'right to be forgotten' - as described here - cannot be relied upon to request erasure from search engines' database. The issue was the subject of many cases recently launched by the Spanish Data Protection Authority. Spanish courts have referred the question to the European Court of Justice. See: SUZANNE DALEY, 'On Its Own, Europe Backs Web Privacy Fights' (*NYTimes*, 9 August 2011) <http://www.nytimes.com/2011/08/10/world/europe/10spain.html>. Also see: PETER FLEISCHER, '"The Right to be Forgotten", seen from Spain' (*Privacy...?*, 5 September 2011) <http://peterfleischer.blogspot.com/2011/09/right-to-be-forgotten-seen-from-spain.html>.

4 Conclusion

BALANCED APPROACH - The first chapter of this article gave a concise overview of the current debate on the 'right to be forgotten'. Whereas the right seems to give back control to individuals and constitutes some sort of 'check' on the data controller's behaviour, it became clear that the right has some important drawbacks as well. In its original form, the 'right to be forgotten' only comes *ex post*, conflicts with free speech (enabling subtle censorship), is very hard to effectively implement in practice and only postpones the illusion of choice. Consequently, the right should be toned down to be applicable only in certain well-defined situations. In an increasingly social Net, personal data disclosure is often a necessity today. And despite the rising awareness of individuals and efforts such as minimisation and anonymisation, data subjects still often disagree with unforeseen types of processing and/or simply change their mind. The current regulatory framework does not provide individuals with a satisfactory level of control over their data in the information society. A moderated 'right to be forgotten', therefore, seems an adequate translation into practice of the individual's acclaimed control-right.

FOCUS ON THE 'WHOLE PICTURE' - The second part analysed the right's potential implementation in a more concrete manner. It became clear that the impact of norms, the market or code alone are not sufficient to restore the control-balance and should be complemented by adequate legislative efforts. A brief examination of the current EU framework demonstrated the gap that currently exists, suggesting the merit of an actual 'right to be forgotten'. In the last part, a concrete proposal was made in which the right has a well-defined scope and includes an exception-clause to avoid any negative consequences a broader interpretation would entail. The 'right to be forgotten', therefore, should definitely not be 'forgotten'. Instead, a potential adoption of the right should be thought through thoroughly and not be the result of a panic reaction to the events of the day. The main objective should always be to give individuals a balanced control over their personal data. An adequate implementation of the 'right to be forgotten' will definitely contribute to a shift in the power balance, to the benefit of each and every individual in the information society.

International Fellow at the Electronic Frontier Foundation
Doctoral Researcher at the Interdisciplinary Centre for Law & ICT,
(University of Leuven)