THE RIGHT TO BE FORGOTTEN

THE RIGHT TO BE FORGOTTEN

Joy Liddicoat[1]
Office of the Privacy Commissioner
Wellington

Introduction

This paper explores the "right to be forgotten". The term became widely used in an attempt to capture the ratio decidendi of the Court of Justice of the European Union (ECJ) ruling on 13 May 2014. This ruling required the search engine Google to remove, upon request, specific online search results which included personal information. The ruling strongly divided legal, technical, private sector and civil society stakeholders. Many predicted diametrically opposed and equally certain legal consequences. But what is this legal concept? How does it relate to the right to privacy and how, if at all, is this relevant to New Zealand? The Office of the Privacy Commissioner has not developed a final view on this topic. This paper therefore simply outlines the concept of this so-called 'right to be forgotten' and critically analyses its implications for New Zealand. An update of recent developments including from the European Data Privacy Commissioners art 29 Working Party and wider policy implications is also provided.

What are the origins of this emerging right?

The phrase "the right to be forgotten" existed well before the 2014 Court ruling. Data regulators, civil society groups and others were articulating a "right to be forgotten" as early as 2006, linking it to well established principles of what the French called the right to oblivion and those in the United States of America called "practical obscurity". The concept quickly caught on with Internet law commentators and came to the attention of European privacy and data law makers.

In early 2012, for example, the European Union was debating the implications of new technologies, including the Internet, and the application of data protection laws online. Vice President of the European Commission, Vivean Reding, signalled that EU data protection reform, which was well overdue, should include provision for removal of online personal information:[2]

> Another important way to give people control over their data: the **right to be forgotten**. I want to explicitly clarify that people shall have the right – and not only the 'possibility' – to withdraw their consent to the processing of the personal data they have given out themselves. (emphasis in original document).

[1] Acknowledgements: I am grateful to assistance from Tim Henwood, at OPC and also to Judge Harvey for the useful resources at: DJH: http://www.cambridge-code.org/googlespain.html

[2] Viviane Reding, Vice President, Eur. Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5 (Jan. 22, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF at p 5.

Emphasising, that this 'right to be forgotten' was not an absolute right, the Vice President went on to say:[3]

> There are cases where there is a legitimate and legally justified interest to keep data … The archives of a newspaper are a good example. It is clear that the right to be forgotten cannot amount to a right of the total erasure of history. Neither must the right to be forgotten take precedence over freedom of expression or freedom of the media.

This European legal view of the "right to be forgotten" (being based on privacy and data protection laws), was (and remains) in stark contrast, indeed fundamentally different from, the legal positioning of the United States of America. The US legal position was founded in constitutional protection of free speech, with online companies (and various other US based Internet groups and stakeholders) viewing any removal or deletion of online information as a prima facie violation of freedom of expression.[4] These opposing views were well known and were just a small part of a wider global debate on internet governance playing out among and between governments, the private sector, civil society and the technical and academic communities at the time of the ECJ ruling. Courts in other countries, such as Argentina, had also made rulings requiring deletion of search engine results.

What is the right to be forgotten and how does it relate to the right to privacy?

Briefly, the facts and legal basis of the case were as follows:[5]

> On 5 March 2010, Mr Costeja González, a Spanish national resident in Spain, lodged a complaint with the Spanish Data Protection Authority, AEPD, against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) ('La Vanguardia'), and against Google Spain and Google Inc. The complaint was based on the fact that, when Mr Gonzales searched for his name using the Google search engine in 2009, two prominent results appeared relating to home-foreclosure notices from 1998, when he was in temporary financial trouble. The notices had been published in Spanish newspaper La Vanguardia and recently digitised en masse online. The results contained links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.
>
> Mr González requested, first, that La Vanguardia be required either to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. Second, he requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that these were no longer included in the search results and no longer appeared in the links to La Vanguardia. Mr González stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant.

---

3 Ibid.

4 For a useful overview see, for example, Professor Jeffry Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. 88 available online http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

5 Google Spain and Google Inc v Agencia Espanola de Proteccion de Datos (AEP) and M C Gonzales 13 May 2014, available at: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d50cc57fb6d9ae4925aff5d9bbd76b8b00.e34KaxiLc3eQc40LaxqMbN4Ob3uSe0?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=102488

> In July 2010, the AEPD rejected the complaint in so far as it related to La Vanguardia, taking the view that the publication by it of the information in question was legally justified - it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to an auction in order to secure as many bidders as possible.
>
> However, the complaint was upheld in so far as it was directed against Google Spain and Google Inc. The AEPD considered operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and also act as intermediaries in the information society. The AEPD took the view that it had the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considered that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense. The AEPD took the view that this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to erase the data or information from the website where this appears, including when retention of the information on that site is justified by a statutory provision as was so in this case.

The case was taken on appeal before the Spanish National High Court, which stayed proceedings in order that certain legal questions on the interpretation of EU Directive 95/46, on which the relevant Spanish laws were based, could be put before the ECJ. The Spanish, Polish, Italian and Austrian Governments as well as the European Commission also joined the action and were heard on legal arguments relating to interpretation and application of the EU Directive.

In May 2014 the European Court of Justice upheld the AEPA decision and ruled that Google Inc Spain should break links to the old newspaper stories about Mr Gonzalez's debt. [6] The decision was based on European privacy law, including access to data and the right to correction. The Court of Justice of the European Union (ECJ) concerns (1) Territoriality of EU rules, (2) applicability of EU data protection rules to a search engine and (3) Right to be forgotten (RTBF).[7]

The court held:

(a) Activities of a search engine did fall within the EU law definitions of 'processing of personal data'.

(b) The AEPA had jurisdiction to apply data protection laws to the activities of the search engine in the case in question.

(c) Google was obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

(d) The rights related to a request for delinking of search engine results override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his or her fundamental rights is justified by the preponderant interest of the

[6] Ibid.

[7] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

> general public in having, on account of its inclusion in the list of results, access to the information in question.

Google moved swiftly to implement the ruling and to limit its ambit to those countries falling within EU jurisdiction.

While the case has been given some wide-sweeping publicity and commentary on the so-called "right to be forgotten" it is in fact a limited and quite specific decision and does not establish a general right to be forgotten. Nor does implementation of the ruling have the effect of "forgetting" information about a person. It simply requires Google to remove links returned in search results based on an individual's name when those results are "*inadequate, irrelevant or no longer relevant, or excessive.*" Google is not required to remove those results in all cases – in particular, if there is an overriding public interest in them "for particular reasons, such as the role played by the data subject in public life."[8]

In this case, Google accepted the ECJ decision and responded by making available a form for EU citizens to complete to request a breaking of links to material they consider to breach the relevance principle.

What are the likely implications for New Zealand law?

There are no Human Rights Review Tribunal cases directly on the question of the right to delink search engine results, nor directly on the right to be forgotten.

However, in an interim decision in *Hammond v Credit Union Baywide*, the Tribunal did reference the concept of the right to be forgotten.[9] This judgment related to an interlocutory proceeding on the question of publication by the news media of a screen shot of a photo on the complainant's private Facebook page, which had subsequently been downloaded by her employer.[10] That case is probably worthy of a separate discussion, but what is very relevant for the purposes of this paper is that the Tribunal noted that the lack of a right to be forgotten was a factor supporting an order for non-publication by the media. The Tribunal noted:

> It is relevant that once the image of the cake is released into the public domain via the media, that image will be, to all intents and purposes, indelible. The saying is that a picture is worth a thousand words. *In this day and age Ms Hammond is at risk of being forever associated with that image. We must recognise that at the present time there is no clearly established right under New Zealand law to be forgotten.* (emphasis added).

This lack of protection therefore clearly weighed in the Tribunal's mind and it remains to be seen if this is relevant in any other media publication cases.

In general terms, Privacy Commissioner John Edwards made it clear in 2014, shortly after the ECJ ruling, that OPC does not have a position on the right to be forgotten and wants

---

8 At Para 94, the Ruling.

9 *Hammond v Credit Union Baywide* (In-Court Media Application) [2014] NZHRRT 56 (2 December 2014) http://www.nzlii.org/nz/cases/NZHRRT/2014/56.html at para 7.5.

10 The final judgment *Hammond v Credit Union Baywide* [2015] HRRT 6 (2 March 2015) is available at: http://www.justice.govt.nz/tribunals/human-rights-review-tribunal/decisions-of-the-human-rights-review-tribunal/html-decisions-and-headnotes/2015/hammond-v-credit-union-baywide-2015-nzhrrt-6

to hear the variety of views.[11] That remains our position and the last year has not shown any pressing need to address this issue in New Zealand.

Perhaps this is because New Zealand law also differs from European law in significant ways, for example there is no concept of "data controller" or "data processor" as well as other legal differences. Perhaps also, it is because while there may not be a right to be forgotten in New Zealand, there is a wide range of other mechanisms that, put together, provide a strong basis for ensuring personal information can be corrected. The Privacy Act provides a right to request correction of information and to include a statement of asserting why information is disagreed with if a correction is not made. For example, Privacy Act Principle 8 states:

> An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

The obligation in this Principle applies not only at the time information is collected, it is also a continuing obligation.

Whether in any given case a New Zealand regulator had jurisdiction over an internet search engine's activities would also remain to be seen. Similarities with the New Zealand situation in relation to Google are strong and echo aspects of the ECJ facts. Google is established in New Zealand for tax law purposes, and has a small local business established for marketing services to New Zealand businesses involving New Zealand customer information (thereby monetising the New Zealand search functionality). If we accept the logic of the European court, that makes it sufficiently established here and might also apply to other search engines that are similarly established here. However, it is very important not to single out any particular company, nor to pre-determine any particular case.

In addition, s 14 of the Privacy Act requires the Commissioner to have due regard to:

> …the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way.

This is a careful balancing exercise.

OPC prefers to, and has a history of, working through issues in a principled way as they arise. For example, in 2010 OPC conducted an inquiry into Google's collection of wifi information in the Street View Wi-Fi sniffing case.[12] That was a very obvious example of an activity in New Zealand, involving information about New Zealanders. We concluded that although Google had a legitimate reason for collecting the openly accessible WiFi information, it failed to properly notify the New Zealand public about that collection, and the collection was unfair. We also concluded that Google had breached the Privacy Act when it collected payload information (the content of communications) from unsecured networks. It had no legitimate reason for that collection, and the collection was seriously intrusive. To its credit, Google acknowledged for several months that it made serious mistakes, particularly in collecting the payload information and worked with our Office,

[11] John Edwards, "A right to be forgotten in New Zealand?"1 July 2014, available at: https://privacy.org.nz/blog/right-to-be-forgotten/

[12] https://privacy.org.nz/news-and-publications/commissioner-inquiries/google-s-collection-of-wifi-information-during-street-view-filming/

including making a number of undertakings about future product development and deletion of the relevant data.

A further factor in the New Zealand context is the scope for any common law or Bill of Rights Act action. The tort of privacy in New Zealand includes the concept that privacy can "grow back" over what was previously publicly available information. See, for example, the case of *Tucker*[13] where a man seeking "crowdsourced" funding for a heart operation was found to have been convicted of sexual offences earlier in his life. He sued to prevent the disclosure of that information. He obtained an interim injunction, but was ultimately unsuccessful, because media outlets not affected by the interim order ran the story before his full case could be heard. The Court nonetheless laid the foundation for the tort of breach of privacy, with the implication that it could exist even in relation to information that had previously been publicly available.

A range of other existing or proposed laws are also relevant to the deletion of personal information. The Harmful Digital Communications Bill will allow a court to make an order against online content hosts to take down or disable public access to material, an order to publish a correction or to provide a right of reply, and an order to release the identity of the author. Clause 20 also creates a broad safe harbour for online content hosts protects, protecting them from any civil or criminal liability for the content of digital communication they host if they follow a notice, notice, takedown procedure.

Section 92C of the Copyright Act provides a safe harbour that internet service providers are not liable for storing infringing material unless they are aware the material infringes copyright and do not delete the material or prevent access to it as soon as possible after becoming aware of the infringing material (eg by notice).

The Films, Videos, and Publication Classification Act 1993 contains a police power to seize restricted publications or films under s 107 and objectionable publications under s 108. The Court can order the destruction of an objectionable publication (s 116) and make orders for disposal and forfeiture following a prosecution.

Under the Harassment Act 1997 the court has the power to impose special conditions (s 20) on restraining orders – this could extend potentially extend to take-down of material that constitutes harassment. An amendment is pending that would make it a condition of every restraining order that applies to a continuing act of harassment such as the posting of offensive material in any electronic media, that the person against whom the restraining order is made must take reasonable steps to prevent the specified act from continuing. This could include steps to take-down or disable access to published material that is the subject of the restraining order.

Remedies that may be granted by the Human Rights Review Tribunal where it is satisfied on the balance of probabilities that the defendant has breached the anti-discrimination provisions of the Human Rights Act include an order restraining the defendant from continuing or repeating the breach and such other relief as the Tribunal thinks fit (s 92I).

The Criminal Procedure Act 2011 enables breaches of suppression orders to be prosecuted, but does not apply to a person who hosts material on websites or other electronic retrieval systems that can be accessed by a user unless the specific information has been placed or entered on the site or system by that person.

[13] *Tucker v News Media Ownership* High Court of Wellington, 7 November 1986 (McGechan J) available at: http://www.nzlii.org/nz/cases/NZHC/1986/216.pdf

There are also restrictions in the Credit Reporting Code and in the Criminal Records (Clean Slate) Act. Finally the Broadcasting Act 1989 provides that in the event that a material error of fact has occurred, broadcasters should correct it at the earliest appropriate opportunity.

In New Zealand therefore, there is a wide variety of possible protection mechanisms, depending on the facts of a particular case.

How can we effectively regulate and enforce this right in a global online environment?

While this is the question posed by our conference organisers, I do not think it is quite the right one now that we understand what the so-called 'right to be forgotten' relates to. And before we consider how New Zealand regulators can respond, it's important to understand how European regulators are dealing with the implications of this case, particularly how to add nuance and meaning to the ECJ ruling in practice. The Italian Privacy Authority, for example recently declined to uphold a complaint about a refusal by Google to remove a link to an article reporting on a judicial inquiry involving the complainant. The Authority decided this was a recent event and one where there was a strong public interest, ruling that, in this case, freedom of the press outweighed the right to be forgotten.[14]

In another complaint the Italian Authority found that automatically generated "snippets" typically included with search results could be ordered corrected if they did not reflect accurately the information to which they referred. In that case, the snippet associated the name of the complainant with crimes more serious than those in the relevant investigation. In fact, Google had already rectified this problem before the Authority required it, but the ruling will be useful for determining the parameters of future cases.[15]

In this region, the Asia Pacific Privacy Authorities, of which the New Zealand Office of the Privacy Commissioner is a member, has been considering the implications of these developments. APPA has found that a number of significant number policy and implementation issues arise from the ECJ ruling, including:

(a) What is the substantive effectiveness of the ruling which is to remove search results by names only (ie the results can still be searched by other means such as by the description of the event) and not to remove the source itself from the search engines?

(b) There are regulatory concerns about leaving the implementation of the RTBF judgement with multiple commercial organisations which have to make judgements on the different rights of individuals based on often one-sided information. These companies may come to different conclusions in each removal case, raising concerns about legal certainty, consistency and the rule of law;

(c) The jurisdictional issue of search engine implementations being confined to the EU (and variably including a few other European countries), making the RTBF protection largely ineffective when the public can search for the removed contents via global sites of other search engines;

[14] Glyn Moody, "When must search engines concede the "right to be forgotten"? A new ruling from Italy helps clarify when public interest prevails." ArtsTechnica, 4 April 2015 http://arstechnica.com/tech-policy/2015/04/when-must-search-engines-concede-the-right-to-be-forgotten/

[15] Ibid.

(d) How to deal with the conflicting needs to notify the publisher after an adjudication process and not generate publicity on the issue to the detriment of the requester. The United Kingdom publisher, the Telegraph's approach to collate and re-publish a list of Telegraph stories affected by removal[16] highlights the conflict.

APPA concluded that if RTBF is to expand from the EU to cover Asia Pacific or the rest of the world, it will not likely be as a result of a global legal requirement. Instead, if APPA members wish to pursue RTBF in their jurisdictions as a compliance action, they would need to invoke their own legal instruments.

The Office of Privacy Commissioner (OPC) has not ruled on the right to be forgotten and, as mentioned earlier, we do not see this as a particularly new or pressing issue. For the purposes of this seminar, it might be better to just ask questions, such as:

- What is the onus on a search engine or other online service provider if a New Zealand person asserts a right of correction (a term which is defined as including deletion) under information privacy principle 7?
- Does the "purpose" element of the non-retention principle (principle 9) absolve search engines of the obligation to proactively purge old content?
- What guidance, if any, would be useful for agencies and how could this be best developed?
- Is delivering a set of search results in response to a query, an "action" to which IPP 8 applies, requiring the search engine operator to ensure the results are "accurate complete relevant up to date and not misleading?

Whether or not a search engine breaks a link, it remains open to the Privacy Commissioner to hold end users to account. For example, an employer or insurer relying unfairly on out of date search results might well be in breach of and liable under IPP 8.

As a regulator, OPC faces new complaints and enquiries that push us to learn more and understand more. From drones to the exacerbating effects of social media; from advancements in CCTV capability to the challenges of digitising records or shifting to the cloud; and from increasingly sophisticated workplace biometrics to app permissions.

We recognise that we need to be proactive in helping people to make privacy easy. Making sure individuals maintain their right to privacy while ensuring businesses don't feel unduly restrained by bureaucracy that hasn't kept pace with technology. To this end, we have developed a technology strategy 'Making the Future'. We now have a clear work programme to support this strategy and ensure we stay up to date with technology trends.

Latest Developments

Given that the ECJ ruling is still less than a year old, it is not surprising that all parties affected by it - EU data protection authorities, Internet companies, privacy lawyers, and individuals - are still trying to work out exactly what it means in practice. In February 2015 Google published the report of the Advisory Council to Google on the Right to Be Forgotten.[17] The Advisory Council included legal and technical experts including Jimmy

[16] http://www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html

[17] Available at: https://www.google.com/advisorycouncil/

Wales, founder of Wikipedia, Frank La Rue, former United Nations Special Rapporteur on the Right to Freedom of Expression and Luciano Floridi, Professor of Philosophy and Ethics of Information at the University of Oxford, among others.

The Council carried out seven consultation meetings in Europe and developed guidance on the application of the ruling including criteria for assessing requests for delinking of search results, including: [18]

The person's role, if any, in public life including:

- Individuals with *clear roles in public life* (for example, politicians, CEOs, celebrities, religious leaders, sports stars, performing artists) - delisting requests from such individuals are less likely to justify delisting, since the public will generally have an overriding interest in finding information about them via a name-based search.
- Individuals with *no discernable role in public life*: delisting requests for such individuals are more likely to justify delisting.
- Individuals with a *limited or context-specific role in public life* (for example, school directors, some kinds of public employees, persons thrust into the public eye because of events beyond their control, or individuals who may play a public role within a specific community because of their profession): delisting requests from such individuals are neither less nor more likely to justify delisting, as the specific content of the information being listed is probably going to weigh more heavily on the delisting decision.

The nature of information that points to strong privacy interest (such as intimate details of a person's private life, personal financial information, personal identifying information, criminal activity information, information about children, information that is false or heightens privacy interest because of a risk of harm, or information that heightens privacy interest because it is in digital image or video form. There is detailed guidance on the relevance of the source of information (journalists, bloggers and so on) as well as on the age of the information. Procedural aspects for requests are also detailed including notification of original publisher, how to challenge a de-listing decision and processes for transparency reporting.[19]

So what is the demand for delisting? By February 2015 Google had received more than 220,000 requests. Approximately 60% of these were rejected. Google officials commented that while many of the requests are straightforward – a clear cut accept or reject –others "raise complex legal and ethical questions" and that Google is now expected to exercise "judgment calls" that it "never expected or wanted to make," such as "complicated decisions that would in the past have been extensively examined in the courts, now being made by scores of lawyers and paralegal assistants".[20] This role of internet intermediary in law enforcement is a contentious one and has raised significant concerns about the rule of law and procedural fairness.

In further developments, the art 29 Working Party also began work on responding to the ECJ ruling. The art 29 Working Group is an independent advisory body on data protection and privacy, set up under art 29 of the [EU's] Data Protection Directive, and

[18] Ibid.
[19] Ibid.
[20] Peter Barron, in an article by Julia Powles, "Google acknowledges some people want to be forgotten" The Guardian, 19 February 2015, available at: http://www.theguardian.com/technology/2015/feb/19/google-acknowledges-some-people-want-right-to-be-forgotten

made up of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor, and the European Commission.

In November 2014, the art 29 Working Party issued its "common interpretation of the [ECJ] ruling."[21] This includes the controversial view that "limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com." Put more clearly, the art 29 Working Party believes that search engine companies should be required to remove links in their results worldwide, not just in Europe. In fact, other search engine companies, such as Bing, have already begun implementing the decision in Europe. All of these developments have been followed closely[22] and will continue to be over the next few years.

Conclusion

It is important to see this 2014 decision against this legal background and wider global debate. Intermediary liability remains controversial and contested terrain, but in New Zealand we must come back to our national legal framework.

There are some clear conceptual differences between the right to be forgotten and the right to privacy. The right to privacy includes non-disclosure of personal information to third parties, including into the public domain. The right to be forgotten, on the other hand, centres on information which is already in the public domain – personal facts which are already publicly known – but purports to create rights to limit who can access that information from a particular point in time and/or in a particular jurisdiction.

In New Zealand it is unlikely that a right to be forgotten will be established separately by statute. The Law Commission finished its four year review of the Privacy Act in 2011 and did not suggest there should be any new right to be forgotten. However, they did propose protections for anonymity or pseudonymity.

This year OPC has started a new project, focusing on transparency reporting and asking: What is the role of the regulator in this field? We will shortly be issuing a discussion paper on this topic and calling for inputs as we develop a clearer view on this for implementation this year and into 2016. We have many free online resources available and privacy training modules available on our website: www.privacy.org.nz and are highlighting these and the importance of good information handling in Privacy Week this year. – worth putting the date of Privacy week in here?

In the meantime, let's get back to Mr Gonzales. He sued for the right to be forgotten on the Google's search engine– but has the Internet ultimately been his friend or foe in this quest? No matter which search engine you now use to search for Mr Gonzales, thousands, possibly millions, of results now point to his previous debt situation. More than ever

[21] Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain and *Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*" c-131/1 November 2014.

[22] See, for example, Luciano Floridi 11 November 2014, http://www.theguardian.com/technology/2014/nov/11/right-to-be-forgotten-more-questions-than-answers-google

before this is a matter of large-scale scrutiny: it is a matter of public record, legal debate, academic research and judicial examination.

The chances are high that Mr Gonzales, and the fact of his debt which gave rise to this case, will never be forgotten. Was this a desirable outcome in terms of the publicly available information about his former activities? Whatever your view on that, it is true that without the Internet widespread publication of this would not have been possible and Mr Gonzales' new found jurisprudential legacy will continue for many years.