

Information Privacy and the “Right to be Forgotten”: An Exploratory Survey of Public Opinion and Attitudes

In 2012, the European Commission proposed draft Data Protection Regulation which included the "right to be forgotten". This proposed right has been greatly debated. In this exploratory survey of public opinion in Ireland, it appears individuals want this "right to be forgotten" to be implemented. However there is scepticism as to how it will be implemented and ultimately whether it will be a success. The aim of this proposed right is to give users more control over their personal data. Individuals believe that placing an expiry date is a more feasible option than attempting to erase all online information if they request to do so. There is some ambiguity surrounding what this right would mean in practice. The survey also explores individual's attitudes toward information privacy. This article finds that individuals disclose a significant amount of personal information, feel they have little control over their information privacy and do not feel protected by current legislation.

1 Introduction

As part of draft new legislation on general data protection, the European Commission has proposed the inclusion of a “right to be forgotten”. Although this concept has attracted quite a lot of attention in recent years, it is neither new nor unique to a European context. In the United States, discussion about such a right can be traced back at least to the early 1970s¹, and indeed the notion of a “fresh start” is deeply embedded in American culture. Comparisons have been drawn with the means by which an individual’s record might be wiped clean within areas such as bankruptcy, law or juvenile crime. However, the EU and US have very different perspectives on the right to be forgotten. The current European proposal is being hotly debated on both sides of the Atlantic and has been argued to be not just a threat to the commercial interests of large US multinationals, but also to core values such as the freedom of expression and freedom of speech.^{2,3,4}

There is quite a degree of scepticism about the feasibility and enforceability of the “right to be forgotten”, were it to become part of European law. Considerable doubt hangs over how it might operate in practice. However, there is general acknowledgement that the balance of power between the rights of individuals and the interests of government agencies and commercial enterprises must be re-aligned so as to give individuals more control over how personal information about them is gathered and used. Initiatives such as the “right to be forgotten” and “Privacy by

¹ Jean-François Blanchette and Deborah G. Johnson, “Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness,” *The Information Society*, 18 (2002): 33–45.

² Steven C. Bennett, “The ‘Right to Be Forgotten’: Reconciling EU and US Perspectives,” *Berkeley Journal of International Law*, 30 (2012): 161-195.

³ Jeffrey Rosen, “The Right to be Forgotten,” *Stanford Law Review Online*, 64 (2012): 88-92.

⁴ Ambrose, M., & Ausloos, J. (2012). The Right to be Forgotten Across the Pond. Available at SSRN 2032325

Design”⁵ refute the mantra that “privacy is dead” and have as their core objectives the empowerment of individuals to preserve and restore their digital privacy. The “right to be forgotten” is based on the assumption that information will remain forever online without intervention⁶.

This paper reports the findings of an exploratory opinion survey recently conducted in Ireland of a non-random sample of 260 internet users. We sought to obtain a sense of how people feel about the proposed “right to be forgotten” and how it might be implemented. We also examined general attitudes and behaviour as regards online privacy. The sample surveyed considered themselves as relatively well informed about the issues asked. The authors’ academic discipline is business information systems so our interest is how privacy regulations impact the use, management, and development of technology. Ireland has particularly strong economic and cultural ties with the US, especially within the ICT sector, with most of the main US corporations having substantial activities based in Ireland. However, in the wake of recent revelations by former CIA and NSA employee Edward Snowden about transatlantic data transfers, Ireland has come under scrutiny from European leaders and digital rights activists for allegedly having a lenient data protection régime.⁷ Given Ireland’s important role as an intermediary between the EU and US, it therefore serves as an interesting test-bed of public opinion about the right to be forgotten.

This paper is organised as follows: Section 2 briefly reviews the literature surrounding the right to be forgotten. Section 3 outlines the research approach taken. Section 4 presents the findings of our study. Section 5 then concludes with closing remarks and future considerations.

2 Literature Review

Article 17 of the European Commission’s proposal for a General Data Protection Regulation, unveiled in January 2012, makes provision for a “right to be forgotten”, with special consideration being given to the treatment of personal information disclosed by children. Such a right would enable users to request their online data to be removed if it is not being held for a particular reason. There are some general exemptions, such as information held for historical, statistical and scientific research purposes, as well as legal records, information of public interest, and a number of other limited purposes. The right to be forgotten is also known as the “right to oblivion”. Both France and Italy have previously presented proposals for such a right

⁵ Ann Cavoukian, “Privacy by Design - Primer,” Information & Privacy Commissioner, Ontario, Canada, September 2013

⁶ Meg Leta Ambrose, “A Digital Dark Age and the Right to be Forgotten,” *Journal of Internet Law* 17.3 (2013): 1.

⁷ Derek Scally, “Merkel call for data protection rules puts Ireland in spotlight,” *Irish Times*, July 15, 2013.

to be introduced into legislation^{8,9} and the current proposal follows on from a French charter (“*Le Droit à l’Oubli*”) signed in 2010 by a dozen major companies, with the notable exclusions of Google and Facebook.¹⁰

The advantages of the right to be forgotten include giving data control back to the user while also keeping an eye on data controllers’ behaviour. The disadvantages include the challenge of how the right will be implemented in practice, what boundaries will be put in place and the resolution of the conflict between a right to be forgotten and the rights of free speech and freedom of expression¹¹. The United States Constitution does not clearly address information privacy. Instead information privacy is regulated through state constitutions based on type of information, industry and use¹². Two interpretations of the “right to be forgotten” have developed: the right to erasure and the right to oblivion. In the US, proposed deletion of information falls within the oblivion¹³ conception of the “right to be forgotten” while the proposed EU Data Protection legislation combines the concepts of oblivion and erasure¹⁴. However, some US laws have already imposed a limit on the length of time on which information can be held and/or reported by companies. The Video Privacy Protection Act requires businesses with information about subscribers not to be held for longer than two years¹⁵. The Cable Communications Policy Act requires written statements to be sent to subscribers once a year detailing what personal information the company holds on them, what it is used for and how it can be accessed¹⁶. The Fair Credit Reporting Act bans reporting on civil suits, tax liens and other derogatory facts after seven years¹⁷. In Turow et al’s study, there was a strong preference for a right to delete; of the American respondents, 63% prefer immediate deletion of data that marketers hold about them and 25% chose “a few months.” option. 92% percent want

⁸ Norberto Nuno Gomes de Andrade, “Oblivion: The Right to Be Different from Oneself. Reproposing the Right to Be Forgotten,” *Revista de Internet, Derecho y Política*, 13 (2012): 122-137.

⁹ Cécile De Terwangne, “Internet Privacy and the Right to Be Forgotten/Right to Oblivion,” *Revista de Internet, Derecho y Política*, 13 (2012): 109-121.

¹⁰ Alessandro Mantelero, “The EU Proposal for a General Data Protection Regulation and the roots of the ‘right to be forgotten’,” *Computer Law & Security Review*, 29 (2013): 229-235.

¹¹ Jef Ausloos, “The ‘Right to be Forgotten’ – Worth Remembering?,” *Computer Law & Security Review*, 28 (2012): 143-152.

¹² Ambrose & Ausloos, *op. cit.*

¹³ A right to oblivion would protect against reputation, identity, and dignity harms suffered by a user whose information has landed online and lingered longer than appropriate e.g. this has historically been applied to cases such as criminal activity (Ambrose & Ausloos, *op. cit.*)

¹⁴ A right to erasure shifts the power between data users and controllers and does not necessarily include an element of time e.g. deletion/erasure of information that a data subject has disclosed passively (Ambrose & Ausloos, *op. cit.*)

¹⁵ Video Privacy Protection Act Act, see: <https://www.govtrack.us/congress/bills/112/hr6671>

¹⁶ Cable Communications Policy Act, see: <https://www.govtrack.us/congress/bills/98/s66/text>

¹⁷ Fair credit reporting Act, see: <http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act>

a law requiring websites and advertising companies to delete all stored information upon request¹⁸.

2.1 Digital Surveillance and User Profiling

In his modern classic *Nineteen Eighty-Four*, which was originally published in 1949, Orwell depicted a society in which there was “no way of knowing whether you were being watched at any given moment ... You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.”¹⁹ The information age has stealthily ushered in the spectre of societal “überveillance” whereby the activities of citizens or consumers, depending on one’s perspective, can covertly be recorded and monitored as a consequence of the proliferation of mobile devices, digital sensors, and ubiquitous always-on networks amongst the general public. Every email, telephone conversation, SMS, tweet, photograph, social media status update, mouse click and internet transaction can potentially be captured by a myriad of systems, now increasingly interlinked through intelligent Web 2.0 cloud-based services. The “right to be forgotten” therefore addresses a problem of the digital age: how may a person escape their past? How can embarrassing incidents, moments of weakness, and personal failures be obliterated from the public eye? Whereas the human mind forgets or remembers selectively, the internet commits everything to memory.²⁰

It is possible with the current protocols for internet communication to record virtually every activity of an internet user, such as the data they receive and send and the users they communicate with. This extensive data collection is far more intrusive than was possible in previous eras. In traditional commercial relations, data is typically obtained only once a purchase occurs. However, on the internet, there are strong commercial incentives to deliberately subvert privacy. Many of the current business models are based on the concept of “one-to-one marketing” that require far more knowledge about individual preferences and buying habits than was previously available. Web sites commonly offer to “personalise” their display for users or ask extensive questions about a user’s interests before any commercial relationship has been established.

Currently, the generation and collection of personal data on a daily basis is immense. This has led to an inability to predict its uses and how it is stored and processed. The advances in electronic tools have progressed the storage, selection and retrieval of data. Proposed reforms to data protection legislation aim not to hinder or oppose technological development but to provide a basis for the technological improvements in order to re-balance the situation.²¹

¹⁸ Joseph Turow, Jennifer King, Chris J. Hoofnagle, Amy Bleakley, and Michael Hennessy, “Americans reject tailored advertising and three activities that enable it,” Working paper, September 2009, available at SSRN: <http://ssrn.com/abstract=1478214>.

¹⁹ George Orwell, *Nineteen Eighty-Four* (London: Penguin Modern Classics, 2009), 5.

²⁰ Rosen, *op. cit.*

²¹ De Terwangne, *op. cit.*

2.2 Voluntary Disclosure

The disclosure of personal information is sometimes viewed as "risky" behaviour which can violate a person's privacy²². Whatever about data that is covertly obtained, the amount of sensitive data that internet users *voluntarily* reveal online on a daily basis is alarming. For example, a person might willingly choose to share their home location and then broadcast on Facebook that their entire family is going on a foreign holiday for a fortnight, thus potentially leaving themselves open to becoming the victims of a burglary. On the other hand, one could take the position that there is excess paranoia about the "dark side" of the internet and that, on the whole, surveillance technologies help to make the world a safer place.

Walking away from the internet isn't an option for many people so they must be selective and cautious about what information they share. The decision to voluntarily provide data on-line can therefore be thought of as a form of "self-surveillance"²³.

However, not all on-line users are equally qualified to make this decision. In particular, children and young adults may in their naivety disclose sensitive information, not being fully aware of its unintended uses and consequences. This is especially the case with social networking sites, where younger users can feel under peer pressure to regularly share information about their social activities, physical locations, and likes. Social media sites are mechanisms by which users project an image of themselves to others. Younger users may feel a greater need to be seen in a positive light by their peers, thus giving rise to "self-enhancement" behaviour whereby the version that they choose to portray of their life is motivated by a desire to be admired by those within their network. They present partial truths because they manipulate the online identity they want their peers to see.²⁴ Young people may also be unsure where to draw the line between "public" and "private" spheres either due to their naivety or they feel these spheres are outdated concepts²⁵. There is something of a "privacy paradox" whereby people might voice their concerns about revealing certain personal data online, but then proceed to freely disclose that data online.²⁶ In their study of social networking and personal data security, Lang et al.²⁷ found that a lot of young people are openly publishing personal information of a sensitive nature; of the online profiles that they examined, over half contained photographs or other material of a potentially embarrassing nature. The key point here is that the type of

²² Alice E. Marwick, Diego Murgia-Diaz, and John G. Palfrey, "Youth, privacy and reputation", Berkman Center Research Publication No. 2010-5, Harvard University, 2010.

²³ H. Jeff Smith, Tamara Dinev and Heng Xu, "Data Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, 35 (2012): 989-1015.

²⁴ Jolene Zywica and James Danowski, "The Faces of Facebookers," *Journal of Computer-Mediated Communication*, 14 (2008): 1-34.

²⁵ Marwick et al., *op. cit.*

²⁶ Patricia A. Norberg, Daniel R. Horne and David A. Horne, "The Privacy Paradox: Personal Data Disclosure Intentions versus Behaviors," *The Journal of Consumer Affairs*, 41:1 (2007): 100-126.

²⁷ Michael Lang et al., "Social Networking and Personal Data Security: A Study of Attitudes and Public Awareness in Ireland," in *Proceedings of International Conference on Management of e-Commerce and e-Government* (Nanchang: IEEE Computer Society, 2009), 486-489.

information that persons choose to share on social media sites is very much dependent on the image they want to project of themselves to a certain community. In time, they may regret having revealed some of this information, were it to be allowed to persist. In addition to what might be regarded as naïve voluntary disclosure by children and young adults, there is also a possibility of users unwittingly disclosing information because of a lack of awareness. For example, by the act of sharing a photograph online, a person in addition to publishing an image might also reveal their exact whereabouts at a certain date and time (because of meta-data embedded within GPS-enabled digital cameras, smartphones and other location-aware devices). Thus unknown to a person, a profile of their physical movements could be built up over time, revealing a pattern of daily behaviour which not just violates their privacy but may also threaten their physical security (e.g. cyberstalkers). Similarly, by omitting to read online privacy policies, users might “voluntarily” grant permission to websites to track them through cookies or some other mechanism. Therefore an argument could be made that users should have the right to retract data that they unwittingly shared about themselves either by mistake or through ignorance.

2.3 Categories of Information

In a widely referenced internet article posted by Peter Fleischer, chief privacy counsel of Google, it was argued that the inherent conflict between “right to be forgotten” and the right to freedom of speech needs to be debated by reference to a coherent framework of concepts.²⁸ He proposed that the implications of a “right to be forgotten” need to be separately considered in so far as they apply to different categories of information. Fleischer suggested the following taxonomy, the categories of which have different consequences for the freedom of speech:

1. “If I post something online, do I have the right to delete it again?”
2. “If I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it?”
3. “If someone else posts something about me, do I have a right to delete it?”

In the view of Rosen²⁹, it is the third of these categories that most seriously infringes on free expression/speech. It leads into the debate on “consent” because in order to delete a posting made by another person, the permission of that other person may be needed. Another debate against the “right to be forgotten” involves viewing this right as a form of censorship³⁰. This proposed right will allow individuals to remove their personal information as they please which may result in the inaccessibility of important information³¹.

As we now enter the era of “big data” and advanced business analytics, we not alone leave behind digital “footprints” (i.e. data that we create about ourselves) as we traverse our way through online information systems, but also data “shadows” (i.e.

²⁸ Peter Fleischer, “Foggy Thinking about the Right to Oblivion,” Blog, March 9, 2011. <http://peterfleischer.blogspot.ie/2011/03/foggy-thinking-about-right-to-oblivion.html>.

²⁹ Rosen, *op. cit.*

³⁰ Fleischer, *op. cit.*

³¹ Ausloos, *op. cit.*

data generated about us by some other person or agent).³² Thus, substantially more data is created *about* an individual rather than *by* an individual nowadays. This is pertinent to the third question above because, notwithstanding the right to free expression, if some other body creates false or misleading information about you, should you not have the right to have it deleted? There are already provisions in existing European data protection laws to address this issue, but the proposed new legislation aims to strengthen and extend the rights of individuals in these regards.

2.4 Protection and Restoration of Personal Reputation

The issue of the right to be forgotten has arisen at this juncture in our history because we have now come to realise that the shelf-life of digital information is potentially everlasting, with unexpected long-term implications for a person's reputation.³³ The combination of vast digital storage, interconnected servers, and advanced search engines means that certain information which otherwise would have faded from memory continues to persist, and in some cases may have been resurrected (e.g. where previously inaccessible documents become available through digital archives). There arises the possibility that a person might be unfairly judged on the basis of some past actions, the record of which they cannot obliterate from the public domain.³⁴ Privacy campaigners have drawn attention to the danger of posting too much data online as to do so might be detrimental to one's career or personal relationships. Perhaps for the current generation of young internet users, the horse has bolted from the stable as regards internet privacy safeguards. Vast amounts of personal data have already been published online, hosted on remote servers in the sprawling domain of cyberspace. When the seal of privacy is broken, it may be impossible to ever restore it because information placed into the public domain cannot easily be suppressed or "forgotten". Whereas a few years ago, users may not have thought that a photograph posted on Facebook might affect their chances of finding employment, of late there has been an increase in the number of companies checking the social media profiles of potential job candidates. According to a report by Eurocom³⁵, "almost one in five technology industry executives said that a candidate's social media profile has caused them not to hire that person". The ethical dilemma presented here is aptly captured by Robert Frost in his poem *The Star-Splitter*: "If one by one we counted people out / For the least sin / It wouldn't take us long to get so we had no one left to live with. / For to be social is to be forgiving."

³² Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice," *SCRIPTed*, 8:3 (2011): 229-256.

³³ *Ibid.*

³⁴ De Terwangne, *op. cit.*

³⁵ Eurocom Worldwide, "One in Five Technology Firms Has Rejected a Job Applicant Because of Social Media Profile – Eurocom Worldwide Annual Survey," Press Release, March 15, 2012. <http://www.eurocompr.com/prfitem.asp?id=14921>.

2.5 Privacy Rights of Deceased Persons: “Digital Afterlife”

There have been a number of sad cases recently in Ireland, UK, and USA where incidents of cyberbullying have led to teenage deaths. To further exacerbate these terrible tragedies, some of the internet “trolls” whose hurtful comments initially caused the trouble then continued to post disrespectful posthumous messages on their victims’ social media profiles. Although these are extreme cases, they serve to draw attention to the more general issue of the privacy rights of deceased persons. Should the “right to be forgotten” apply only to living persons, or should deceased persons be given the dignity of having their on-line data erased if they or their relatives so wish? At the present time, deceased persons have very limited rights under data protection legislation across Europe and the proposed general regulation makes no specific provision to alter this situation.³⁶ However, the German Federal Constitutional Court ruled in its *Mephisto* that individuals have a right to posthumous personality protections³⁷. Persons who have departed this world may continue to have a living, active presence in the world of online social media. If their relatives don’t have the passwords to their accounts, they remain open and on-line “friends” may continue to receive automated messages and reminders or even be prompted, rather eerily, to “re-connect”. Some service providers will shut accounts down after a period of inactivity, whereas others will remain active unless a relative of the deceased makes contact in writing, providing proof of death and personal relationship. Of late, some companies have started to offer services (e.g. Google Inactive Account Manager) whereby users can specify in advance what should happen to their “digital remains” e.g. send it to a friend, erase it entirely, or preserve it. The debate about the “right to be forgotten” and preservation of the dignity of deceased persons has only begun to attract interest relatively recently but is a growing area. There is also a fraud prevention aspect here: appropriate controls must be put in place to prevent the identity of a deceased person being stolen. It has been reported that each year in the US, the identities of nearly 2.5 million deceased persons are fraudulently used to open credit card accounts and apply for other services.³⁸

2.6 Implementation of the “Right to be Forgotten”

The initial draft of the proposed legislation leaves a lot open to interpretation as to how it might be implemented and there are concerns that it will fail to deliver on expectations.³⁹ Proposed solutions include Privacy by Design (PbD), the use of expiry dates, “self-destruct” mechanisms, manual deletion of data, and digital rights

³⁶ Edina Harbinja, “Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?,” *SCRIPTed*, 10:1 (2013): 19-38.

³⁷ Hannes Rösler, “Dignitarian Posthumous Personality Rights-An Analysis of US and German Constitutional and Tort Law,” *Berkley Journal of International Law*, 26 (2008): 153-205.

³⁸ Martha C. White, “Grave Robbing: 2.5 Million Dead People Get Their Identities Stolen Every Year,” *TIME Magazine Online*, April 24, 2012. <http://tinyurl.com/ocpss3>.

³⁹ Rolf H. Weber, “The Right to Be Forgotten: More Than a Pandora’s Box?,” *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2 (2011): 120-130.

management (DRM).^{40,41,42} Ironically, the right to be forgotten may necessitate a need for more personal data to be recorded because in order to be able to delete information about a person, it shall be necessary to associate that information with an identifiable person, which may mean increased personal meta-data embedded within media objects such as photographs, videos, and documents. In order for more internet users to control their personal information online, there is a need for these users to become more experienced with privacy-protecting technologies⁴³.

The “right to be forgotten” is a particularly daunting challenge for business owners. In practice, a business is unlikely to have effective control over data that has been copied and re-published by others. How far would be deemed reasonable for a business to go as regards pressing third parties to erase this data?⁴⁴

The Centre for Democracy and Technology in the European Network and Security Agency (ENISA) has criticised the proposed legislation as being not feasible, impractical and ultimately counterproductive for consumers. ENISA has called for it to be the “right to erase” data that a user has himself shared with online service providers rather than a right to be forgotten as the latter would be extremely difficult to police on an open internet.⁴⁵ At present, a number of internet sites permit users to submit “take-down” requests, such as Google Streetview (where parts of scenes can be obfuscated), Facebook (where content can be taken down if it is of a graphic nature)⁴⁶, and South Africa’s Internet Service Providers Association⁴⁷. According to Google’s Transparency Report, the highest reason for government/court take-down requests is defamation (39%), followed by privacy and security (18%).⁴⁸ Additionally, Google now typically receives of the order of four to five million URL removal requests each week from copyright owners, a twenty-fold increase on the typical volumes of early 2012.⁴⁹ If, - in addition to governments, courts, and copyright holders, - private individuals were to be given legal privileges to request content take-downs, the volume of requests might rise to such levels that corporations would likely engage in push back tactics.

⁴⁰ Koops, *op. cit.*

⁴¹ European Network and Information Security Agency (ENISA), “The Right to be Forgotten – Between Expectations and Practice.” <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten>. November 2012.

⁴² Chris Conley, “The Right to Delete,” in *Proceedings of AAAI Spring Symposium: Intelligent Information Privacy Management* (Stanford University, CA, USA, March 22-24, 2010).

⁴³ Joseph Turow, *Americans & online privacy: The system is broken*, Annenberg Public Policy Center, University of Pennsylvania, 2003.

⁴⁴ Sally Annereau, “Are new data protection proposals for a ‘right to be forgotten’ workable?,” *The Guardian*, April 22, 2013. <http://www.guardian.co.uk/media-network/media-network-blog/2013/apr/22/data-protection-right-to-forgotten>.

⁴⁵ ENISA, *op. cit.*

⁴⁶ BBC News, “Facebook makes U-turn over decapitation video clip,” October 23, 2013. <http://www.bbc.co.uk/news/technology-24635498>

⁴⁷ See <http://ispa.org.za/code-of-conduct/request-a-take-down/>

⁴⁸ See <http://www.google.com/transparencereport/removals/government/>

⁴⁹ See <http://www.google.com/transparencereport/removals/copyright/>

3 Research Method

Data was collected using a Web-based questionnaire during the months of August-September 2013. The survey instrument contained 24 questions, the majority of which were either Likert scale items or checkboxes, with a number of open-ended comment textboxes also included. There were four main groups of items on the questionnaire, relating to: (1) general demographic variables; (2) attitudes towards the right to be forgotten; (3) attitudes towards online privacy; and (4) perceived online risks, safeguards and controls. A number of the questions were adapted from survey instruments previously published in the literature.

To pilot test the Web-based questionnaire, a “soft launch” was conducted whereby a selection of colleagues with domain knowledge and questionnaire design expertise were invited to participate in a trial run and provide feedback on any issues that might cause problems or confusion. In response to this feedback, a number of enhancements were made to the questionnaire before it was fully launched.

A combination of two non-probability sampling techniques was used, namely “snowballing” and convenience sampling. Participants were solicited through personal messages sent via LinkedIn, Twitter, and Facebook. As our population of interest was not the general public as a whole but rather those who have some level of awareness of the “right to be forgotten” and online privacy issues, the use of social media to attract respondents and the use of a Web-based instrument to collect data are methodologically justifiable. Although it may have been better if the sample was randomised, for practical reasons it was not possible to do so. Nevertheless, we have confidence that the 260 persons who responded provide us with a strong indication of opinion amongst our population of interest because of the high number of responses received and the demographic spread.

Respondents ranged in age from 17 to 61, with a mean of 29 years. For the purposes of testing for differences of opinion amongst persons of different age, we split the data into four age groups roughly corresponding with the interquartile breakpoints (17-23, 24-26, 27-32, and 33+). The gender split was uneven, being 59% female and 41% male; this ratio varied considerably across the age groups, with only the 33+ group having a balanced mix. As regards nationality, the 260 respondents came from 14 different countries, regionally distributed as follows: Ireland (212: 82%), Other EU (32: 12%), North America (12: 5%), and Asia/Middle East (4: 5%). The majority (74%) of respondents were in employment, with students making up 17% of the sample, jobseekers 5%, and retired persons/others 4%.

Across all age groups, the respondents have levels of internet experience commensurate with their age. In the upper age group (33 yrs+), 88% have used the internet for more than 10 years. In the youngest age group (17-23), 71% are internet users for less than 10 years. The most commonly used devices to connect to the internet are laptops (87%) followed by smartphones (81%). This finding is notable because of the additional privacy issues associated with mobile devices. Less than half of respondents access the internet through PCs. The use of smartphones is more pronounced amongst the younger age groups, with an apparent substitution effect visible in the 24-26 and 33+ age groups where laptops and tablets take over.

The questionnaire data was analysed in SPSS using descriptive statistics, cross-tabulations, and non-parametric tests of correlation (Spearman's rho, hereafter abbreviated as r_s) and tests for differences (Mann-Whitney, Kruskal-Wallis).

4 Discussion of Findings

4.1 Attitudes towards the “Right to be Forgotten”

Although our sampling strategy deliberately targeted an Internet-savvy computer-literate population, 39% of them admitted to having very little or no knowledge of their online privacy rights. When we compared responses across age brackets, we found that the 27-32 group were most informed, with a statistically significant cohort saying that they have considerable knowledge about their rights ($p < .05$). We surmise that this may be because they have arrived at a point in their professional and personal lives where online privacy has become more of a priority than it may previously have been. Significant differences ($p < .01$) in privacy awareness were also found when comparing respondents from different regions; non-Irish EU respondents claimed to know more about their rights than those from all other regions. Of those who felt they had sufficient knowledge to hold an opinion, 37% ($n=178$) felt that existing legislation provides no protection at all against violation of on-line privacy, and 63% ($n=189$) believe that they have no effective legal protection against reputational damage caused by social networking sites.

Overall, respondents in this study agreed that persons should not always be judged on the basis of past behaviour, and were very strongly of the view that the “right to be forgotten” should be implemented into legislation (99% in favour). When presented with Fleischer's three categories of on-line information and asked for their opinions about how such a right might apply, (1) 86% indicated a belief that a person should have a right to erase data provided about oneself by oneself, (2) 82% felt that information about a person provided by others should also be subject to erasure upon request, and (3) 86% expressed the opinion that personal information originally provided by an individual, which is subsequently copied and re-circulated by another person, should be liable to be taken down.

These findings reveal an overwhelming endorsement of the right to be forgotten amongst our target population of internet users in Ireland. The reasons for this can partly be explained by reference to the results of a question that asked respondents about their perceived ability to exert control over how their online personal information is currently used. 60% of respondents felt that they presently have little or no control to correct inaccurate or untruthful information about themselves, and 59% believed they have little or no control to remove embarrassing or damaging information posted on the internet. Further insights were provided by open-ended comments, such as the following indicative selection of remarks:

“As we are freely able to supply personal information at our discretion, we should also be able to remove personal information which appears online at our discretion.”

“I feel you should have the right to request an organization to remove all your personal information from its systems. Also, the process for doing this should be designed in such a way as to not put barriers in the way of people who wish to make this request.”

“I want to be in control over the amount of personal information [about me] that people have access to. If I really think about it, we are all put in a very vulnerable situation with the amount of information available ... I am concerned that I may be subjected to on-line subliminal advertising specifically geared towards me because of the private information that is so readily available”.

“In a world where "cyber bullying", "trolling" and digital crime is growing, more should be done to protect the privacy of users. Mistakes can be made, and if someone accidentally or intentionally reveals more information about themselves or others, then they should have the right to retract the details, especially if one's living condition or state of mind will be affected.”

However, there were also a number of dissenting opinions against the implementation of the right to be forgotten:

“It would be a waste of time in my opinion to go down this road. We live in an age of shared information, for better or worse. The only control we now have is to live a life where we have no need to worry what about us is shared / No skeletons in the cupboard.”

“I feel that Internet users should take their own responsibility in what they disclose on the Internet. If they don't want personal information to be used against them, don't disclose it.”

What is also notable is that, although nearly everybody wants to see the right to be forgotten enacted into law, only two-thirds of the respondents believe it will actually be a success. Amongst the reasons cited for believing it would not work are the following:

“I do believe individuals should have the right to remove their personal information from sites/databases ... However, the ability of the site/database owners to identify individuals who want their information erased and then successfully erase all traces of it after it was previously stored/used seems rather doubtful at the least, and extraordinarily costly if it is actually possible.”

“The government's ability to implement such legislation has been found lacking in previous cases so I would have no confidence in their ability to implement and monitor [this new legislation].”

“There is no way in reality it is workable to enforce a law to require companies to remove information about you on a whim. The information itself might be indexed and copied to countless sites. The overhead and appeals process would probably cause a massive workload and ultimately be a failure. If implemented, ‘Right to be Forgotten’ would simply spawn businesses who harvest data forever, outside of western jurisdictions.”

The majority (87%) of respondents accept that it is not easy to erase personal information online, and 84% believe that placing an expiry date on information disclosed online would be a more feasible option than attempting to erase all information.

4.2 Attitudes towards Personal Privacy

When asked about the amount of personal information they reveal online, 32% of respondents indicated that they disclose nothing or only a small amount, with a further 58% saying they release “only what I have to”. On the face of it, it appears that the 17-23 age group are less zealous than the other age groups as regards keeping personal information to themselves, but this difference is not statistically significant. Also, contrary to our expectations, no significant differences were found between males and females in this regard. In a separate question that explored the reasons for withholding personal information, 74% of respondents either agreed or strongly

agreed with the statement “I tend to reveal minimal personal information about myself online because I value my rights to privacy”.

We found in our study a negative correlation ($r_s = -.401$, $p < .001$) between a person’s perceived online safety (“*I feel safe publishing my personal information online*”) and their level of apprehension about disclosure (“*I feel uncomfortable about my personal information being in the hands of others*”), which suggests that those who are not anxious about their personal data being accessible by others feel so because they see no major threat, and vice versa. As it turned out, 66% of respondents indicated that they do indeed feel uncomfortable about their personal data being in the control of others. More specifically, 72% would be bothered if third parties were to maintain a history of their online activities and movements, and in this regard females were found to be more concerned than males ($p < .05$).

Returning to Fleischer’s three information categories, it is of note that 22% of our sample had no fears at all that online information shared with friends might be inappropriately disclosed by their friends to others, with 51% being only slightly concerned. This reflects a high level of trust in friends. However, the same cannot be said of trust in others or trust in online companies. 39% were either very or extremely concerned that other Facebook users might abuse their personal information, and 58% were either very or extremely concerned that online companies might divulge their information to other parties without their explicit consent.

As regards preferences for how personal online profiles and “digital remains” should be treated in the event of one’s death, the majority (53%) of respondents would rather for their accounts to be closed down due to inactivity. Only 20% want their profile to remain available for others to see.

4.3 Perceived Levels of Risk and Control over Personal Data

Control is a critical element that underpins the right to be forgotten because it aims to give users control over their online personal data.

We found an interesting relationship between perceived level of control and the incidence of adverse experiences. The more control that respondents feel they have over their online privacy, the less chance they have ever been the victim of online fraud ($r_s = -.136$, $p < .05$) or had an unpleasant experience as a result of an online disclosure ($r_s = -.154$, $p < .05$). This can be looked at in opposite ways. It may be that people feel they are in control because nothing unfortunate has yet happened to them, or alternatively it may be that nothing bad has happened because they are genuinely in tight control.

As regards adverse online incidents, 39% had been subjected to privacy violations of some kind, while 20% indicated that their personal reputation was damaged as a result of material posted online. When asked about the probability of reputational damage arising either from a person’s online information being accessed by unintended persons (e.g. employers, teachers) or being used to spy / cause embarrassment, opinions were divided. Upon running a Kruskal-Wallis test, we discovered that those in the 33+ age group see themselves as considerably less likely to be damaged in this way, whereas the younger age groups are more fearful ($p < .05$). This may be because the older age group are not Facebook / Twitter users to the same extent, perhaps have

not disclosed as much potentially embarrassing information about themselves online, or maybe have simply become less self-conscious about such matters with age. The less control a person has over their privacy online, the more uncomfortable they feel about information being in the hands of others ($r_s = -.162, p < .05$). As expected, those who feel they have the least control are also the most concerned that other internet users might abuse their personal information ($r_s = -.167, p < .01$), online companies might divulge their information to other parties without explicit consent ($r_s = -.178, p < .01$), or on-line companies might use their information for purposes other than stated in the privacy policy ($r_s = -.151, p < .05$). The level of an individual's perceived control over privacy is also correlated with the amount of information they choose to disclose. The more they reveal, the less control they feel they have over their ability to prevent their data from being used by online companies in unintended ways ($r_s = -.137, p < .05$). This is interesting because it suggests that people are giving away their information in the knowledge that they are sacrificing control. It may be that they are happy to do so in the expectation of receiving enhanced online services on the basis of "value exchange"⁵⁰, but it may also be because they feel compelled to do so in order to avail of fairly normal functionality. As one respondent commented:

"It seems that in order to use the internet to its fullest you need to click 'Yes' that you agree to provide certain information under the terms and conditions of use. If you click 'No', access is generally denied for that particular website. So if you wish to use Amazon, Google, Gmail, Facebook or any of the big hitters, you have to divulge a certain amount of personal information."

5 Conclusions

Many would like to see the "right to be forgotten" entered into legislation but scepticism surrounds how this might work in practice. Does society need to preserve what is on the internet for historical context, or should much of today's content explosion be regarded as ephemeral and transferred into the digital dustbin? The right to be forgotten would enable a person to generate a clean slate, released of the fear that compromising information recorded online might hover over them for the remainder of their lives. However this will not be easy to implement because information systems have not traditionally been designed to forget. EU Commissioner Viviane Reding has expressed the view that the "right to be forgotten" legislation needs to stand the test of time so as to be able to accommodate new waves of future technologies that we have not yet countenanced.⁵¹ Therefore, information systems developers need to radically change the way that systems are designed and built, and university educators need to change the graduate curriculum. The intent of the *Privacy by Design*⁵² approach, which in October 2010 was recognised as a global privacy standard by the International Conference of Data Protection and Privacy

⁵⁰ Weber, *op. cit.*

⁵¹ Matt Warman, "EU Privacy regulations subject to 'unprecedented lobbying'," The Telegraph, February 8, 2012. <http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html>

⁵² See <http://www.privacybydesign.ca>

Commissioners, is that fundamental privacy requirements should be embedded into systems from the outset. For legacy systems, these same principles inform the *Privacy by Redesign* approach.

Particular attention must be given to the modern “digital natives” generation who have grown up in a society surrounded by ICT. Should society turn a blind eye towards youthful carelessness, or will this generation feel pangs of regret when they attain job-seeking age? We agree with the sentiment expressed by one of our respondents that:

“Privacy awareness should be thought in schools, especially with the explosion of social media, the risks involved in divulging information about yourself, and the consequences of cyberbullying. Even if this type of legislation is passed, it won't stop young people making mistakes.”

Some evidence emerged that young females are more vulnerable than males. Females are more concerned about the level of protection of their privacy and reputation afforded by current legislation. This may be because they care more about perceptions formed about them on the basis of information posted online, tend to engage in social media to a larger extent than males, and are not always treated equally in society as regards behavioural norms in comparison to males. Our findings are in contrast with Turow et al's study, in which it was found that regardless of the fact that their respondents were the victim of adverse experiences and feel they have no control over their personal information online, they still feel that businesses and laws do in fact protect them⁵³.

Our results are in agreement with Turow's study where 80%+ feel they have little/some control over how their online information is used⁵⁴. Harris-Westin developed a segmentation grouping of individuals based on their perception of privacy issues. *Privacy Fundamentalists* are those who believe there is a need for privacy. Individuals who are seen as *Privacy Unconcerned* believe there is no need to be concerned about privacy⁵⁵. The remainder other than these two groups are *Privacy Pragmatists*. Interestingly, in Tufekci's study of 700 college students, no relationship between concern for privacy and information disclosure on social network sites was found, because the students surveyed instead managed audience concerns through privacy settings and using nicknames⁵⁶.

With the European Parliament considering proposals to reform data protection law for 27 member states, implementation and compliance will be difficult as no one size fits all. We hope that this paper can make a useful contribution by informing policy makers of the current state of public opinion in regard to the right to be forgotten debate.

Note: On October 21st 2013, the LIBE committee of the European Parliament approved the compromise text of the proposed EU General Data Protection Regulation. This text contained the amendment that the "right to be forgotten" has been replaced by the "right to erasure" which

⁵³ Turow et al., *op. cit.*

⁵⁴ Turow, *op. cit.*

⁵⁵ Alan F. Westin, “Social and political dimensions of privacy,” *Journal of Social Issues*, 59:2 (2003): 431-453.

⁵⁶ Zeynep Tufekci, “Can you see me now? Audience and disclosure regulation in online social network sites,” *Bulletin of Science, Technology & Society*, 28:1 (2008): 20.

requires that any data subject has the right to have their personal data erased upon request. If the data controller is asked to erase such data, this company should also forward this request to others companies whom also have this data⁵⁷.

⁵⁷Hunton & Williams LLP, "European Parliament Approves Compromise Text on Regulation", Blog, October 21st 2013, Available: <https://www.huntonprivacyblog.com/2013/10/articles/european-parliament-approves-compromise-text-on-regulation/>