The Right to be Forgotten: Forget about It?

Wesley Yi-Hung Weng*

This essay aims to evaluate the concept of 'the right to be forgotten' in both Formosan and European Regime, with the latter based on the GDPR. I will focus on the purpose and the objective of the law. The arguments of this essay will be articulated in three substantial sections between an introduction and a conclusion: (1) identify and justify an adequate theoretical framework to probe and evaluate the current European GDPR; (2) examine the potential balance between competing rights and technical applications; and (3) construct a coherently theorised regulatory framework for Formosan data protection law regime.

1. Introduction: Setting the Scene

This essay aims to critically evaluate scepticism about the EU[1] General Data Protection Regulation (GDPR hereafter) on personal data protection,[2] specifically on the ideas and concepts of the right to be forgotten. The Regulation, undoubtedly, is another significant milestone of the European data protection model.[3] Before the Data Protection Directive,[4] historically, there was no effective and specific international instrument which focused on interferences through the processing of personal data. It was, indeed, a main regulatory instrument in Europe, extended its worldwide influence (Article 25 of the Directive). Nevertheless, the model has been challenged by the U.S. academics.[5] This is again, however, enshrined in the following GDPR.[6]

* Assistant Professor, College of Law, Shih Hsin University. PhD in Law, Durham University, UK.

[1] The Treaty of Lisbon amending the Treaty on European Union (TEU) and the Treaty establishing the European Community has entered into force on 1 December, 2009. Consequently, as from that date, references to the EC shall be read as the EU.

[2] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[3] The difference between the European and US model of data is best described by Francesca Bignami: '[i]n the European Union, privacy is essential to protecting citizens from oppression by the government and market actors and preserving their dignity in the face of opposing social and political forces. In the United States, privacy is secondary.' Francesca Bignami, 'Transgovernmental Networks vs. Democracy: The case of the European Information Privacy Network' (2005) 26 MICH J INT'L L 807. See also, Joel Reidenberg, 'Setting Standards for Fair Information Practice in the U.S. Private Sector' (1995) 80 IOWA L REV 497, 500.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.

[5] Fred H. Cate, Peter Cullen & Viktor Mayer-Schönberger (2014). "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines." https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf (accessed May 11, 2018).

[6] The EU data protection model will remain its influence by reading Article 44 of the GDPR, which states that: 'Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third

The Directive, as well as the GDPR, considers both the human rights approach and the economic approach from which it aims to harmonise data protection legislation of member states (Article 1 of the Directive and the GDPR). However, dilemma between promoting free flow of personal data to function internal market and protecting the fundamental rights and freedoms of nature persons is commented as rather problematic in the field of science and technology and their commercial applications. For example, limitations on collecting, processing and using personal sensitive data are considered as barriers on biomedical research improving human health. This also happens in all fields of data science and IT applications, e.g., Big Data, Artificial Intelligence, and Machine Learning. The most common objection raised by some scientists, and unsurprisingly most enterprises and their lobby groups goes, such interests are diminished by the personal data protection barriers.[7] Following this line of reasoning, they may feel even more irritated by the reform of the General Regulation, for the GDPR impressively seeks to reinforce the position of data subjects and enhance the responsibility of data controllers from the outset. For the opponents, the more responsibility data controllers are charged, the higher cost and more limitations will be imposed on using samples and personal data from individuals.

A sad disaster to them.

However, it should be noted that the previous argument holds a presumption that the interests of internal market (e.g., research interests) and data protection rights, in particular the right to privacy, are always competing. In other words, this presumption excludes or at least underestimates the possibility that both interests considered may be fostered and protected in an optimal way since it sees the balancing test as weighing one interest against the other. The above thinking has been termed the conflict model.[8] On the basis of this model, the GDPR thus presents new challenges to the scientists.

This essay will focus on the issues of the right to be forgotten, as the idea might be the most discussed and misunderstood topic currently in Taiwan concerning the GDPR. If someone objects to a webpage appearing in a name-based search for them, they first need to contact the search engine to ask them to de-index the page from searches based on their name. Based on the information provided, in June 2018, the statistics released by Google showed that in the year following the judgment, there were 693,937 requests to remove 2,595,192 pages across the European Economic Area (EEA) . The statics given by Google simply shows that requests received over time rockets. [9]

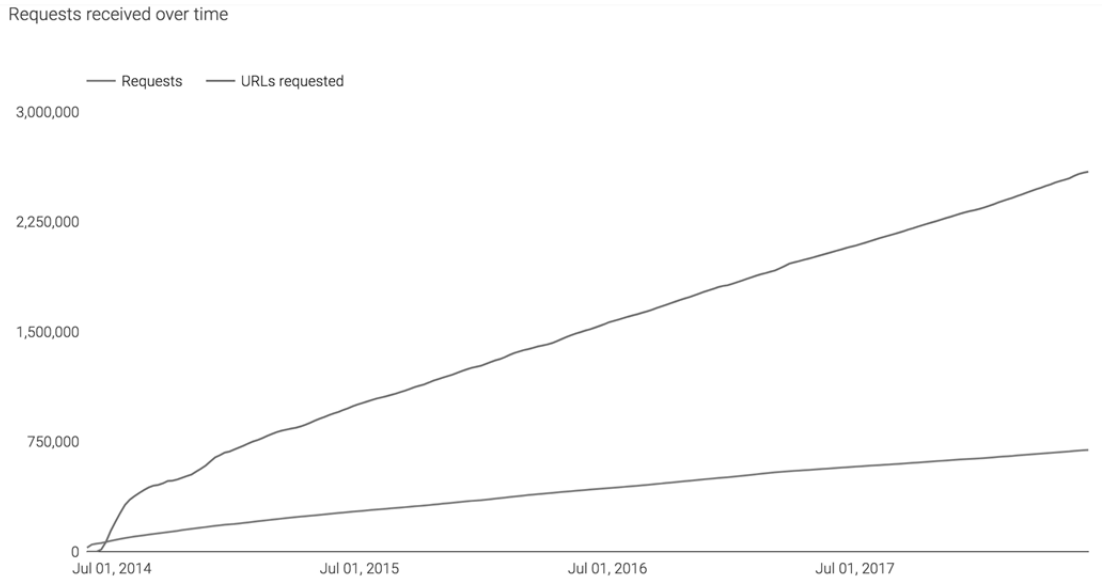
---

country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.'

[7] E.g., *R v Department of Health ex p. Source Informatics* [2001] QB 424.

[8] Deryck Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' in Sheila AM McLean (ed), *First Do No Harm: Law, Ethics and Healthcare* (Ashgate Publishing 2006) 155.

[9] Google, Transparency Report, available at: https://transparencyreport.google.com/eu-privacy/overview?hl=en_GB, (last visited: 23 June 2018).



As regards to Formosan governmental request to remove content, Google highlights that the Taiwan Centers for Disease Control requested to delist a page from Google Search containing a list of HIV patients' personally identifiable information and a request from a Member of Parliament to remove a search result linking to a news article that allegedly defames him.[10] This demonstrates that the right to be forgotten is not only carefully and largely practised in the EU, but also around the globe including Taiwan.

2. Introducing A Theoretical framework

2.1 The EU Data Protection Model: The EU Law and the ECHR

The European data protection model is notoriously complex – it has even been considered too complex to achieve the ultimate goal of full harmonisation within the EU before the GDPR.[11] To have an initial image regarding the model, it is better to start form looking at the whole picture of the European human rights legal regime. The EU is under an obligation to uphold international law when exercising its powers.[12] Article 12 of the Universal Declaration of Human Rights (UDHR)[13] states that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

This principle resonated with Article 17 of the International Covenant on Civil and Political

[10] Google, Transparency Report, available at: https://transparencyreport.google.com/government-removals/by-country/TW?hl=en_GB , (last visited: 23 June 2018).
[11] Peter Blume, 'Will it be a better world? The proposed EU Data Protection Regulation' (2012) 2 International Data Privacy Law 130-136.
[12] Case C-286/90 *Anklagemyndigheden v. Poulsen and Diva Navigation* [1992] ECR I-6019, para 9. Paul Craig and Gráinne De Búrca, *EU Law: Text, Cases and Materials* (5th edn, OUP 2011) 341.
[13] It was proclaimed by the General Assembly of the United Nations on 10th December 1948. Available at: < http://www.un.org/en/documents/udhr/> accessed 28 February, 2010.

Rights (ICCPR). According to Article 216(2) TFEU,[14] if international agreements are entered into by the EU, those agreements are held to be an integral part of the EU legal order.[15] However, it should be noted that the EU is not a party to any of these aforementioned international instruments and the Union itself is not directly bound by them (although individual member states that have ratified these instruments will be).

However, it should be noted that before the Treaty of Lisbon, the EU was not a party of any of these aforementioned international treaties[16] – including the ECHR. Yet with the fact that all EU Member States are parties of the Council of Europe,[17] the relationship between the ECHR and the EU in matter relating to human rights, subsequently, has become more complex. The foundations of the rights protection within the EU legal system are inspired by the integration of human rights norms developed by its Member States and of the norms of the ECHR, including their common national constitutional traditions and international/ European human rights instruments. According to the ECJ's consistent attitude after the *Staunder* case,[18] general principles of EU law including protection for fundamental rights and freedoms are granted. This is deemed complicated: **before the successful/ completely accession** to the ECHR,[19] the ECJ, in the data protection regime,[20] retains the freedom to 'go beyond' the ECHR 'in recognizing rights as part of EU law.'[21] It is observed by Craig and De Búrca that[22]

> It remains to be seen how strictly the ECJ will treat the stipulation that Charter rights corresponding to ECHR rights shall have the 'same' meaning as the ECHR rights, but it seems clear that the ECJ is willing to look closely at the relevant ECtHR case law for guidance.

Data protection and the right to privacy are included in the general principles of EU law.[23] In light of this, before the introduction of the GDPR, interpretation of the Data Protection Directive (and the Data Protection Acts of Member States at national level, which are intended to implement the Data Protection Directive) must take the ECHR into account. This

[14] I.e., Article 188L, which is the article number used in the text of the Lisbon Treaty.
[15] Case 181/73 *Haegeman v Belgium* [1974] ECR 449, para. 5. Under this circumstance, the member states are bound by international agreements as a result of their duties under Community law, not international law. See Case C-239/03 *Commission v. France (Etang de Berre)* [2004] ECR I-9325, para 26. Also, Paul Craig and Gráinne De Búrca, *EU Law: Text, Cases and Materials* (5th edn, OUP 2011) 344.
[16] The EU itself is not bound by the UN Charter directly but is bound by it indirectly due to the EC Treaty. As regards the ICCPR, it is indeed a source of the general principles of the EU law (for counter opinion, see Case C-249/96 *Grant v. South West Train Ltd.* [1998] ECR I-621, paras. 44-47.) See Paul Craig and Gráinne De Búrca, *EU Law: Text, Cases and Materials* (5th edn, OUP 2011) 366-369.
[17] Beyleveld, 'Data Protection and Genetics: Medical Research and the Public Good' 281-282.
[18] Case 29/69 *Stauder v. City of Ulm* [1969] ECR 419. This attitude was later confirmed by the *Internationale Handelsgesellschaft* case (Case 11/70 *Internationale Handelsgesellschaft v. Einfuhr- und Vorratstlle für Getreide und Futtermittle* [1970] ECR 1125), the *Second Nold* Case (Case 4/73 *J. Nold v. Commission of the European Communities* [1974] ECR 507) and *Amministrazione delle Finanze delle Stato v Simmenthal* (Case 106/77 *Amministrazione delle Finanze delle Stato v Simmenthal* [1978] ECR 629) See also: Craig and Búrca (n 8) 364-366, Beyleveld, 'An Overview of Directive 95/46/EC in Relation to Medical Research' 6, and Helen Fenwick, *Civil Liberties and Human Rights* (4th edn, Routledge-Cavendish 2007) 138.
[19] The accession by the EU to the ECHR will be successful once the accession agreement has entered into force, which requires the ratification by all member parties to the ECHR as well as the EU itself.
[20] Case C-28/08 *Commission v Bavarian Lager* 29 June 2010.
[21] Craig and Búrca 367.
[22] Ibid 367.
[23] Cases C-465/100, 138 and 139/01 *Rechnungshof v. Österreichisher Rundfunk* [2003] ECR I-12489.

can be confirmed by reading Recital 10[24] and Article 1.1 in conjunction with Recital 1 of the Data Protection Directive. It has been frequently observed that the influence of European human rights law is increasing perceptibly after the Amsterdam Treaty came into force.[25] This has been affirmed by the Treaty of Lisbon. Consequently, the implementation of EU instruments into domestic law is subject to respect for the ECHR.

The author believes that the situation remains the same after the GDPR, as Article 1(2) of the Regulation states that '[t]his Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.'[26] This can be further justified on the basis of recital of the GDPR in relation to the restrictions concerning specific principles and the certain related obligations of the controllers imposed by Union or Member State law, e.g., the duties of the data controller regarding the right to be forgotten. Recital 73, to be clear, not only subtly refers '**necessary and proportionate in a democratic society to safeguard public security**', but puts that 'those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.'

To look at the right to be forgotten enshrined in the GDPR and to deal with the forthcoming collisions of the new GDPR rights, it is therefore essential to understand how the ECtHR examines the ECHR, in particular Article 8 regarding the right to private life. The standard interpretative approach applied by the ECtHR to examine Articles 8-11 of the ECHR has been termed the 'constitutional approach'[27] or the 'interference-violation approach.'[28] The standard formula consistently followed by the Court can be presented in the sub-stages set out below:

(1) To assess whether any interference is 'in accordance with the law' or 'authorised by the law,'[29] two sub-principles can be distinguished. First, the interference must be 'governed by law,'[30] rather than by any ordinary administrative orders. Secondly, the law must be foreseeable by a rational agent.

(2) To assess whether any interference serves the purpose of the legitimate interests listed in the concerned article.

(3) To examine whether any interference is 'necessary in a democratic society.'

[24] Recital 10 of the Data Protection Directive: 'Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law…'
[25] Fenwick (n 68) 138.
[26] See also, Recital 1: 'The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.'
[27] Foundation for Information Policy Research, *Paper No. 4: The Legal Framework: an Analysis of the "Constitutional" European Approach to Issues of Data Protection and Law Enforcement* (UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004) 9.
[28] Stephen Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation* (Martinus Nijhoff Publishers 2008) 89.
[29] This review stage is also termed as the 'rule-of-law criteria'. See: David Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd edn, OUP 2002) 536-537.
[30] Ibid 537.

The interference here can be either within or outside the scope of Article 8 since there are a number of rights covered in it. If any violation in question cannot be justified in the earlier sub-stage, then there is a violation incompatible with Article 8. If so, there is no need to move on to examine the further stages. With reference to the above formula, it seems possible to evaluate competing rights and interests: if any interference is justified, the right being violated is overridden in specific competing case at issue. In this case, the last stage of the ECtHR balancing test approach requires the evaluation of the *principle of proportionality*.[31] However, the balancing test here is rather unclear and inconsistent. This is because of the combination of: (1) the need of a wider margin of appreciation; (2) the limitation set out in Article 8(2) is broadly framed; and (3) the principle of proportionality lacks clear guidelines. Accordingly, this character does cause a significant problem: **it is difficult to ascertain exactly what local courts should be 'taking into account' to determine the hierarchy of protected rights and interests when developing domestic human rights law.**[32]

This happens in the circumstances of conflicts between the right to be forgotten and other fundamental rights and freedoms, e.g., the right of freedom of expression and the right to know as such. Consequently, to understand a European data protection model and to further deal with how to strike a balance between the competing fundamental rights and freedoms, pros and cons of the ECtHR approach must be referenced. This has been dealt with and will assist later discussions of the essay.

2.2 Data Subjects' Autonomy and the Will-conception of Rights

After sketching up the European data protection model through the legal lens, a theoretical backdrop has to be presented to the subsequent analysis of the right to be forgotten. The concept linking the two streams of discussion is the autonomy of the data subject, which can be identified as an agent. Here, borrowing from Alan Gewirth's argument, I conceptualise a data subject as an agent (who is at the same time being recognised as a human individual, protected by the GDPR) as 'an actual performer of actions or a prospective purposive performer of actions who does (perform) something voluntarily for a purpose that it has chosen.'[33]

Today, data is indeed gold. However, as data records human agents' daily behaviours, threats to fundamental rights and values are thus generated, e.g., personality, autonomy, fairness, justice, solidarity of a community, and of course, privacy[34], which are all protected under the data protection law. This is even crucial to a 'netizen' who, while believing the possibility of enhanced freedom from bureaucratic reality, leaves digital footprints behind in the online

[31] The principle of proportionality embraces three sub-principles, i.e., (1) suitability; (2) necessity; and (3) proportionality in the narrow sense. See: Lord Hoffmann, 'The Influence of the European Principle of Proportionality upon UK Law' in Evelyn Ellis (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999) 107.

[32] N. A. Moreham, 'The Right to Respect for Private Life in the European Convention on Human Rights: a Re-examination' (2008) 1 EHRLR 45-46.

[33] Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001) 72. It refers to a being with capacity to control its ability of doing something (X) through its unforced, informed choice so as to try to achieve its purpose (E).

[34] Solon Barocas and Helen Nissenbaum, Big Data's End Run around Anonymity and Consent, in Privacy, Big Data, and the Public Good Frameworks for Engagement, Edited by Julia Lane, Victoria Stodden, Stefan Bender (CUP, 2014), Helen Nissenbaum, 44.

world. In the age of self-media, the netizens as agents both produce and collect/ process data and information over the internet. I, following Daly[35], adopt the conception of an agent's autonomy by Raz, who argues that:[36]

> The ruling idea behind the ideal of personal autonomy is that people should make their own lives. The autonomous person is a (part) author of his own life. The ideal of personal autonomy is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decision throughout their lives.

This might be identified as a will-conception theory to rights, which means that an agent has no perfect duty to itself to defend his/ her possession of these fundamental rights and freedoms. In this respect, agents can waive the benefits of the fundamental rights and freedoms. However, to be regarded as a will-conception theory, this is not sufficient: the fundamental rights are claim-rights under the will-conception means that 'duties imposed on other agents by the positive rights are subject to the rights-holder wishing assistance, while duties imposed by negative rights are subject to interference being against the rights-holder's will.'[37] Hence, the justification that there are both positive and negative rights under the conception is needed: firstly, as Bernal rightly puts that the autonomy involves the presence of meaningful choice in agent's lives and them being free from "coercion, restraint, or excessive undue influence", with "freedom from manipulation [being] as important in this context as freedom from coercion',[38] it is thus considered that other agents categorically ought not to interfere with an agent's having the fundamental needs against his/ her will. Secondly, entailed by Raz, his conception of personal autonomy is not antithetical to state action. He sees a role for the government, while warning of the dangers of concentrating power in the hands of the few, to 'take positive action to enhance the freedom of their subjects'[39]. As the agent's negative right to resist the undue influence of concentrations of power which may manipulate or coerce choices and choice-making, and can have both public (i.e., state-controlled) and private (i.e., corporate) character protected, it is entailed that the positive right requires duties not only from the government, as Raz considers above, but also from other agents.

This essay is specifically concentrating on the things on the internet. As the Internet has long since moved away from being an open space of individual freedom, and has become instead, as Daly noted, "a heavily commodified space which has seen the emergence of for-profit actors performing a 'gatekeeping' function over data flows, both for their own economic benefit as well as for the state's surveillance and law enforcement capabilities"[40] True, Large companies, i.e., Google, Amazon, and Facebook, as the data processors and the so-called Little Brothers, may control more data than the governments ever do.

In this case, the understanding that fundamental rights and freedoms operate under the will-

[35] Daly, Angela, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart 2016) 22.
[36] J Raz, *The Morality of Freedom* (OUP, 1988) 369.
[37] Deryck Beyleveld and Shaun D. Pattinson, 'Moral Interests, Privacy, and Medical Research' in Michael Boylan (ed), *International Public Health Policy and Ethics* (Springer Netherlands 2008) 2.
[38] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP, 2014) 25. Also, Daly, Angela, The Internet, User Autonomy and EU Law. Private Power, Online Information Flows and EU Law: Mind the Gap (Hart 2016) 22.
[39] J Raz, *The Morality of Freedom* (OUP, 1988) 427.
[40] Daly, Angela, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart 2016) 21.

conception principle entail that an agent can waive the benefits of generic rights if they wish to do so. Accordingly, he/ she does not have duties to protect, or at least not to harm, their own generic agency interests if he/ she does not wish to do so. However, such a waiver should not endanger, again, equally or more important generic rights/ interests of other agents. Moreover, such a waiver should be based on permitting an informed agent to engage freely in activities that are not favourable to the interests of the agent protected by fundamental rights and freedoms.[41] However, this is subject to the proviso that positive action to protect an agent's fundamental rights and freedoms cannot be required of another agent if the other agent's assistance conflicts with (at least) equally such important rights or interests of another agent.[42]

3. Conceptualising the Right to be Forgotten

3.1 Data Subjects' Ability of Controlling Their Data and the Notion of the Right to be Forgotten

J. Y. Interpretation No. 535 of Formosa, firstly, in 2001 the Constitutional Court regards the right to privacy as a type of fundamental rights and freedoms:

> … However, the ways in which police checks are conducted including searches, street checks, and interrogations may have a great effect upon personal freedom, right to travel, property right and *right to privacy* and therefore such checks must be in accordance with the rule of law as well as legal principles guiding police functions and legal enforcement. Thus, to fully ensure the *constitutional* protection of people's *fundamental rights and freedoms*, the requirements and procedures of police checks as well as legal remedies for unlawful checks must be prescribed clearly in the law… (emphasis added)

This opinion was then reaffirmed by J. Y. Interpretation No. 585 in 2004:

> *T*he right of privacy, though not clearly enumerated under the Constitution, is an indispensable fundamental right protected under Article 22 of the Constitution because it is necessary to preserve human dignity, individuality, and the wholeness of personality development, as well as to safeguard the freedom of private living space from interference and the freedom of *self-control* of personal information (See J.Y. Interpretations Nos. 509 and 535). (emphasis added)

Under this interpretation, an abstract article[43] for safeguarding all the other unlisted types of fundamental rights and freedoms is applied. This interpretative method is then followed by J. Y. Interpretation Nos. 603 and 613.[44] As the majority of [45] the Formosan Honourable Justices,

---

[41] Deryck Beyleveld, 'The Principle of Generic Consistency as the Supreme Principle of Human Rights' (2012) 13 Human Rights Review 12.
[42] Ibid 14.
[43] Article 22 states that '[a]ll other freedoms and rights of the people that are not detrimental to social order or public welfare shall be guaranteed under the Constitution.' Article 23 further declares that '[a]ll the freedoms and rights enumerated in the preceding Article shall not be restricted by law except by such as may be necessary to prevent infringement upon the freedoms of other persons, to avert an imminent crisis, to maintain social order or to advance public welfare.'
[44] For the German Constitutional Courts' opinions in relation to the justification of the right to privacy, see: Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer 2010) 4-5.

at the time when Interpretations were given, obtained their law degrees from Germany, it is unsurprising to find out that this approach, which refers to human dignity and the right to personality in order to justify the right to privacy, borrows from the German Constitutional Court's opinions.[46] The conceptualised idea of the right to privacy, overlapping with rights under the data protection,[47] is also written in the Personal Data Protection Law (PDPL) of Taiwan, which aims to govern the collection, processing and use of 'personal information'[48] so as to prevent infringement upon *the right to personality*.

However, it is almost too obvious to state that uncontrolled utilisation of the technologies thus can come into conflict with the protection of fundamental rights and freedoms of individuals. The concern is crucial in the age of data applications, as the image of personal bodily integrity of an individual may very soon become a complete picture in the eyes of data controllers. It has been remarked by Koops and Leenes:

> …In the vast majority of technologies developed and used in real life, its influence is to the detriment of privacy. That is, technology often has the side-effect of making privacy violations easier…
>
> …Examples in law enforcement and e-government show technology offers increasing opportunities for large-scale monitoring – from intercepting all telecommunications…to monitoring the movements of people. In the private sector, technology enables more *control* of people, from workplace and transaction monitoring to personalization of consumer relationships, with new applications like facial recognition and RFID monitoring looming ahead… (emphasis added)[49]

In this regard, as personal data partially make up an 'extended self' demonstrating an agent's personality and its possibility of free development, it is thus harmful to the agent to diminish/ weaken the protection of such legal interests. Bernal provides three reasons to show that why it is particularly dangerous in the age of value-added data applications: (1) without connecting with its the data subject(s), data have limited value, in particular in the age of Big Data; (2) to the data subjects, losing control over their own data can have more serious impact than the value of the property itself; and (3) in relation to the online world, rather than the agent (data

---

[45] Until September 2011, 9 out of 15, and after October 2011, 6 out of 15 obtained their law degrees from Germany.

[46] In an empirical study analysing the patterns of foreign law citations by the Formosan Constitutional Court, it has been observed that 'justices with learning experiences in Germany are more likely to cite German constitutional laws whereas those with learning experiences in the United Stated more frequently cote American constitutional laws.' Wen-Chen Chang, 'Transnational Constitutional Dialogues: An Empirical Study on Foreign Law Citations by the Constitutional Court of Taiwan' in Shu-Perng Hwang (ed), *Constitutional Interpretation: Theory and Practice Vol 7 Part II* (Institutum Iurisprudentiae, Academia Sinica 2010) 483-518.

[47] According to the former Honourable Justice Tze-Chien Wang, the right to privacy is included in the concept of the right to personality. In other words, the right to privacy is merely *one* of the rights/ interests protected by the PDPL: the purpose of the PDPL is to protect the right of personality in relation to the *collection, processing and utilisation of personal data*. See: Tze-Chien Wang, 'The Issue and the Development of Protecting the Right to Personality (III): the Materialization of the Right to Personality and Its Scope' (2007) 97 Taiwan Law Journal 36.

[48] The official translation of the PDPL (in English) does not distinguish different ideas between personal data and personal information. The title of the PDPL, for example, is translated as the 'Personal Information Protection Act'. This error has repeatedly been made through the whole official English translation of the PDPL. See: < http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021 > accessed 24th April, 2011.

[49] Bert-Jaap Koops and Ronald Leenes, ''Code' and the Slow Erosion of Privacy' (2005) 12 Michigan Telecommunications and Technology Law Review 245.

subject) herself, it is through the data that the agent has impacts online.[50]

To strike a balance, accordingly, a series of new rules are suggested in the proposal in order to gain more **power of control for data subjects**. Indeed, early in the 2012 EU General Data Protection Regulation proposal, it is indicated that there are worries on behalf of the data subjects in relation to the loss of control of their personal data, which 'eats away at their **trust in online and other services** and holds back the growth of the **digital economy** in general.'[51] (original emphasis) In this regard, data subjects will have easier access to their own personal data; the right of data portability, i.e., easier to transfer of personal data from one data controller to another; and **the right to be forgotten**, i.e., the possibility to delete personal data if, for instance, there are no legitimate grounds for retaining it. These new rules with respect to data subjects' power of control over their personal data not only favour the trust element of data processing, but also reflect the rule-preclusionary conception of property.[52] This is therefore encouraged and hence fulfilled in the current GDPR, which reflects justified data subjects' autonomy and the will-conception of rights.

The notion of the right to be forgotten is particularly subtle and 'troublesome', as Townend argued, 'lawyers, archivists, historians and philosophers grapple with the theoretical and practical implications.'[53] Nevertheless, it must be noted that, the right to be forgotten has not been read as a natural right. Historically, not until the Charter of Fundamental Rights of the European Union is adopted, the data protection rights are not explicitly written in text. The included protection has then raises a series of debate over data protection reform. It was Viviane Reding, the European Commissioner, who gave a speech regarding the right to be forgotten, firstly, as a key part of Europe's data protection regime, caused an 'immense amount of comment.' [54] Two sets of issues can be identified:

1. The relationship between the right to forgotten and the right to forget

When dealing with relevant online issues, it was difficult to figure out how the new right would help with issues such as the greater powers of leading search engines and social medias, as well as the Big Brothers (governments) to set the terms of data collection. As commentators point out, this 'probably serves the purpose of (first-person) forgetting, more so than the desire to be forgotten.'[55]

It has been emphasised by Mayer-Schönberger, a leading legal expert of internet law with a

[50] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP, 2014) 179-181.
[51] European Commission, 'Why Do We Need an EU Data Protection Reform?' (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf> accessed 30 Janurary 2012.
[52] The principle argues that (1) Article 22 of the Convention on Human Rights and Biomedicine presupposes that we own our bodies in the rule-preclusionary sense; (2) unless we can own our bodies under the rule-preclusionary conception, we can own nothing in these terms; and (3) it is dialectically necessary for us to suppose that we own our bodies under the rule-preclusionary conception. See: Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001) 171-194.
[53] Townend J, "Data Protection and the 'Right to Be Forgotten' in Practice: A UK Perspective" (2017) 45 International Journal of Legal Information 28.
[54] Kieron O'hara, Nigel Shadbolt, and Wendy Hall, A Pragmatic Approach to the Right to Be Forgotten, in Global Commission on Internet Governance and Royal Institute of International Affairs, *Designing Digital Freedom: A Human Rights Agenda for Internet Governance* (2017), 77.
[55] Ibid.

popular book[56] that forgetting is overall beneficial to the society. He argues that 'human' memory benefits an agent, but the ability to forget is crucial as well. It used to be expensive and difficult to remember for human agents than to forget, but this has been changed in the digital age.[57] This is because the default is now to remember (which he named as 'digital memory'). Yet lining in the age of remembering is never easy in his view: with the passage of time, people change, ideas evolve and views adjust, but memories remain.[58] Hence, he proposed the technical solution of 'expiration dates', which contains the ideas of information expire and automatic deletion, to deal with the above problem.[59] This seems to be adopted by the later Google Spain case.

However, this essay should articulate the difference between the right to be forgotten and the right to forget. To be clear, it has been argued in the academic literature that the right to be forgotten at stake should be distinguished from the right to forget:[60]

> Z commits a faux pas in front of X and Y, X may forget, but Y may not (and then may remind X); Z's forgetting the event is neither here nor there. Not only is the forgetting of Z's faux pas a random event, but it is very unlikely to happen simultaneously over all rememberers; the collective memory, taken as the union of the memories of its members, is quite robust against forgetting.

In this scenario, it has rightly been distinguished that as the locus of forgetting is the remember.[61] This essay further argues that though the expire date is indeed, as Mayer-Schönberger puts, 'so central to what it means to be human,'[62] it is only one reason codified in the GDPR as 'no longer necessary.' I have argued that the central idea of the surrounding rights are the possibility and ability to control one's own data. Hence, if an agent chooses to preserve her own data forever, it might not be a good idea to have it automatically deleted.

2. The relationship between the right to be forgotten and the right to erase/ delete

A very initial debate on whether the right should be distinguished from the right to erase/ delete, or, it simply refers to better enforcement of the much more minor rights that are enshrined already in the Directive 95/46/EC.[63] To deal with the issue, what is the concept of the right to be forgotten must firstly be identified. Commentators, unsurprisingly have

[56] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009).
[57] Ibid, 197.
[58] See also: David John Harvey, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age*, (Hart Publishing, 2017), 289.
[59] Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (Princeton University Press, 2009) 198.
[60] Kieron O'hara, Nigel Shadbolt, and Wendy Hall, A Pragmatic Approach to the Right to Be Forgotten, in Global Commission on Internet Governance and Royal Institute of International Affairs, *Designing Digital Freedom: A Human Rights Agenda for Internet Governance* (2017), 75.
[61] Ibid.
[62] Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (Princeton University Press, 2009) 198.
[63] Reding claimed that a right to be forgotten would clarify and strengthen existing rights. See: ´Viviane Reding, "The EU Data Protection Reform: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age." Speech presented at the Digital Life Design Conference, Munich, January 24, 2012. Available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm. (Last visited: 20 June, 2018).

different ideas as the lack of defined context before the 2014 Google Spain Case[64] produced a vacuum[65] in this regard. Mayer-Schönberger, for example, on the basis of the principle of purpose of data protection, argued that all data **should** have an expiration date, so that forgetting became a default. [66]

Nevertheless, this remains too vague to determine, at least, whether the right can be distinguished as a new right. Considering the right to be forgotten as simply clarifying and strengthening/ expending the existing rights in Directive 95/46/EC, Reding[67] and Zanfir[68] claimed that **the right has already been implicit**. On the other side, Rosen argued that the 2012 GDPR proposal created 'a sweeping new privacy right' that threatens to the right of free expression on the internet.[69]

It has been argued by Bernal, for example, that the right to be forgotten is 'subtly but importantly' different form the right to delete (erase).[70] In his words, the former seems to be 'rewriting or erasing of history, or a kind of censorship, ' but the letter is about controlling of data, which, under proper understanding and implementation, is not in conflict with freedom of expression. From the aspect of duty, it is argued by him that we can impose duties (both moral and legal) to data controllers to delete/ erase data subject's data, but we cannot, theoretically and practically, impose duties on people to forget.[71] In his mind, as what this essay has justified, what does matter is the controlling abilities of data subjects to their own data. On the basis of the possibility of infringing on free speech, to Bernal, the right to be forgotten seems to be more 'dangerous', as he describes that the right to be forgotten which rewrites history is something that is a rejection of society and something ultimately undemocratic.[72]

The differences between the two rights identified by Bernal seem to be later confirmed in the CJEU judgment of the Google Spain decision. In that case the defence of Google Spain which states that the information was already public, and there was no right and, technically, no power to erase it. Given the reasons that (1) Google Spain was performing an extra privacy-relevant function, by bringing links to public information together on a single webpage; and (2) the information could be made available through the search engine as long as the

[64] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014 (ECLI:EU:C:2014:317).
[65] Christiana Markou, "The 'Right to be Forgotten': Ten Reasons Why it Should be Forgotten." In Reforming European Data Protection Law, edited by Serge Gutwirth, Ronald Leenes and Paul de Hert, (2014,Springer) 203–226.
[66] Viktor Mayer-Schönberger, (2009, Princeton University Press) *Delete: The Virtue of Forgetting in the Digital Age*.
[67] Viviane Reding, "The EU Data Protection Reform: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age." Speech presented at the Digital Life Design Conference, Munich, January 24, 2012. Available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm. (Last visited: 20 June, 2018).
[68] Gabriela Zanfir, "Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right." In Reforming European Data Protection Law , edited by Serge Gutwirth, Ronald Leenes and Paul de Hert, (2014, Springer) 227-249.
[69] Jeffrey Rosen, "The Right to be Forgotten." 2012 Stanford Law Review 88.
[70] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP, 2014) 177.
[71] Ibid.
[72] Ibid., 201.

searcher's interest was not in the person involved,[73] this defence was rejected by the Court. Hence, it can be argued that the Google Spain judgement considers that, as O'hara, Shadbolt, and Hall put:

> "forgetting" does not involve deletion, and so a right to be forgotten is distinct from a right to erasure. In that sense, the concept is somewhat closer to the notion of forgiving and moving on discussed earlier. Erasure is already a data protection right "where personal data storage is no longer necessary or is irrelevant for the original purposes of the processing for which the data was collected" (article 32 of the DPD). Furthermore, as this is a right, it is not necessary for the data subject to show that he has been harmed or the information is prejudicial; it is sufficient that he objects. However, it is accepted that archives have special requirements to hold information and to keep full records.

Moreover, on the basis of the judgement, it should be noted that as the search engines are simply searching the data and providing the related linkage of the URL of webpages but information itself owned by others, the duty to apply the right to be forgotten is **merely obliged to de-index the linkages of the webpages**.[74] De-indexing thus makes the personal data and information very difficult to locate and in a sense restores a significant element of obscurity.[75] In this respect, it should also be noted that, a purely technical and comprehensive solution to enforce the right to be forgotten in the open Internet is generally impossible.[76] On the basis of the above interpretation as such, it is plausible to imply that retaining such data (which should be forgotten) is acceptable (this is because, in the CJEU decision, forgetting does not involve deletion), but no further processing is allowed.

This article argues that, however, the right to be forgotten, should be interpreted as the same idea as the right to erase, but strengthening the right to erase after. This is because:

1. According to Art. 17 of the GDPR, the given title 'the right to erasure' is followed by a reference to the right to be forgotten between brackets.[77] Hence, rather than commentators who claims that the right to be forgotten is merely found in Art. 17 para. 2 of the GDPR, this essay argues that the scope of the right to be forgotten covers all paragraphs of Art. 17.

2. That being said, para. 2 is served as a specific component of what has already been referred in Art. 12 of the Data Protection Directive (DPD). This 'new' component can be understood as, under the age of internet and highly development of data science

[73] Kieron O'hara, Nigel Shadbolt, and Wendy Hall, A Pragmatic Approach to the Right to Be Forgotten, in Global Commission on Internet Governance and Royal Institute of International Affairs, *Designing Digital Freedom: A Human Rights Agenda for Internet Governance* (2017), 79.

[74] For the same interpretation in Formosan publications, see, e.g., Chi-wei Chang, Remember, Forget or Be Forgotten on the Internet: Review the Personal Data Protection in the Digital Age Based on the Decision of the Court of Justice of the European Union Regarding the Right to be Forgotten, 148 Chengchi Law Review 21-22.

[75] David John Harvey, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age*, (Hart Publishing, 2017), 288.

[76] For analyses of the technical problems in achieving the right see: The Right to Be Forgotten – Between Expectations and Practice (European Network and Information Security Agency (2011) available at https://www.enisa.europa.eu/publications/the-right-to-be-forgotten (last visited: 20/06/2018).

[77] See also: Herke Kranenborg, 'Right to Erasure ('Right to Be Forgotten)', Christopher Kuner, Lee Bygrave and Christopher Docksey. "Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)" Commentary on the EU General Data Protection Regulation (GDPR) 60.

applications, a specific basis of claim right. Such component aims to remove the showing of the list of the results produced by the search engine when searching data subject's personal data: 'to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.'[78] In other words, this is simply the right to restrict the access to information and personal data: take **reasonable** measures with consideration of the circumstances at issue to inform all data controllers who are further responsible for the data processing that all links to this personal data, including copies or replicates, must be erased. However, the publicised document itself, which is not addressed in the Google Spain case as the responsibility of the publisher of the website was not at issue, together with the removal of the searching results, can be dealt with the right to be erase. This essay, therefore, argues that the component is, indeed, not so 'new' but specifically providing a stronger method to assist the success of the right to erase in the age of internet and social media.

3. From the reading of the entire regulations in both Art. 17 and Art. 19 of the GDPR, neither the right to erase nor the right to be forgotten, in any case, is an absolute right. This has been put on the recital 4 of the GDPR that '[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.' The main challenge regarding the right to be forgotten in the Google Spain case, obviously, was its relationship and balance with the freedom of expression/ press.[79]

Looking at Art. 3 and Art. 11 of the PDPL, there are regulatory wordings regarding the right to delete. It seems plausible for Taiwan to maintain its current legislation with respect to the concept of the right to be forgotten enshrined by the GDPR. However, this is simply a premature judgement, because the data subjects are unable to request the search engine to de-link their personal data on the basis to the following grounds:

1. The data subject withdraws consent where there is no other legal ground for the processing；[80] (Art. 17 (1) (b))

2. The data subject objects to the processing and there are no overriding legitimate grounds for the processing (Art. 17 (1) (c));

3. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) regarding child's consent in relation to information society services (Art. 17 (1) (f));

4. and the requirement to inform controllers who process the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data on the basis of available technology and the cost of

[78] Art. 17 para. 2, GDPR.
[79] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González. 2016, Case C-131/12. CJEU Grand Chamber. para 85.
[80] As the essay has put, the rights covered by data protection is a will-conception of right with possibility to waive, and hold again such a right.

implementation with reasonable steps including technical measures. (Art. 17 (2))

Consequently, it is ill-founded to argue that current Formosan PDPL regarding the right to delete is legally identical to the GDPR. However, it should be noted that there are quite a few exceptions in connection with the right at issue. In this regard, it remains unsolved in the Google Spain case to strike a balance between the right to be forgotten and its exceptions, e.g., mainly freedom of expression and freedom of press, where that right could be overridden.[81]This will be further discussed in the next section.

3.2 The Right to Be Forgotten and Its Competing Rights

We have learnt that the right to erasure (the right to be forgotten) is not an absolute right. Striking a balance between the right to be forgotten (or any other rights under the conception of data protection rights) and competing rights, e.g., the freedom of expression, however, is by no means a new issue. It has been acknowledged that there is indeed a 'culture gap' regarding the balance of the competing rights between the US and Europe.[82] Following the European model, to deal with balancing test in connection with the right at stake under the GDPR, this essay has argued that to figure out the notions and interpretation of the GDPR by reading relevant (past and future) decisions of the CJEU, the ECHR and judgements of the ECtHR are of central importance. It is thus reasonable to look at the ECtHR decisions for further reference.

Apart from the Google Spain case of the CJEU, *Węgrzynowski and Smolczewski v. Poland* of the ECtHR[83], has been exemplified by academic commentators to deal with competing rights under Articles 8 and 10 of the ECHR.[84] Specifically, the balance is demanded between the right to respect for private life (including the right to privacy and data protection rights) and the right to freedom of expression, both of which require equal respect by the court. In this regard, it has been concluded by the Court to accept the reasoning of the Warsaw Regional Court that 'it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations.'[85] It is thus concluded that it is not for the courts to remove from the public domain **all** traces of publications but in a reasonable sense.

Indeed, it can be found that the Court expands freedom of expression in this case and it is true that the (not very new) right to be forgotten as well as the right to erase are not intended to suppress freedom of express, information and media. However, it is arguable that such

[81] See, e.g., Meg Leta Ambrose and Jef Ausloos, "The Right to be Forgotten Across the Pond," Journal of Information Policy, 2013, 3: 1-23, cited from Kieron O'hara, Nigel Shadbolt, and Wendy Hall, A Pragmatic Approach to the Right to Be Forgotten, in Global Commission on Internet Governance and Royal Institute of International Affairs, *Designing Digital Freedom: A Human Rights Agenda for Internet Governance* (2017), 77.
[82] Michael J. Kelly and David Satola, The Right to Be Forgotten (May 9, 2017). University of Illinois Law Review, Vol. 1, 2017, 38.
[83] Węgrzynowski and Smolczewski v. Poland - 33846/07 Judgment 16.7.2013.
[84] Herke Kranenborg, 'Right to Erasure ('Right to Be Forgotten)', Christopher Kuner, Lee Bygrave and Christopher Docksey. "Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)" Commentary on the EU General Data Protection Regulation (GDPR) (2019) 62.
[85] Para. 65.

direction has been fully brought into the CJEU, in particular the Google Spain case and further illustrations.

Art. 17 of the GDPR has thus provided us some hints by stating that the right to have one's personal data erased/ to be forgotten without undue delay applies: (a) the personal data are no longer necessary regarding the purposes for which they were collected or otherwise processed; (b) the data subject withdraws the consent on which the processing is based and there is no other legal ground for the processing; (c) the data subject objects to the processing and there are **no overriding legitimate grounds** for the processing; (d) the personal data have been **unlawfully processed**; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected concerning the offer of information society services to children pursuant to Article 8 of the GDPR.

The above six grounds are actually overlapping. Kranenburg argues that due to 'recital 65 in which it is stated that the right to erasure can be invoked by a data subject, where the processing of his or her personal data does not otherwise comply with this Regulation', Art. 17(1)(d) can be seen as a general clause of the right.[86] To identify legal obligations and to further ensure necessity of the purpose consisted by Art. 17(1), it must be noted that 'the burden of proof following an objection has switched; instead of the data subject, the data controller has to demonstrate compelling legitimate grounds for processing the data.'[87]

Reconciling the rights, therefore, one should look at 'the nature of the data in question, its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life'.[88] A handful of descriptions can be sketched in this regard. First, as a special component of the right to erasure, the scope of the right shall be narrow thus related merely to search engines and provides limited searching results to have personal information. Secondly, to strike a balance between competing rights, the original materials of expression may, under certain circumstances, be unnecessary to be deleted whilst it is difficult if not almost impossible for a modern agent who lives in the age of internet to locate personal data with ease. Thirdly, as the right under the will-conception, it is both positive and negative. Furthermore, in such a case, *only* data subjects can voluntarily waive the benefits by their free choice when not interfering with their duties to other individuals or organisations. Hence, in carefully considering requests to de-link, it is crucial to be sure that what waived here is the benefits of being remembered, whether true or not.

To look at reconciling on the basis of Art. 17(1)(d) of the GDPR, alternatively, it is logical to ensure when the data should be subject to have such a right to be overridden. It has been

[86] Herke Kranenborg, 'Right to Erasure ('Right to Be Forgotten)', Christopher Kuner, Lee Bygrave and Christopher Docksey. "Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)" Commentary on the EU General Data Protection Regulation (GDPR) (2019) 63.
[87] Ibid.
[88] Case C-131/12, Google Spain, at paras. 81 and 97. See on this also Kranenborg 2015, pp. 77-79. More hints can also be found by reading the WP29 guidelines on the implementation of the Google Spain ruling. See: Article 29 Working Party (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Brussels, 26 November 2014.

categorised by Bernal that there are six main (but non-exclusive) sorts of scenarios that such right may be limited in a proportionate[89] way: (1) for the data subject's own good[90]; (2) for communication; (3) for administrative and economic; (4) for keeping a good, accurate, and useful historical record; (5) for security; and (6) for **freedom of expression**.[91] This can be again observed in Art. 17.3 of the GDPR, in which the right to erasure shall not apply to the extent that processing is necessary.

To strike a balance whenever the rights are competing, outcome of a request may differ depending on the case at stake. Therefore, assessments need to be carefully made on a case-by-case basis with a dynamic and rather uncertain relevance for competing rights. Specifically, for instance, the Information Commissioner Office (ICO) of the UKs, through its report as an interpretation, concluded a criterion with a series of themes. For example, it is proposed that 'the public interest in information about public figures is stronger',[92] which corresponds to the J.Y. Interpretation No. 689 of the Formosan Constitutional Court. However, there is no standard to decide the publicity, but again, on a case-by-case basis, to decide whether the individual play a role in public life. It is followed by the opinion on the basis of the minimum principle, that the less the data reveals about someone's private life, the more likely its availability in search results is accepted by the ICO.[93] Moreover, in connection with criminal records,[94] the ICO considers again on a case-by-case basis, but is likelier to favour de-indexing for cases 'that are more minor, and that happened longer ago.'[95]

4. What Shouldn't Be Forgotten: A Theorised Regulatory Framework

4.1 Data Abusing: Function Creep

This essay has demonstrated that the right to erasure itself was facing challenges from new tech, thus the EU has made it clear that the right to be forgotten can assist to deal with the issue – it is increasingly difficult for data to subject to. It should be clarified that, while data-related science and technologies develop rapidly, how to deal with the data applications regarding 'function creep'. Can the right to be forgotten capable of assisting perfectly?

'Function creep,' i.e., further unintended or unnecessary processing of personal data in a way incompatible with the original purpose for which it was collected, is the most significant concern regarding modern data-tech applications (a buzzword on its own), e.g., Big Data, Artificial Intelligence, Machine Learning. Function creep happens not only with the knowledge or consent of data subjects, but also without the active involvement of data subjects. Function creep, by its nature, raises an obvious problem in that it goes against the principle of obtaining personal data for specific, explicit and lawful purpose(s) and processing

[89] Andrew Scott, An unwholesome layer cake: intermediary liability in English defamation and data protection law. In: Mangan, and Gilles , (eds.) The Legal Challenges of Social Media. (Edward Elgar, 2016), 240.
[90] Bernal named that it is a 'paternalistic reason' to limit the right to delete where ' it is in the individual's interest that the data be kept', e.g., one's medical data. Ibid.
[91] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP, 2014) 202.
[92] ICO, ' Overview of the General Data Protection Regulation (GDPR)', July 7, 2016.
[93] Ibid.
[94] It shall be noted that the criminal record is a sort of sensitive personal data in both the EU and Formosan data protection law regime.
[95] ICO, ' Overview of the General Data Protection Regulation (GDPR)', July 7, 2016.

it in a compatible manner.[96]

Function creep thus generates privacy and data protection concerns. 'Profiling' refers to the profiling of individuals' behaviour, which relates to one's information privacy by linking individuals to personal data. Profiling could be carried out through data mining. For example, biometric database with passengers' record could figure out, in particular with the use of technologies such as Big Data, how regular one visits a particular place, etc. This is different from another specific type of abuse of personal data, namely 'tracking', referring to 'the ability to monitor in real time an individual's actions or to search databases that contain information about these actions'.[97] Briefly, tracking specifies the question 'where was/is she/he?' and profiling probes that 'why she/he was/is there?'

By looking at the contents of the right to be forgotten, this essay finds out that such a right is capable of controlling potentional personal data leaks, e.g., secondary disclosures and used as a source of personal data. Although the action of collecting and processing personal data serves, at least possibly, the original purpose, it must be done in an adequate, relevant and reasonable manner. Accordingly, *unless such a purpose aims to protect an absolute right and is the proportional method of achieving the goal*, it can hardly be accepted that an overall or any unnecessary extent of the 'image of an individual's personality' is needed for any purpose.

However, it seems to the author that, technically, future misuse of profiling data and those original personal data may not be possible to be FULLY forgotten in the era of Big Data. Nevertheless, with respect to the risks of future misuse, Lord Steyn of the UK Court holds the opinion that '[i]f future scientific developments require it (i.e., contemporary use of retained samples in connection with the detection and prosecution of crime), judicial decisions can be made, when the need arises, to ensure compatibility with the ECHR.'[98] It must be, therefore, very clear that the right to be forgotten is a legal idea (with legal consequences) rather than a technical idea which may never be achieved.

In this regard, a category of data would need to be highly concentrated apart from the data in the Google Spain case regarding the right to be forgotten: 'not just data that data subject has the right to delete, but data to which attention must be drawn and for which there is a simple, direct and clear method for deletion.[99]' To articulate, though the Google Spain case presents merely pre-stage of profiling, namely large-scale searching, collecting, and retention of personal data, such an act is essential for later stages of profiling. This essay thus further argues that the coverage scope of the right to erasure (the right to be forgotten) should not only include the deletion of the original personal data documents/ materials and de-linking websites from the searching engine to have a search result changed, but also the profiled

[96] Article 5.1 (b) of the GDPR: Member States shall provide that personal data must be: 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');.'

[97] John D. Woodward and others, *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns* (RAND Publications 2001) 24-25.

[98] *R v Chief Constable of South Yorkshire* [2004] UKHL 39 para 28. Lord Brown also agrees this viewpoint, see: ibid para 86.

[99] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP, 2014) 204.

information, whether the profiling is processed by the machine automatically or not. The reasoning behind this argument goes as follows.

1. Such sort of personal directly related to the data subject's (as an agent) autonomy. Hence, the possibility to generate risks and actual harms is rather high. As Paul de Hert observes that '[p]rivacy and human dignity must preserve the roots of the individual's autonomy against outside steering or against disproportionate power balances in vertical, but also in horizontal power relations,'[100] there is a need to deal with the question stems from the interference on the individual's autonomy and free will of choice. This should be particularly noted that, in an *unbalanced* power, relations which threatens not only human rights and freedoms, but also 'the very nature of our society.' [101]

2. The profiling data can be collected and processed for further profiling. This can harm the main purpose of data minimisation e.g., 'extending data retention for further unlimited periods.'[102]

3. Scientists or pro-scientist commentators with 'extremely positive' attitude toward technology applications tend to have proponents which are not giving adequate thought to the consequences if they fail.[103] Two plausible choices they may have in this regard. First, they may argue that restriction on profiling is more or less acceptable, but such limitations should not 'block' the developments of scientific research and its value-added applications. Second, they may even abandon regulation and assume that technological prospects might/ be able to dictate the 'right direction' or to try at least to 'hold the regulatory line, concentrating resources on the most serious violations.'[104] However, this is simply not the way the GDPR accepts: '[t]echnology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a **high level** of the protection of personal data.[105]

4.2 A Proposed Regulatory and Institutional Framework

As a preliminary matter, it should be noted that both Taiwan's academic lawyers and policymakers have adopted elements of western jurisprudence, particularly the German system. This results in a rather complex hybrid legal regime.[106] Under no circumstance is the assessment of the fluid nature of the right to privacy in Taiwan able to avoid these systematic complexities.

The European countries and Taiwan share a high level of similar protection of personal data

[100] Paul de Hert, 'Biometrics at the Frontiers: Assessing the Impact on Society' <http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/iptsBiometics_FullReport_eur21585en.pdf> accessed 29 June 2018.
[101] Ibid 91.
[102] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP, 2014) 204.
[103] Daniel J. Solove, *Nothing to Hide: the False Tradeoff between Privacy and Security* (Yale University Press 2011) 199.
[104] Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (OUP 2008) 315.
[105] Recital 6 of the GDPR.
[106] Chung-Lin Chen, 'In Search of a New Approach of Information Privacy Judicial Review: Interpreting No. 603 of Taiwan's Constitutional Court as a Guide' (2010) 20 Indiana International and Comparative Law Review 27.

by having a main regulatory provision. In the EU it was the Data Protection Directive and the current GDPR. As regards to the main data protection regulatory instrument in Taiwan, since the Personal Data Protection Law (as well as the former Computer-Processed Personal Data Protection Law) is profoundly influenced by the European model, it is inevitable that they share a great number of common regulatory methods. For example, the main legal protection bases both aim to protect fundamental rights and freedoms of individuals/ the right to personality, and in particular their right to privacy with respect to the collection, processing and use of personal data.

It has been suggested by the WP29 (of the EU) and the 1981 Data Protection Convention[107] of the Council of Europe that a number of basic data protection principles, e.g., the principle of purpose specification, the principle of proportionality, and the principle of precautionary,[108] have to be taken into account when processing biometric data.

Reflecting the influential European model, the PDPL also covers a number of general data protection principles. As regards to biometric data, it is stated by the Human Biobank Management Act in its Article 20 that '[a]ny use of biological specimens, derivatives and relevant data and information in the Biobank shall not be used for purposes other than biomedical research.'

However, such principles are inevitably followed by a number of exceptions. A more detailed comparison between the European and Formosan provisions will be provided in the next subsection, focusing on the differences.

Overall, looking micro-comparatively at the developing technologies at hand, the Formosan regulatory tools are similar to the European ones. However, it is referred by the Constitutional Court that '[d]espite the admissibility of other nations' similar legislations and domestic popular polls as materials used in interpreting the Constitution, they cannot be used as the sole basis of determining the meanings and intents thereof.'[109] This is particularly true in terms of the complex hybrid Taiwanese legal regime. It is thus unsurprising to find that some local commentators may criticise the fact that the European model of regulating personal data is impractical due to the rigid approach of seeking maximum privacy protections, which can become a barrier to the free flow of information.[110] Many local commentators thus hold the opinion that the European model may not be suitable for Taiwan.

---

[107] The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (*T-PD*, 2005) <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf> accessed 13 June 2018.

[108] Working Document on biometrics, 1 August 2003, available at:
< http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf >, accessed 14 May 2011. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (*T-PD*, 2005) <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf> accessed 13 February 2010.

[109] J. Y. Interpretation No. 603.

[110] Ming-Li Wang, 'Information Privacy in a Network Society: Decision Making Amidst Constant Change' (2010) 5 National Taiwan University Law Review131-136.

However, I argue that there is a need to re-affirm the European model in the Formosan data protection regime.[111] This is because:

a. Although the European model has set a high standard for protecting the right to (informational) privacy, it is not prohibitive since such a right is a fundamental right. On the contrary, it is welcomed.

b. It must not be forgotten that one of the very fundamental purposes of the Data Protection Directive is to *improve the information flow*. With this in mind, in Recital 3 of the GDPR re-claims that 'Directive 95/46/EC of the European Parliament and of the Council seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.' Indeed, the improvement of the information flow and privacy are two sides of the same coin. Therefore, there seems to be a misunderstanding behind the objection to the GDPR on the grounds that it places greater emphasis on the protection of personal data rather than the free flow of information. Meanwhile, the WP29 addresses that the interpretation should not be 'unduly restricted' or 'overstretched.'[112]

c. The benefits of this right can be waived by valid consent under the will-conception, thus conflict between the rights and interests does not necessarily arise; and when there is actually a conflict between values regarding advances of science and technology and privacy and data protection values, without a valid consent, there is a violation of the right to privacy and the right to data protection unless there is a substantive justification.

On the other hand, the practice and the enforcement of the right to be forgotten as well as all rights covered by the data protection regime in Taiwan will need, proposed by this essay, to have an independent supervisory authority. It is because, for example, there must be a governmental authority to effectively deal with disputes and removal against the search engine. The independent supervisory authority has been indicated in the Directive as the main safeguard on data protection in Europe. It has been suggested that the national supervisory authority in each Member State plays multi-functional role as the promoter, the guardian, and the defender of the data protection. Some regulatory safeguards in the Directive such as prior checking of processing operations (Article 20) and notification (Article 18) are essentially related to such authorities. To be more specific on the processing of biometric data at the domestic level, for example, several European countries require that processing biometric data for the health purposes must be checked or authorised by an Ethics Committee and supervisory authority.[113]

Crucially, it is stated by Article 45(2)(b) that any transfer of personal data to a third country (or an international organisation) may take place where the European Commission 'has decided that the third country, a territory or one or more specified sectors within that third

[111] See also: Directorate-General Justice European Commission, Freedom and Security,, 'Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments' (2010) <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf> accessed 30 Janurary 2012, para. 27.
[112] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data* (No 01248/07/EN, WP136, 2007) 5-6.
[113] Rouillé-Mirza and Wright 222-223.

country, or the international organisation in question ensures an adequate level of protection', including the assessment of 'the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States.'

However, the Formosan data protection regime is quite different from the European model in this regard – there is no supervisory authority responsible for the application of the PDPL. Article 25 of the PDPL simply states that

> [f]or the non-government agency that violates the provisions of this Law, one of the following actions may be ordered jointly with a fine *as regulated by the government authority in charge of subject industry* at the central government level, municipality directly under the central government, or county or city government…

This evokes radically divergent views.

Perhaps the most common characteristic shared by the data protection regimes worldwide is that there is always a gap between the law and the explosive growth of technology. This problem might be tackled to some extent by the government authorities themselves rather than an 'outsider,' since those authorities are: (1) usually more professional to specific technologies than those law makers in general; and (2) easier to make quick and targeted responses.[114] Accordingly, it might be argued that the Formosan model is easier to manage and to adapt to data protection concerns in connection with specific technologies. For example, it less likely for law experts in the Ministry of Justice to be aware of the possibility of function creep problem in the private field, yet the scientific experts under the Ministry of the Economic Affairs may identify and deal with these issues more easily.

However, what appeared in the first reading of such a flexible management model in Taiwan has emerged as a tangled set of experiences that reflected quite the opposite to what was intended. As might be easily assumed, public agencies have adopted quite different strategies to meet the PDPL requirements and have developed diverse interpretations and decisions in relation to similar cases. For example, for public officials in scientific capacity, the worship of the 'research privilege' cannot be totally avoided. In contrast, the authorities regulating the media and press may try to be more favourable towards privacy concerns (or any other competing interests such as protection of minors) on the basis of trends towards higher supervision. This thus commits a hydra-headed bureaucracy problem. Based on the inefficient and problematic experiences of the PDPL and considering the integrity of the whole data protection framework, Taiwanese scholars suggest that the law-makers should follow the European approach to establish a supervisory authority to supervise this area.[115]

5. Conclusion

[114] Wang 146, cited from Richard Stewart, 'Reformation of American Administrative Law' (1975) 88 Harvard Law Review 1669.
[115] However, this is not accepted by the legislators when amending the law.

The central aim of this essay is to evaluate the concept of the right to be forgotten. Having set out the background in the introduction, this essay then turned to its main theme.

1. identify and justify an adequate theoretical framework to probe and evaluate the current European GDPR

It has been argued by this essay that to look at the right to be forgotten enshrined in the GDPR and to deal with the forthcoming collisions of the new GDPR rights, it is therefore essential to understand how the ECtHR examine the ECHR, in particular Article 8 regarding the right to private life. The standard formula consistently followed by the Court can be presented in the sub-stages requiring the evaluation of the *principle of proportionality.*

Moreover, the author argues that data protection rights including the right to be forgotten are rights under will-conception. In this respect, agents can waive the benefits of the fundamental rights and freedoms and duties imposed on other agents are both positive and negative. In this case, the understanding that fundamental rights and freedoms operate under the will-conception principle entail that an agent can waive the benefits of generic rights if they wish to do so, but on the basis of permitting an informed agent to engage freely in activities that are not favourable to the interests of the agent protected by fundamental rights and freedoms.

2. examine issues regarding striking a balance between competing rights and technical applications

The right to be forgotten has not been read as a natural right. This essay has distinguished the difference between the right to be forgotten and the right to forget. Furthermore, the author argues that the right to be forgotten, should be interpreted as the same idea as the right to erase, but strengthening the right to erase after. However, it would be wrong to consider that Formosan government to maintain its current legislation with respect to the concept of the right to be forgotten enshrined by the GDPR.

On the other hand, although the right to erasure (the right to be forgotten) is not an absolute right, reconciling the competing rights is never easy. To strike a balance whenever the rights are competing, outcome of a request may differ depending on the case at stake. Therefore, assessments need to be carefully made on a case-by-case basis with a dynamic and rather uncertain relevance for competing rights.

3. produce a coherently theorised regulatory framework for Formosan data protection law regime.

To deal with the data applications regarding ‘function creep’, the right to be forgotten might be helpful. It seems to the author that, technically, future misuse of profiling data and those original personal data may not be possible to be FULLY forgotten in the era of Big Data. It must be, therefore, very clear that the right to be forgotten is a legal idea (with legal consequences) rather than a technical idea which may never be achieved. This essay thus further argues that the coverage scope of the right to erasure (the right to be forgotten) should not only include the deletion of the original personal data documents/ materials and de-linking websites from the search engine to have a search result changed, but also the profiled information, whether the profiling is processed by the machine automatically or not.

As regards to the data protection law regime in Taiwan, I argue that there is a need to re-affirm the European model in the Formosan data protection regime. Moreover, the practice and the enforcement of the right to be forgotten as well as all rights covered by the data protection regime in Taiwan will need, proposed by this essay, to have an independent supervisory authority.

Bibliography

1. Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data* (No 01248/07/EN, WP136, 2007)
2. Bert-Jaap Koops and Ronald Leenes, ‘'Code' and the Slow Erosion of Privacy’ (2005) 12 Michigan Telecommunications and Technology Law Review 245.
3. Case 181/73 *Haegeman v Belgium* [1974] ECR 449
4. Case 29/69 *Stauder v. City of Ulm* [1969] ECR 419
5. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014 (ECLI:EU:C:2014:317)
6. Case C-239/03 *Commission v. France (Etang de Berre)* [2004] ECR I-9325,
7. Case C-286/90 *Anklagemyndigheden v. Poulsen and Diva Navigation* [1992] ECR I-6019
8. Cases C-465/100, 138 and 139/01 *Rechnungshof v. Österreichisher Rundfunk* [2003] ECR I-12489
9. Christiana Markou, “The ‘Right to be Forgotten’: Ten Reasons Why it Should be Forgotten.” In Reforming European Data Protection Law, edited by Serge Gutwirth, Ronald Leenes and Paul de Hert, (2014,Springer) 203–226.
10. Chung-Lin Chen, ‘In Search of a New Approach of Information Privacy Judicial Review: Interpreting No. 603 of Taiwan's Constitutional Court as a Guide’ (2010) 20 Indiana International and Comparative Law Review 27
11. Daly, Angela, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart 2016)
12. Daly, Angela, The Internet, User Autonomy and EU Law. Private Power, Online Information Flows and EU Law: Mind the Gap (Hart 2016)
13. Daniel J. Solove, *Nothing to Hide: the False Tradeoff between Privacy and Security* (Yale University Press 2011)
14. David Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd edn, OUP 2002)
15. David John Harvey, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age*, (Hart Publishing, 2017)
16. Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001)
17. Deryck Beyleveld and Shaun D. Pattinson, ‘Moral Interests, Privacy, and Medical Research’ in Michael Boylan (ed), *International Public Health Policy and Ethics* (Springer Netherlands 2008)
18. Deryck Beyleveld, ‘Conceptualising Privacy in Relation to Medical Research Values’ in Sheila AM McLean (ed), *First Do No Harm: Law, Ethics and Healthcare* (Ashgate Publishing 2006) 155.
19. Deryck Beyleveld, ‘The Principle of Generic Consistency as the Supreme Principle of Human Rights’ (2012) 13 Human Rights Review 12
20. Foundation for Information Policy Research, *Paper No. 4: The Legal Framework: an Analysis of the "Constitutional" European Approach to Issues of Data Protection and Law Enforcement* (UK Information Commissioner Study Project: Privacy & Law Enforcement, 2004)
21. Francesca Bignami, ‘Transgovernmental Networks vs. Democracy: The case of the European Information Privacy Network’ (2005) 26 MICH J INT’L L 807.
22. Fred H. Cate, Peter Cullen & Viktor Mayer-Schönberger (2014). “Data Protection

Principles for the 21st Century: Revising the 1980 OECD Guidelines." https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf (accessed May 11, 2018).
23. Gabriela Zanfir, "Tracing the Right to be Forgotten in the Short History of Data Protection Law: The 'New Clothes' of an Old Right." In Reforming European Data Protection Law , edited by Serge Gutwirth, Ronald Leenes and Paul de Hert, (2014, Springer) 227-249.
24. Google, Transparency Report, available at: https://transparencyreport.google.com/eu-privacy/overview?hl=en_GB, (last visited: 23 June 2018).
25. Herke Kranenborg, 'Right to Erasure ('Right to Be Forgotten)', Christopher Kuner, Lee Bygrave and Christopher Docksey. "Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)" Commentary on the EU General Data Protection Regulation (GDPR)
26. ICO, ' Overview of the General Data Protection Regulation (GDPR)', July 7, 2016.
27. J Raz, *The Morality of Freedom* (OUP, 1988)
28. Jeffrey Rosen, "The Right to be Forgotten." 2012 Stanford Law Review 88.
29. Joel Reidenberg, 'Setting Standards for Fair Information Practice in the U.S. Private Sector' (1995) 80 IOWA L REV 497, 500.
30. John D. Woodward and others, *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns* (RAND Publications 2001)
31. Kieron O'hara, Nigel Shadbolt, and Wendy Hall, A Pragmatic Approach to the Right to Be Forgotten, in Global Commission on Internet Governance and Royal Institute of International Affairs, *Designing Digital Freedom: A Human Rights Agenda for Internet Governance* (2017)
32. Lord Hoffmann, 'The Influence of the European Principle of Proportionality upon UK Law' in Evelyn Ellis (ed), *The Principle of Proportionality in the Laws of Europe* (Hart Publishing 1999)
33. Meg Leta Ambrose and Jef Ausloos, "The Right to be Forgotten Across the Pond," Journal of Information Policy, 2013, 3: 1-23
34. Michael J. Kelly and David Satola, The Right to Be Forgotten (May 9, 2017). University of Illinois Law Review, Vol. 1, 2017, 38.
35. Ming-Li Wang, 'Information Privacy in a Network Society: Decision Making Amidst Constant Change' (2010) 5 National Taiwan University Law Review131-136.
36. N. A. Moreham, 'The Right to Respect for Private Life in the European Convention on Human Rights: a Re-examination' (2008) 1 EHRLR 45-46.
37. Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP, 2014)
38. Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP, 2014)
39. Paul Craig and Gráinne De Búrca, *EU Law: Text, Cases and Materials* (5th edn, OUP 2011)
40. Paul de Hert, 'Biometrics at the Frontiers: Assessing the Impact on Society' <http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/iptsBiometics_FullReport_eur21585en.pdf> accessed 29 June 2018.
41. Peter Blume, 'Will it be a better world? The proposed EU Data Protection Regulation' (2012) 2 International Data Privacy Law 130-136.
42. *R v Chief Constable of South Yorkshire* [2004] UKHL 39 para 28.
43. Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (OUP 2008)
44. Solon Barocas and Helen Nissenbaum, Big Data's End Run around Anonymity and Consent, in Privacy, Big Data, and the Public Good Frameworks for Engagement, Edited

by Julia Lane, Victoria Stodden, Stefan Bender (CUP, 2014)

45. Stephen Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation* (Martinus Nijhoff Publishers 2008)

46. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (*T-PD*, 2005) <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Biometrics_2005_en.pdf> accessed 13 June 2018.

47. The Right to Be Forgotten – Between Expectations and Practice (European Network and Information Security Agency (2011) available at https://www.enisa.europa.eu/publications/the-right-to-be-forgotten (last visited: 20/06/2018).

48. Tze-Chien Wang, 'The Issue and the Development of Protecting the Right to Personality (III): the Materialization of the Right to Personality and Its Scope' (2007) 97 Taiwan Law Journal 36.

49. Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009)

50. Viviane Reding, "The EU Data Protection Reform: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age." Speech presented at the Digital Life Design Conference, Munich, January 24, 2012. Available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm. (Last visited: 20 June, 2018).

51. Węgrzynowski and Smolczewski v. Poland - 33846/07 Judgment 16.7.2013

52. Wen-Chen Chang, 'Transnational Constitutional Dialogues: An Empirical Study on Foreign Law Citations by the Constitutional Court of Taiwan' in Shu-Perng Hwang (ed), *Constitutional Interpretation: Theory and Practice Vol 7 Part II* (Instit 世 utum Iurisprudentiae, Academia Sinica 2010) 483-518.

53. Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer 2010)

翁逸泓
（世新大學助理教授）

中文摘要

本文期能基於歐盟一般個資保護規則(General Data Protection Regulation, GDPR)而檢視「被遺忘權」在臺灣與歐洲法規範下之內涵。本文認為基於歐洲人權法整體架構，歐洲人權法院之詮釋方法有助於被遺忘權內涵之區辨，並且，基於意志論(will-conception)之理論內涵，才是正確之理解。就被遺忘權之內涵本身言，本文認為事實上與刪除權之內涵同一，只是解釋上更擴張其在數位時代之適用範圍與實現方式。不過就臺灣目前狀況來看，雖然個資法規範了刪除權，但是卻並無法真正地實現被遺忘權。

而就與其相競合之權利，例如表意自由權言，個案審查仍為當前之態樣。再就基於個人資料加值利用的功能潛變與人格剖析問題，本文認為被遺忘權應當更近一步地適用於剖析(profiling)。最後，本文認為臺灣在法規面上應更盡力彌平與歐盟個資保護模式之落差，而成立一個獨立之專責管制機關係為當務之急。`