The Right to be Forgotten—the EU and Asia Pacific Experience (Australia, Indonesia, Japan and Singapore)

Professor Dr Bruno Zeller

Professor Dr Leon Trakman

Dr Robert Walters

Associate Professor Dr Sinta Dewl Rosadi*

keywords to be inserted by the indexer

Abstract

This article explores the right to be forgotten or otherwise known as the right to erasure in the EU and Asia Pacific. The right to be forgotten has quickly become an important concept of data protection law. It allows a person to request that their personal data and information be deleted or removed from an internet website. Subsequently, from the application of this right, a person has a level of their personal privacy protected over the internet. However, the acceptance and implementation of this right by Australia, Indonesia, Japan, Singapore and the EU varies. With the implementation of the EU General Regulation on Data Protection in May 2018, the right to be forgotten is well entrenched in the EU. This article investigates an issue of growing significance because of Australia's engagement with these countries, accentuated by the use of the internet. First, one of Australia's closest neighbours, Indonesia, has the largest Islamic population. Secondly, Singapore being a Commonwealth country along with Australia, has also adopted the common law, and has strong trade and other bilateral partnerships. Thirdly, of all the Asian nations, Japan, that recently obtained equivalency from the EU in data protection law, has seen the right emerge in that state. The right, in many respects is also in conflict with other rights and freedoms (right to expression) and other areas of the law. It is an area of law that may never be settled, as technology continues to evolve. This article will highlight the current status of the right to be forgotten across these

* Bruno Zeller B.Com, B.Ed, Master of International Trade Law (Deakin), Ph.D (The University of Melbourne), Professor of Transnational Commercial Law, University of Western Australia; Leon Trakman B.Com, LLB (Cape Town), LLM, SJD (Harvard), Professor of Law and Former Dean, Faculty of Law, University of New South Wales, Sydney; Robert Walters LLB (Victoria), MPPM (Monash), Ph.D Law (Victoria), Lecturer Victoria Law School, Victoria University, Melbourne, Adjunct Professor, European Faculty of Law, The New University, Slovenia, Europe; Sinta Dewl Rosadi, LLB (Unpad), LLM (Washington College of Law, American University), Ph.D (Unpad), Associate Professor in Law at Faculty of Law University of Padjadjaran, Bandung, Indonesia.

jurisdictions, with what can be considered three models of data protection and privacy law. These laws have been developing separately throughout the EU, South East Asia and the Pacific.

Introduction

Personal data has fast become a currency on the internet. Personal data is collected, stored and used in an ever-increasing variety of ways, producing a "panoptic on beyond anything ever imagined".[1] Since the rise of the internet and technology supporting the many systems that collect personal data, people have become increasingly aware of their personal privacy being exposed and also exploited. Subsequently, there have been calls by segments in the community to ensure that individuals have some control over their personal data. To some extent this has been achieved by the establishment of data protection law. It must be noted that the online protection of privacy is a by-product of the implementation of data protection law. One element of control afforded to individuals, which has emerged in data protection law, is the right to be forgotten (otherwise known as the right to erasure).

The origins of the right to be forgotten are seen in the French *droit à l'oubli*, and the laws of Switzerland,[2] which allowed—as an example—a rehabilitated criminal to object to the publication of the facts of his conviction. The underlying premise is that criminals do not remain of public interest forever, so the public should not have access to their criminal records indefinitely.[3] James Steyer believes the right to be forgotten addresses a serious issue in the digital age.[4] Steyer argues that people often self-reveal [online] before they self-reflect and may post sensitive personal information (data) about themselves—and about others—without realising the consequences.[5]

This article "sketches the field" in order to better understand the underlying issues by comparing the data protection and privacy laws more broadly across the Asia Pacific (Australia, Indonesia, Japan and Singapore) and the EU. A regional study is also important for Australia to better understand whether the right to be forgotten has been considered and to what extent that has occurred. Of interest is that in both Indonesia and Singapore the right to privacy does exist, to varying degrees, however, the right to be forgotten has not yet been fully accepted. In addition, Japan considers privacy as an important part of society.

Any discussion regarding the right to be forgotten must commence with the EU, as it has set the benchmark for data protection and privacy law. In brief, the right to be forgotten contributes to a person obtaining a level of privacy over the internet. However, it must also be understood that privacy as a right means different things in and to different countries, religions and cultures. This article does not attempt to conceptualise privacy, as this is beyond the scope of the article. However, a basic understanding is required in order to appreciate the variations in the regulations of privacy laws in the examined countries. Moreover, the development of data protection and privacy law can, to date, be best described as consisting of three models, which are similar conceptually, but vary greatly. We advance the following arguments in relation to those models. First, the EU model, while it balances the needs of the single market with privacy, the supranational polity and its Member States, treats privacy as a fundamental right. The other states discussed in this article do not. Secondly, Singapore has created a business friendly model. Australia's balanced model sits somewhere between the EU and Singapore, and could itself emerge as compromise benchmark.[6] The remaining countries of Indonesia and Japan, while being capable of being compared to

[1] L. Lessig, *Code: Version 2.0* (Perseus Books, 2006), pp.205–208.
[2] L. Lessig, *Code: Version 2.0* (Perseus Books, 2006), pp.205–208; Swiss Federal Court, 23 October 2003, 5C.156/2003.
[3] L. Lessig, *Code: Version 2.0* (Perseus Books, 2006), pp.205–208; Swiss Federal Court, 23 October 2003, 5C.156/2003.
[4] J. Steyer, *Why Kids Need an Eraser Button* (Common Sense Media, 2013), *http://www.commonsensemedia.org/blog/why-kids-need-aneraser-button* [Accessed 21 January 2018].
[5] J. Steyer, *Why Kids Need an Eraser Button* (Common Sense Media, 2013), *http://www.commonsensemedia.org/blog/why-kids-need-aneraser-button* [Accessed 21 January 2018].
[6] Robert Walters, Leon Trakman and Bruno Zeller, *Data Protection and Privacy Law Asia Pacific and Europe* (Springer, 2018) forthcoming.

these respective models, are standalone. In the case of Japan, there is evidence to suggest that, with the recent adequacy assessment obtained and approved by the EU, it is closer to the EU's model than any of the countries discussed in this article.[7] The remaining countries can be best described as combining these three models, or, as not yet having specific data protection laws. Arguably, the approach taken by each country will determine whether it and its citizens consider the right to privacy as important, and whether the right to be forgotten should form part of that legal framework.

In examining whether the right to be forgotten has been implemented and accepted in these jurisdictions, one must first understand how privacy has evolved and been accepted by Western states and states in Asia, that have very different religious and cultural beginnings.

(a) Privacy and varying cultural traditions

In brief, the right has in Western Liberal Tradition primarily arisen from the relationship between the individual with society and the nation state. This liberal thought is something that Thomas Hobbes and John Locke describe as protecting the right(s) derived from the "state of nature" of mankind and forms the basis of the ideals of freedom and self-interest, which incidentally underpinned the French Revolution.[8] From the early beginnings privacy scholars have continuously attempted to provide a solid theoretical foundation to the right to privacy. De Boni and Prigmore argue for the protection of a right to privacy from an Idealistic, neo-Hegelian philosophical point of view. De Boni and Prigmore see privacy, not as a "human right", but as the logical consequence of the Hegelian idea of free will.[9] This thought is based on traditional Anglo-Saxon empiricist philosophy, which the EU, its Member States and Australia have adopted. Furthermore, this Anglo-Saxon thought does not consider religious influence or thought of privacy, such as those religions outside of Christianity.

Contrary to the Western Liberal Tradition, other religions have considered privacy as a right.

While privacy is not a value rooted in Indonesian culture, this has not been a cultural or social impediment for Indonesians. Traditionally, and long before the advent of the internet, privacy was regarded as a value that has been used to improve the happiness and spirituality of Indonesian people.[10] Moreover, there is a divide between those Indonesians who reside in the larger cities compared to the rural counterparts, who have traditionally viewed privacy differently. As a generalised observation, residents of the larger cities, such as Jakarta, have become more individualistic, and place a greater value on their personal privacy; there is less emphasis on such individualism in rural Indonesia.[11] Education and social class has also influenced and shaped the understanding of privacy across Indonesia, particularly the implementation of privacy law. Nonetheless, Indonesia being a predominantly Muslim country does generally view privacy as a right. In other words, personal privacy has been viewed by many Muslim scholars as a fundamental human right.[12] That position holds well for Indonesia as they begin to develop their data protection laws. In Islam, privacy stems from the *Maqasid al Shariah*, from which personal rights (*haqq*) are derived. According to the Maqasid, all individual rights are God-given and by their nature are not absolute.[13] In the exercise of such rights, the state is guided by two main functions: *al amr*, or the promotion of certain positive conduct, and *al nahy*, or the prohibition of a negative conduct.[14] The establishment of rules and

[7] Robert Walters, Leon Trakman and Bruno Zeller, *Data Protection and Privacy Law Asia Pacific and Europe* (Springer, 2018) forthcoming.

[8] C.B. Macpherson (ed.), T. Hobbes, *Leviathan* (Penguin); John Locke, Second Treatise of Government (Prometheus); Derek Matravers (ed.), Jean-Jacques Rousseau, *The Social Contract* (London, 1981).

[9] M. De Boni and M. Prigmore, "A Hegelian basis for information privacy as an economic right", in M. Roberts, M. Moulton, S. Hand and C. Adams (eds), *Information systems in the digital world*, Proceedings of the 6th UKAIS conference (Manchester, UK, Zeus Press, 2001).

[10] Privacy International, *Final Report: Privacy: Personal Data Protection in Indonesia* (2013).

[11] Privacy International, *Final Report: Privacy: Personal Data Protection in Indonesia* (2013).

[12] H. Kamali, *The Right to Life, Security, Privacy and Ownership in Islam* (Cambridge: Islamic Texts Society, 2007); T. Mahmood, *Human Rights in Islamic Law* (New Delhi: Institute of Objective Studies, 1993).

[13] I. Madieha Azmi, "Personal Data Protection Law: The Malaysian Experience" (2007) 16 Info. & Comm. Tech. L. 130.

[14] I. Madieha Azmi, "Personal Data Protection Law: The Malaysian Experience" (2007) 16 Info. & Comm. Tech. L. 130.

institutions such as the institution of *hisbah* is regarded as the machinery by which to promote positive conduct. Essential to the prohibition of negative conduct is the creation of a list of offences such as outraging modesty, spying, *ghibah* (revealing embarrassing details about others), disclosing matrimonial secrecy, defamation and trespass to property.[15] Therefore, the right of privacy comes in two normative frameworks: the first is the prohibition of intrusion into others' privacy, and the second is the instructions and guidance for keeping secrets.[16] Personal privacy is guaranteed in the Qur'an in *Surah al Taubah: 105, Surah Fussilat: 40* and *Surah Saba: 11*. All conduct of a person deserves the highest respect in terms of privacy and secrecy. Any attempt to collect information on the activities of individuals amounts to spying (*tajassus*), *a* conduct forbidden in Islam.[17] Thus, for people of Islamic faith, privacy is considered one of the most important concepts of society.

Japanese history highlights that it is a very homogenous society, with limited multiculturalism, and the predominant religion is Shinto, followed by Buddhism and Christianity having a minimal presence.[18] Nonetheless, this has not deterred the courts from placing privacy as an important issue for Japanese society. The bases for the protection of privacy and more broadly data protection in Japan can be traced to a judgment by the Tokyo District Court on 28 September 1964.[19] The right of privacy has been established under art.13 of the Constitution and/or ss.709 and 710 of the Civil Code—which was transplanted from Germany—by court precedents and applied to specific cases through the general provisions of delict in the Civil Code.[20]

Singapore, similar to Australia is very multicultural, and while their working language is English, the local citizenry speaks Mandarin, Malay, Tamil and to a lesser extent Bahasa. The main religions that make up Singapore are vast, however the most dominant are Buddhism, Taoism, Islam, Hinduism and Christianity. Thus, the consideration of privacy in Singapore can be complex to understand. On the one hand, it has adopted the common law from the UK, which has a well-entrenched understanding and practice of privacy. On the other hand, in referring to the founding father of Singapore, the late former Prime Minister, Lee Kuan Yew stated:

> "I am often accused of interfering in the lives of citizens … had I not done that we wouldn't be here today. And I say without the slightest remorse that we wouldn't be here, we would not have made economic progress if we had not intervened on personal matters—who your neighbor is, how you live, the noise you make, how you spit or the language you use."[21]

Therefore, it could be argued that privacy as a general concept does not exist in Singapore. While beyond the scope of this article, it is likely that citizens of Singapore would view privacy different to their counterparts in Australia, Indonesia and particularly the EU.

It follows that the right to be forgotten does not expressly exist in Singapore. Privacy as a right is viewed differently within Asia. This poses challenges going forward, when some countries view privacy over the internet as a legal right that should be protected. On the other side, countries that already view privacy as a fundamental right, have either fully entrenched the right into their legal framework, or begun to consider privacy as a right. Yet, there are other states that, from a political perspective, have seen the interference of privacy as necessary to advance that state's social and economic objectives.

[15] I. Madieha Azmi, "Personal Data Protection Law: The Malaysian Experience" (2007) 16 Info. & Comm. Tech. L. 130.
[16] I. Madieha Azmi, "Personal Data Protection Law: The Malaysian Experience" (2007) 16 Info. & Comm. Tech. L. 130.
[17] I. Madieha Azmi, "Personal Data Protection Law: The Malaysian Experience" (2007) 16 Info. & Comm. Tech. L. 130.
[18] Religious Facts, Japan, *http://www.religionfacts.com/japan* [Accessed 21 January 2018].
[19] M. Horibe, Chairman, *Privacy Culture and Data Protection Laws in Japan 39th International Conference of Data Protection and Privacy Commissioners* (2017 Hong Kong Personal Information Protection Commission, Japan), *https://www.privacyconference2017.org/eng/files/ppt/masao_horibe.pdf* [Accessed 21 January 2018].
[20] M. Horibe, Chairman, *Privacy Culture and Data Protection Laws in Japan 39th International Conference of Data Protection and Privacy Commissioners* (2017 Hong Kong Personal Information Protection Commission, Japan).
[21] S. Chesterman, *Data Protection Law in Singapore, Privacy and Sovereignty in an Interconnected World* (Academic Publishing, 2018).

Section (1) demonstrates how the right to be forgotten has evolved across the EU. Section (2) compares the Asia Pacific—Australia, Indonesia, Japan and Singapore with the EU—examining to what extent these countries have adopted and accepted the right to be forgotten. Section (3) concludes the article by demonstrating how the EU has accepted the right to be forgotten, although it is arguably still evolving. The concluding remarks will also highlight how the right to be forgotten, is at the very least being considered in Australia, Indonesia, Japan and in the case of Singapore not accepted at all.

(1) European Union

Arguably, the legal concept of the right to be forgotten has largely grown out of the EU. The concept allows an individual to request a search engine to remove personal data and personal information pertaining to them. The discussions regarding the right to be forgotten in the EU can be traced back to the European Commission's conference in May 2009 where a session "Is there a 'fundamental right to forget'?" was held. [22] At that time, a right which embraces forgetfulness or oblivion was considered among some EU Member States.[23] However, the concept cannot be properly understood without examining Directive 95/46/EC

(a) Directive 95/46/EC

Before the General Data Protection Regulation (GDPR) came into effect in 2018, art.12 of Directive 95/46/EC introduced the scope of the right to be forgotten. The former art.12 provided for the "right to access",[24] whereby Member States shall guarantee every data subject the right to obtain from the controller the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data and notification to third parties to whom the data have been disclosed, of any rectification, erasure or blocking carried out unless this proves impossible or involves a disproportionate effort.[25] Throughout the period in which Directive 95/46/EC was operational there were a number of cases in which the EU courts had to consider and decide on the application of the right to be forgotten.

In the 2009 in *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*[26] the Court identified that the right to protection of personal data refers to natural persons and constitutes personal data and that the publication of that data was made accessible to third parties. The facts of the case highlight that farmers challenged the publication of information on the internet site of the German Federal Office for Agriculture and Food, invoking the argument that the EU regulations constitute unjustified interference with their right in respect of privacy and family life and to the protection of personal data, set out in arts 7 and 8 of the Charter of Fundamental Rights of the European Union. The Court noted that the right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society.[27]Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions

[22] Proposition De Loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, Enregistré à la Présidence du Sénat le 6 Novembre 2009. See also LOI No.2016-1321 du 7 Octobre 2016 pour une République numérique—Article 63 (the right to be forgotten for minors). In H. Miyashita, *The Right to Be Forgotten and Search Engine Liability*, Vol.2 (Brussels Privacy Hub Working Paper, 2016).

[23] See fn.23 above.

[24] Council Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 art.12(1)(a) without constraint at reasonable intervals and without excessive delay or expense: confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, communication to him in an intelligible form of the data undergoing processing and of any available information as to their source, knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in art.15(1).

[25] Council Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[26] *Volker und Markus Schecke GbR, Hartmut Eifert v Bundesanstalt für Landwirtschaft und Ernährung* (C-92/09 and C-93/09), 9 November 2010 at [80]–[86].

[27] *Volker und Markus Schecke GbR, Hartmut Eifert v Bundesanstalt für Landwirtschaft und Ernährung* (C-92/09 and C-93/09) at [40].

are satisfied. It provides that personal data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". Moreover, art.52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in arts 7 and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and subject to the principle of proportionality. Satisfying these requirements is necessary to genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.[28] Furthermore, and in accordance with art.6(1) of the TEU, the EU recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union. The principle of transparency set out in arts 1 and 10 of the TEU and art.15 of the TFEU, enables citizens to participate more closely in the decision-making process. The administration, in turn, enjoys greater legitimacy and is more effective and accountable to citizens in its democratic system. However, the Court went further arguing that there was also a need to ascertain whether the limitation imposed on the rights conferred by arts 7 and 8 of the Charter is proportionate. Thus, the competing balance of transparency and proportionality arose in considering the tension between the single market and the right to privacy.[29] More importantly, the Court noted that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary, and that it is possible to envisage measures which affect less adversely that fundamental right of natural persons but which still contribute effectively to the objectives of the EU. The Court ruled that institutions within the EU are obliged to balance the EU's interest in guaranteeing the transparency of its actions and the infringement of the rights recognised by arts 7 and 8 of the Charter. Consequently, no automatic priority can be conferred on the objective of transparency over the right to protection of personal data, even if important economic interests are at stake. By ruling that personal data must apply only insofar as it is strictly necessary, highlighted the fact that the EU will not, in all cases, afford an automatic priority be conferred on the objective of transparency over this right to the protection of personal data. It is argued that a continual balancing act will apply, and these matters will need to be determined on a case-by-case basis. In conclusion, the Court held that the Commission and the Council had not demonstrated that they had sought to strike a proper balance between the various interests involved before adopting the regulations in dispute.[30]

Nonetheless, by 2012, the CJEU was responsible for deciding—indirectly only—the right to be forgotten in the context of definitions of data processing. In the case of *Google Spain SL*[31] the court upheld the complaint of Mr Costeja González. It ruled that an internet search engine operator is responsible for the processing that it carries out of personal data which appears on web pages published by third parties. The Court highlighted that the scope of the right of erasure and/or the right to object, in relation to the *derecho al olvido* (the "right to be forgotten"), the following questions must be asked: Should the rights to erasure and blocking of data, provided for in art.12(b), and the right to object, provided for by [subpara.(a) of the first paragraph of art.14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally and published

[28] *Volker und Markus Schecke GbR, Hartmut Eifert v Bundesanstalt für Landwirtschaft und Ernährung* (C-92/09 and C-93/09) at [48]–[88].

[29] *Volker und Markus Schecke GbR, Hartmut Eifert v Bundesanstalt für Landwirtschaft und Ernährung* (C-92/09 and C-93/09) at [48]–[88]: it is settled case-law that the principle of proportionality, which is one of the general principles of EU law, requires that measures implemented by acts of the EU are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it. It is thus necessary to determine whether the Council of the European Union and the Commission balanced the EU's interest in guaranteeing the transparency of its acts and ensuring the best use of public funds against the interference with the right of the beneficiaries concerned to respect for their private life in general and to the protection of their personal data in particular. The Court has held in this respect that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.

[30] *Volker und Markus Schecke GbR, Hartmut Eifert v Bundesanstalt für Landwirtschaft und Ernährung* (C-92/09 and C-93/09) at [48]–[88].

[31] *Google Inc v Agencia Espanola de Proteccion de Datos, Mario Consteja González* (C-131/12), 13 May 2014 at [95]–[96]. Article 2 of the former Directive 95/46 states that "[f]or the purposes of this Directive: (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject')—an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; (b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

on third parties' web pages?[32] Should he be entitled to invoke his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?[33] More importantly, and in light of the earlier *Volker* case, the Court noted that, in the light of the potential seriousness of that interference, the publication of personal data cannot be justified merely by the fact that the operator of such a search engine has the economic interest in so processing that data.[34] However, inasmuch as the removal of links from the list of results could, depending on the information at issue, affect the legitimate interest of internet users potentially interested in having access to that information, a fair balance should be sought between that interest and the data subject's fundamental rights under arts 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, the interest of internet users, that balance may depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life, contrasted with the public interest in having that information. It is also material to acknowledge that such interest might vary, in particular, according to the role played by the data subject in public life. Thus, as was submitted by Google, in applying the principle of proportionality, any request seeking the removal of information must be addressed to the publisher of the website concerned. The reason is that, whoever makes the information public, is responsible to appraise the lawfulness of that publication and to do so by the least intrusive means. In summary, the balancing of competing rights and principles is complex and will be assessed on an individual basis. This is because most, if not all, legal matters involving personal data pertaining to this issue are likely to be diverged, often materially from case to case.

(i) General Data Protection Regulation (GDPR)—Development

In the same year, 2012, the European Commission circulated the draft of the current version of the GDPR, whereby the right to forgotten was discussed. The drafting of the GDPR resulted in the right to be forgotten, specifying that natural persons would obtain the right to have publicly available personal data and information erased.[35] According to the European Commission, this right would help people to better manage data protection risks online by enabling them to delete their personal data and information if there were no legitimate grounds for retaining that data. During this period, the draft GDPR also elucidated, however, that such a protection had to be reconciled with the right to free expression.[36] At the time, the GDPR was still six years away from being implemented.

The jurisprudence so far has highlighted the emerging issues and acceptance of the right to be forgotten in the EU. In other words, the need to balance economic and business needs with other rights across both the private and public sectors, when considering the right to be forgotten, is real. The balance of commercial interests and human rights is challenging and complex, and is divided as (1) suitability, (2) necessity and (3) proportionality in the narrow sense. It is a three-step process that includes establishing:

- the degree of non-satisfaction, or of detriment, as a first principle;
- the importance of satisfying the competing principle of proportionality; and
- whether the importance of satisfying the latter principle justifies the detriment to or non-satisfaction of the former.[37]

[32] *Google Inc v Agencia Espanola de Proteccion de Datos, Mario Consteja González* (C-131/12) at [95]–[96].
[33] *Google Inc v Agencia Espanola de Proteccion de Datos, Mario Consteja González* (C-131/12) at [3].
[34] *Google Inc v Agencia Espanola de Proteccion de Datos, Mario Consteja González* (C-131/12) at [81].
[35] Draft General Data Protection Regulation, European Commission, European Commission 2012 European Commission (2014), art.17, *Memo: Data Protection Day 2014, Full Speed on EU Data Protection Reform.http://europa.eu/rapid/press-release_MEMO-14-60_en.htm* [Accessed 21 January 2018].
[36] Draft General Data Protection Regulation, European Commission, art.80
[37] X. Groussot, "Rock the KaZaA: Another Clash of Fundamental Rights" (2008) C.M.L. Rev. 1760.

However, according to Alexy, the "Law of Balancing" requires the court to engage in balancing conflicting interests. The law of balancing has been defined as "the greater the degree of non-satisfaction of, or detriment to, one principle, the greater must be the importance of satisfying the other".[38] Nonetheless, this does not remedy all the challenges faced in having to balance the competing needs between the right to be forgotten and other areas of law.

More recently, the balancing of competing and conflicting interests was no more evident than in the case of *NT1 and NT2 v Google and The Information Commissioner* in the High Court of England and Wales.[39] This case is important because it is arguably one of the highest-profile cases regarding the right to be forgotten in a common law jurisdictions.[40] What arose out of this case was the need to balance the right to be forgotten with respect to a person who had received a criminal conviction and wanted the information regarding the conviction removed from the internet. In other words, the claimants sought the removal by the defendant, Google, of search results concerning their previous convictions on the basis that the results conveyed inaccurate, out-of-date and irrelevant information, failed to attach sufficient public interest and/or otherwise constituted an illegitimate interference with their right to be forgotten as established in *Google Spain*.[41] Costello argues that the decision in *NT1/NT2* is particularly relevant, given the traditional hostility of common law jurisdictions to rights of privacy that extend to historical criminal convictions.[42] Common law jurisdictions have traditionally privileged principles of open justice in contrast to the approach of many civil law jurisdictions which, in general, opposes punitive shaming and presumes criminal records to be confidential.[43] The civil law approach is reflected in the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as Data Protection Directive art.8(5) the General Data Protection Regulation. [44]*NT1/ NT2* thus represents an explicit departure from traditional common law attitudes towards criminal histories.[45] Moreover, Costello points out that the judgment is confined to its facts due to the emphasis placed by the judge on a subjective assessment of credibility and remorse.[46] Despite this, the case offers a tentative first step towards clarifying the criteria for a delisting order in cases involving criminal convictions and offers a significant endorsement of the right to be forgotten in such cases.[47] Therefore, as highlighted in this article, the balance of rights, competing and conflicting interests will unlikely never be set in concrete because there are far too many variables.

[38] R. Alexy, *A Theory of Constitutional Rights* (OUP, 2010), p.102.

[39] *NT1 and NT2 v Google and The Information Commissioner* [2018] EWHC 799 (QB).

[40] R. Costello, The Right to be Forgotten in Cases Involving Criminal Convictions, NT1 and NT2 v Google and The Information Commissioner [2018] EWHC 799 (QB) [2018] 3 E.H.R.L.R. 268.

[41] *Google Inc v Agencia Espanola de Proteccion de Datos, Mario Consteja González* (C-131/12).

[42] For a comparative analysis as between a common law and civil law jurisdiction, see J.B. Jacobs and E. Larrauri, "Are Criminal Convictions a Public Matter? The USA and Spain" (2012) 14(1) *Punishment and Society* 3. On the still recent change in the Irish position, see T.J. McIntyre, "Criminals, Data Protection and the Right to a Second Chance" (2017) 58 *The Irish Jurist* 27.

[43] J. Jacobs and E. Larrauri, "European Criminal Records & Ex-Offender Employment", New York University Public Law and Legal Theory, *http://lsr.nellco.org/nyu_plltwp/532/* [Accessed 21 January 2018].

[44] Article 6 provides that criminal convictions "may not be processed automatically unless domestic law provides adequate safeguards".

[45] R. Costello, The Right to be Forgotten in Cases Involving Criminal Convictions, NT1 and NT2 v Google and The Information Commissioner [2018] EWHC 799 (QB) [2018] 3 E.H.R.L.R. 268.

[46] R. Costello, The Right to be Forgotten in Cases Involving Criminal Convictions, NT1 and NT2 v Google and The Information Commissioner [2018] EWHC 799 (QB) [2018] 3 E.H.R.L.R. 268.

[47] R. Costello, The Right to be Forgotten in Cases Involving Criminal Convictions, NT1 and NT2 v Google and The Information Commissioner [2018] EWHC 799 (QB) [2018] 3 E.H.R.L.R. 268. The judge also referred in his decision regarding NT2 to the fact that the crime at issue was not one of "dishonesty". However, there was no discussion of whether the differentiation as between a crime of dishonesty and other crimes was a determinative factor. Again, the implication from the judgment is that, as with a spent conviction, this will be a consideration rather than determinative factor. Focusing on the question of what is in the public interest, when it emphasised differential impacts on the public in its discussion of the offences of both claimants it muddied the waters by introducing dishonesty as a factor. The result is an unclear *mélange* of a public interest test with a categorical sliding scale of offences defined in relation to their relative degrees of deception. The implication that a conviction for a violent crime committed without deception would be more favourably treated than a non-violent offence of dishonesty is problematic on a public policy basis. As criminal acts generally involve an individual recklessly, or knowingly breaking the law, invariably in a manner which seeks to avoid detection, the merits of using honesty as a distinguishing metric is of questionable merit. The most substantively consideration what that treatment of self-help. Both claimants, on the advice of reputation management professionals, had generated content with the express aim of influencing Google's list of returned results prior to the decision in *Google Spain*.

Notwithstanding the above, Jeffery Rosen, in referring to the Vice President of the European Commission, believes that regulators across the EU maintain that all citizens face the difficulty of escaping their past. This is even more evident now that the internet records everything and forgets nothing. [48] When Commissioner Reding announced the new right to be forgotten, she noted the particular risk to teenagers who might reveal compromising information that they would later come to regret. Commissioner Reding articulated the core provision of the right to be forgotten. It provides an individual who no longer wants his or her personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, to request that the data be removed from the system. However, technological changes also bring about new regulatory challenges. The internet, cloud computing, and mobile devices allow each of us to access our data anywhere and at any time. Our data is transmitted from Munich to Miami and to Hong Kong in fractions of a second. In this new data world, we all leave digital traces every moment, everywhere.[49] Do people care about how their data is protected? Do our rules need to be strengthened to give people more confidence and to make it easier for businesses to operate in Europe's digital single market? The simple answer is "yes". In Europe, people do care, with 72 per cent of Europeans saying that they are concerned about how companies use their personal data.[50] Thus, today, the right to be forgotten appears to be firmly entrenched into EU law, and this is evident with the recent implementation of the General Data Protection Regulation.

(ii) GDPR—Implementation

In 2016 the GDPR was established, however it did not came into force immediately and was only fully operational in May 2018. The right to be forgotten has been explicitly written into the GDPR. Article 17(1) provides that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.[51] The right is further underpinned by Recitals 65 and 66 of the GDPR. According to Recital 66, the right to be forgotten has been included to strengthen the right to be forgotten in the online environment. It provides further that the right to erasure should also be extended in such a way that a controller who has made the personal data public is obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of, those personal data.[52] In doing so, that controller is responsible for taking into account available technology and the means available to the controller, including technical measures, to inform the controllers who are processing the personal data with the data subject's request.[53]

Moreover, in accordance with Recital 65, the right to rectification and erasure provides data subjects with the ability to have their personal data concerning them rectified. They also have a "right to be forgotten" where the retention of that data infringes this Regulation or Union or Member State law to

[48] J. Rosen, "The Right to Be Forgotten" Stanford Law Review Online (2012), p.64, *http://www.stanfordlawreview.org/online/privacy-paradox/right-to-beforgotten* [Accessed 21 January 2019]. Viviane Reding, Vice President, "*The European Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, p.5 (22 January 2012), available at *http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF* [Accessed 21 January 2019].

[49] J. Rosen, "The Right to Be Forgotten" Stanford Law Review Online (2012), p.64. Viviane Reding, Vice President, "*The European Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, p.5 (22 January 2012).

[50] J. Rosen, "The Right to Be Forgotten" Stanford Law Review Online (2012), p.64. Viviane Reding, Vice President, "*The European Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, p.5 (22 January 2012).

[51] Regulation 2016/679, art.17: the controller shall have the obligation to erase personal data without undue delay: where one of the following grounds applies the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based according to point (a) of art.6(1), or point (a) of art.9(2), and where there is no other legal ground for the processing; the data subject objects to the processing pursuant to art.21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to art.21(2); the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in EU or Member State law to which the controller is subject; the personal data have been collected in relation to the offer of information society services referred to in art.8(1).

[52] Regulation 2016/679, Recital 66.

[53] Regulation 2016/679, Recital 66.

which the controller is subject.[54] That right is relevant in particular when the data subject has given his or her consent as a child and is not fully aware of the risks involved in the processing, and later wants to remove such personal data, especially on the internet.[55] The data subject should be able to exercise that right, notwithstanding the fact that he or she is no longer a child.

However, Recital 65 goes on to provide exceptions to the right to be forgotten. Recital 65 states that the further retention of the personal data should be lawful where it is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; on the grounds of public interest in the area of public health; for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or for the establishment, exercise or defence of legal claims.[56]

Arguably, the right to be forgotten has been received and adopted by the EU to ensure citizens have the choice about whether their personal data remains on the internet. More importantly, by expressing the right within an EU Regulation as opposed to the former EU Directive, it has arguably raised the level of regulatory status of the right. However, there are a number of conflicting economic rights and legal principles, such as relate to single markets, transparency and proportionality, amongst others, that are in direct competition with the right to be forgotten. Therefore, the right to be forgotten remains an evolving concept, even within and across the EU. What is certain is the fact that EU citizens are afforded a level of right to request from an entity that their personal data be deleted or removed from the internet. It is now worthwhile to contrast the right in the EU with some countries in the Asia Pacific Region, particularly Australia, Indonesia, Japan and Singapore in order to understand how other countries have attempted to regulate the right to be forgotten.

(2) Asia-Pacific

(a) Australia

The Australian privacy laws do not provide a direct right to be forgotten. However, according to the Australian Privacy Principles 11,[57] a business must take steps to destroy or de-identify personal information. Australian Privacy Principles (APP) 13[58] also requires that an APP entity must take reasonable steps to confirm and correct any personal information if it is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant, misleading or an individual request for the entity to correct the information. The problem is that the comprehensiveness of Australian law on the regulation of personal data does not even come close to the EU's.

There is little guidance as to how and what steps are required to be taken to destroy personal information. APP 11.30 states that "reasonable steps" only need to be taken by an organisation to destroy or de-identify personal information.[59] This is subject to a number of limitations and rules. That is, an organisation needs to consider whether possible adverse consequences for an individual are present if their personal information is not destroyed or de-identified— more rigorous steps may be required as the risk of adversity increases. However, practically, an organisation can consider whether the time and cost associated with destroying

[54] Regulation 2016/679, Recital 65. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation.

[55] Regulation 2016/679, Recital 65.

[56] Regulation 2016/679, Recital 65.

[57] Australian Privacy Principles 11.

[58] Australian Privacy Principles 13.

[59] Australian Privacy Principle Guidelines, Chapter 11: Australian Privacy Principle 11—Security of personal information Version 1.0, February 2014.

or de-identification is too great or the costs are too high, such that the organisation may not necessarily have to undertake this function. Moreover, an organisation is not excused from destroying or de-identifying personal information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.[60]

The APP Guidelines note that where it is not possible for an organisation to irretrievably destroy personal information held in electronic format, reasonable steps to destroy it would include putting the personal information "beyond use". Even so, it must be understood that undertaking such a step merely "parks" the personal information within the systems database, server or some other place, so as it is not readily accessible any more. Thus, the information is not permanently deleted or removed.

Nonetheless, the Australian Law Reform Commission (ALRC) had proposed a "right to be deleted", which would be analogous to the EU's right to be forgotten.[61] Support for this proposed law varied.[62] Some believe that Australia's current data privacy and defamation laws are sufficient to address internet privacy concerns.[63] Had the proposal been realised and established, the right to be deleted would today enable a person to have their personal information deleted from the internet. Thus, a system of the right to be forgotten would have existed in Australia.

The ALRC summarised the complex balance between the need for privacy and commercial and public interest as being complex. The ALRC stated that calling something a right is of little value if the right is too readily able to be balanced against competing rights or value and sublimated to those other rights or values. It is inevitable that rights and values will sometimes clash, hence there would seem to be no alternative to qualifying the rights. Once it is accepted that privacy and freedom of speech are both important rights and will sometimes clash, then it seems inevitable that each right must sometimes be qualified.[64] The balancing test involves evaluating competing and often incommensurable rights, interests and values. In particular, breaching someone's privacy might be justified because doing so is in the public interest, and therefore justified. In the state of South Australia, for example, the Court ruled that Google is effectively a publisher and has responsibility for the content which its systems and search engines provide to the public.[65]

To date, the right has had little consideration by the courts of the Commonwealth or any of the States or Territories (Victoria, New South Wales, Queensland, Western Australia, Tasmania, Northern Territory and Australian Capital Territory). An exception to date has been in South Australia. As noted above, in 2015, the state of South Australia provided the first insight and consideration of the principle. The Court in *Duffy v Google Inc*[66] had to consider whether the national privacy principles require organisations to destroy personal data and information. It was argued that, because *Google Inc*[67] published information and data, it was responsible for the content. The Court found that, after a reasonable time had passed following the removal requests, Google became a secondary publisher of the defamatory material. The Court suggested that even continuing to make a URL of the offending content available after a take-down request had been received could make Google responsible as a secondary publisher. This is because Google was responsible for the initial publication being available on a URL provided by it.

[60] Australian Privacy Principle Guidelines, Chapter 11: Australian Privacy Principle 11—Security of personal information Version 1.0, February 2014.
[61] J. Kerr, "What is a Search Engine? The Simple Question the Court of Justice of the European Union Forgot to Ask and What it Means for the Future of the Right to be Forgotten" (2016) 17(1) *Chicago Journal of International Law*.
[62] J. Kerr, "What is a Search Engine? The Simple Question the Court of Justice of the European Union Forgot to Ask and What it Means for the Future of the Right to be Forgotten" (2016) 17(1) *Chicago Journal of International Law*.
[63] J. Kerr, "What is a Search Engine? The Simple Question the Court of Justice of the European Union Forgot to Ask and What it Means for the Future of the Right to be Forgotten" (2016) 17(1) *Chicago Journal of International Law*.
[64] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (2014), p.150.
[65] *Duffy v Google Inc* [2015] SASC 170.
[66] *Duffy v Google Inc* [2015] SASC 170.
[67] *Duffy v Google Inc* [2015] SASC 170.

Even though the case in effect centred on the issue of defamation, the case highlighted the issues surrounding a request for personal data to be removed, namely, in cases when the data was being published by a secondary provider. Based on this case and the Australian Privacy Principles, a possible inference is that the right to be forgotten now exists in Australia. However, there has not been a rigorous debate in Australia as to whether the right fully exists. This is unlikely to occur until the issue is considered by the High Court of Australia.

(b) Indonesia

Indonesia is one of Australia's closest neighbours. To date the right to be forgotten has not been considered by any court in Indonesia.[68] What can be said is that Indonesia's Parliament is moving, albeit very slowly, towards recognising the right to be forgotten. In October 2017, the Indonesian Parliament passed the revised Electronic Information and Transactions (EIT)[69] law that enables data subjects to request that their personal data be deleted. Article 26 s.3 requires each Operator of an Electronic System to delete irrelevant information and records of an individual's personal data and information, under its control, but only upon the direction and request that has been issued through a court order. This limitation in Indonesia is in stark contrast to the EU, whereby data subjects do not need to obtain a court order for their personal data to be deleted in the Member States of the EU. A potential issue that may arise in Indonesia is likely to be the discretion that a court may afford regarding when, where and how personal data is to be deleted, if at all. Another problem that has surfaced is the fact that, in Indonesia, there is no clear definition of personal data, unlike in the respective laws of the other countries discussed in this article that have specifically defined personal data. These gaps will arguably cause difficulties in determining what exactly constitutes personal data. Without properly defining what personal data is, there is no baseline or benchmark in the law that clarifies the boundaries which establish when personal data begins and concludes. This is an area of law that Indonesia will need to consider in light of the practices in Australia, the EU and Singapore that have a clear definition of personal data or personal information, although they vary. This comparison is complicated by the fact that definitions of personal data and information differ. It is outside the scope of this article to compare competing definitions of personal data.

Nonetheless, Indonesia's Parliament is currently in the process of drafting specific data protection laws that is likely to adopt the right to be forgotten. In part, the proposal to establish specific data protection law has evolved from other countries and has also followed the lead of the EU. A number of privacy issues have also surfaced across Indonesia. For instance, the recent Facebook versus Cambridge Analytica issues that resulted in millions of people's personal data being acquired by Cambridge Analytica from Facebook without the consent from data subjects. This resulted in Indonesians in general and the government in particular raising concerns over the practice because it was found that Indonesian Facebook Users were also involved. This, in turn, has resulted in more people demanding the government to implement the proposed Data Protection Bill.[70] Mark Innes highlights that the proposed Data Protection Bill aims to allow data subjects to delete their personal data.[71] It remains to be seen whether the proposal will establish a

[68] Hak untuk dilupakan Direvisi UU ITE Masih Belum Berlaku, *https://tekno.kompas.com/read/2016/11/29/09250047/* [Accessed 21 January 2019].

[69] Electronic Information and Transactions Law No.19/2016.

[70] Bloomberg: facebook-faces-indonesian-police-investigation-over-data-breach, *https://www.bloomberg.com/news/articles/2018-04-06* [Accessed 21 January 2019].

[71] M. Innes, *Indonesia: Government Pushes Draft Data Protection Law Global Compliance News* (2018), *https://globalcompliancenews.com/indonesia-draft-data-protection-law-20180518/* [Accessed 21 January 2019]. The draft law proposes that personal data will be able to be deleted or destroyed, when applicable. However, the proposal is framed in a manner that distinguishes between Personal Data deletion and Personal Data destruction. Deletion is applicable to Personal Data that is processed electronically, while destruction is applicable to Personal Data that is not processed electronically. In other words, a controller is likely to destroy personal data: (a) that no longer has usage value, (b) that has an expired retention period, (c) if there are indications of a leak in the Personal Data management system caused by that particular Personal Data, (d) if there is a written request from the Personal Data Owner to destroy it (no court order is required under the Draft Law but a Personal Data Owner may need to seek a court order to request a Personal Data deletion given requirements under the Electronic Information and Transaction Law and Regulation 20), or (e) that is not related to any dispute resolution proceeding. Furthermore, a controller is likely to have to delete personal data when: (a) that data is no longer needed to achieve the

similar regime to that of Australia, Singapore, Japan, and more specifically the EU. What will be implemented will become crucial to determining the level of the right to delete one's personal data, and subsequently the right to be forgotten.

In summary, the right to be forgotten across Indonesia has a long way to go in order to be entrenched and fully accepted, not only in law, but also by government and the broader community. It requires a shift in accepting that the legal concept will play a more important role in Indonesian society as its citizens continue to embrace and use modern technologies.

(c) Japan

The right to be forgotten properly emerged in Japan, albeit subject to some conjecture. The right to be forgotten was recognised by Judge Hisaki Kobayashi from Saitama District court in Tokyo, in 2015.[72] The Court ordered Google to remove information about a person from its link. The Court ruled that, depending on the nature of a crime, the right to be forgotten should be recognised with the passage of time: "Criminals who were exposed to the public due to media reports of their arrest are entitled to the benefit of having their private life respected and their rehabilitation unhindered".[73] Judge Hisaki Kobayashi went further arguing that it is extremely difficult to live a calm life once information is posted and shared on the internet. It is this point that the Court determined as critical when determining whether the information should be deleted.[74] This appeared to be a watershed moment in the recognition of broader rights in Japan. However, the right to be forgotten has been short-lived and in 2016 the Tokyo High Court overturned the District Court's decision.[75] The Court stated that the right to be forgotten is not a privilege stated in law and that its prerequisites had not been determined. As the data protection laws continue to develop in Japan, how the courts and legislature deal with and respond to the right to be forgotten will need to be watched carefully.

However, in 2017, the Supreme Court of Japan presented the general criteria to be considered in judging whether it would be unlawful for search engine companies to keep providing information (URLs) containing privacy-sensitive articles. The traditional personality right under the Civil Code art.709 may deal with the emerging issues of de-listing in Japan if the privacy harm is brought about by the original publisher.[76] Nevertheless, the Japanese Supreme Court highlighted that this should be determined by "balancing" the legal interest for non-disclosure with the rationale for the information to be transmitted via a search engine.[77] Circumstances which may be considered include the nature and details of the facts; the extent to which the facts belonging to the person's privacy will be transmitted by the provision of information such as the URLs; the degree to which the person thereby suffers from concrete damages; the person's social status and influence; the purposes and meanings of the said [website] articles; the social situations at the time the articles were published; social changes afterwards; and the need for including the relevant facts in the

purpose of the Personal Data management; (b) if the Personal Data Owner has revoked his consent related to the management of the Personal Data, through a written request to the Personal Data Controller; or (c) if the Personal Data Controller uses the Personal Data for purposes that are not in line with the consent or the Draft Law.

[72] "Japan court rejects man's 'right to be forgotten' on Google" (3 February 2003), *The Newpaper*, *http://www.tnp.sg/news/world/japan-court-rejects-mans-right-be-forgotten-google* [Accessed 21 January 2019].

[73] "Japan court rejects man's 'right to be forgotten' on Google" (3 February 2003), *The Newpaper*, *http://www.tnp.sg/news/world/japan-court-rejects-mans-right-be-forgotten-google* [Accessed 21 January 2019].

[74] "Japanese court recognizes 'right to be forgotten' in suit against Google" (27 February 2016), *Japan Times*, *https://www.japantimes.co.jp/news/2016/02/27/national/crime-legal/japanese-court-recognizes-right-to-be-forgotten-in-suit-against-google* [Accessed 21 January 2019].

[75] "Tokyo High Court overturns man's 'right to be forgotten'" (13 July 2016), *Japan Times*, *https://www.japantimes.co.jp/news/2016/07/13/national/crime-legal/tokyo-high-court-overturns-mans-right-forgotten/#.W8mObvZuLcs* [Accessed 21 January 2019].

[76] H. Miyashita, *The Right to Be Forgotten and Search Engine Liability*, Brussels Privacy Hub Working Paper, Vol.2 (2016), a person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable to compensate any damages resulting in consequence.

[77] "A Right to be Forgotten Case before the Japanese Supreme Court", *http://blog.renforce.eu/index.php/en/2017/02/07/a-right-to-be-forgotten-case-before-the-japanese-supreme-court/* [Accessed 21 January 2019].

articles.[78] If the legal interest for non-disclosure clearly "outweighs" the reasons for providing information, search engine providers can be requested to remove the relevant URLs from research results.[79]

The Japanese Supreme Court did not find it necessary to oblige Google to remove the relevant information. According to the Court, the facts of the case, namely relating to child prostitution, is a penalised act which is subject to strong social reprobation including that the arrest of the appellant remained in the public interest. The Court also found that the transmission of information was still limited in scope, as the search results depended on the appellant's name and his prefecture.[80]

What can be observed is that the Act on the Protection of Personal Information 2016 (the Act) has a very different title to other jurisdictions. It was updated in 2015 and 2016 and aims to protect an individual's rights and interests, while considering the utility of personal information. The updates in Japan's laws were developed in order to render it ready to obtain an adequacy decision under the former EU Data Protection Directive directed at facilitating the flows of personal data with the EU.[81]

(d) Singapore

Singapore introduced the Personal Data Protection Act 2012 (PDPA) in 2012. Section 16 of the PDPA provides for the withdrawal of consent on giving reasonable notice to the organisation: an individual may at any time withdraw any consent given, or deemed to have been given, in respect of the collection, use or disclosure by those organisations of personal information about the individual. Additionally, where an individual withdraws consent to the collection, use or disclosure of personal data, the organisation shall cease collecting, using or disclosing the personal data. Furthermore, s.22 allows an individual to request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation. The laws do not allow for a person to request that their personal data be erased or deleted. The notion of a right to be forgotten could be contained in s.25 regarding the requirement to destroy or de-identify personal data when there is no longer any legal or business reasons, and where there is no other material the purpose for retaining the personal data.[82] However, there are considerable limitations imposed in applying this conditional requirement when compared to the principles adapted by the EU.

(3) Concluding remarks

Privacy has been accepted in each of the jurisdictions discussed in this article, although to varying degrees. Moreover, privacy over the internet is gaining a higher level of acceptance and understanding. Arguably, the EU has been leading the way in the development of data protection and privacy law, with Singapore being a notable exception to the EU direction that other states are generally following. Simon Chesterman notes that, throughout Asia, many jurisdictions now embrace data protection laws even in the absence of any formal protection of a more abstract right to privacy—let alone the right to be forgotten.[83] Thus, as highlighted earlier in the article, Walters, Trakman and Zeller believe that in studying and comparing the

[78] "A Right to be Forgotten Case before the Japanese Supreme Court", *http://blog.renforce.eu/index.php/en/2017/02/07/a-right-to-be-forgotten-case-before-the-japanese-supreme-court/* [Accessed 21 January 2019].

[79] "A Right to be Forgotten Case before the Japanese Supreme Court", *http://blog.renforce.eu/index.php/en/2017/02/07/a-right-to-be-forgotten-case-before-the-japanese-supreme-court/* [Accessed 21 January 2019].

[80] "A Right to be Forgotten Case before the Japanese Supreme Court", *http://blog.renforce.eu/index.php/en/2017/02/07/a-right-to-be-forgotten-case-before-the-japanese-supreme-court/* [Accessed 21 January 2019].

[81] N. Higashizawa and Y. Aihara, "Data Privacy Protection of Personal Information versus Usage of Big Data: Introduction of the Recent Amendment to the Act on the Protection of Personal Information (Japan)" (2017) 84 Def. Counsel J. 1.

[82] Personal Data Protection Act 2012 s.25 states that an organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that—the purpose for which that personal data was collected is no longer being served by retention of the personal data; and retention is no longer necessary for legal or business purposes.

[83] S. Chesterman, "After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012" (2012) *Singapore Journal of Legal Studies* 396.

data protection laws of these jurisdiction three models have emerged. Most notable is the EU that has treated the right to privacy as a fundamental right. In other words, the EU model is rights-focused. On the other side, Singapore has developed a business friendly model that treats the right to privacy as secondary to the economic right to the use of personal data. Australia does neither, but takes a more balanced approach between the EU and Singapore. In further contrast, the Indonesian and Japanese models are slightly different again. For instance, Japan appears to be moving closer to accepting the right to be forgotten. However, there remains considerable apprehension in Japan applying that right in the same way as the EU, even though Japan recently received equivalency status by the EU for its data protection laws. Indonesia, on the other hand, have yet to implement specific data protection laws, and therefore, the right to be forgotten is far from being fully accepted there.

Notwithstanding the above, the right to be forgotten has a close connection with the right to withdraw consent. Consent has emerged in data protection and privacy laws of the above-mentioned countries and the EU. In order to exercise the right to be forgotten, one condition is that a data subject withdraws consent on which the processing is lawful and there is no other legal ground for processing that data.[84] However, it is beyond scope of this article to compare what level of consent is afforded to data subjects and how consent is applied. Nevertheless, the right to be forgotten is not specific and there is no black-and-white application of it in practice. Rather, it is argued that as the right evolves along with technology, it will need to be assessed on a case-by-case basis. What can be said is that the establishment of the right to be forgotten within the EU has had a profound impact on the way organisations have had to deal with, and will continue to deal with, erasing personal data and information on the internet.

What will require further work is the need to develop a better understanding of the level of harm arising from the failure to protect personal data. This harm relates to both the nature of the privacy right that is infringed over the internet, and how the ensuing harm from that infringement interrelates with the right to be forgotten. Meg Leta Ambrose and Jef Ausloos argue that privacy as a harm is abstract because harm is often concerned with societal and psychological issues. They are distant because many of the consequences arising from a breach of privacy will only reveal themselves after a series of reactions. The impact from privacy breaches as a result of the misuse of personal data over the internet is uncertain because that breach might never occur, or if it does, any harm arising from it was not reasonably foreseeable, and/or not able to be detected, measured, mitigated or prevented.[85]

Finally, in our view the future direction of this area of law will be heavily influenced by community expectations and perceptions of how and whether people's personal data is secure. The EU has made significant progress in to allowing its citizens the right to be forgotten, although it remains to be seen whether the GDPR is adequate in its present state considering that technology is ever changing.

[84] Regulation 2016/679 art.17(1)(b).
[85] Regulation 2016/679 art.17(1)(b).