Commentary on *The Right to be Forgotten: Forget about It?*

Wen-Tsong Chiou, Associate Research Professor, Academia Sinica

Sharing a similar appearance with the right to erasure, the right to be forgotten (RTBF) is very often considered to be new wine in old bottles. Not only as a liberty right but also a claim right to impose obligations on others, RTBF is yet another exemplar of the right to control one's personal data, which is commonly thought to be the core of a more fundamental right to informational privacy. Its multifaceted nature, however, suggests that RTBF actually has many different roots and serves different interests. In this commentary, I will argue that seeing RTBF as simply one expression of individual will or choice that conveys an agent's self-interests or preferences wrongly dilutes its real significance. Because RTBF, as such, is no more than a permission or even an order to rewrite or erase history merely for personal purposes, it could easily be outweighed by competing interests such as public's right to know or the freedom of speech that opposes obscurity and contest any form of censorship. Instead, RTBF should be understood as a tool for social rehabilitation as well as resistance to the threat to personal independence in an era of big data and algorithms. Such a revised version of RTBF pushes us to think more deeply about the democratic values to which RTBF can contribute and to delineate more properly the extension and intension of the concept.

RTBF as an Omnibus Right to Erasure

The term "right to be forgotten" is not explicitly used in any statutory law in Taiwan. To the extent that the concept is understood as about the erasure of personal data and the prohibition of its further dissemination, a more conventional right to request deletion of personal data, which is clearly stated in the Personal Data Protection Act (PDPA), is the long-existed basis of the relatively new term. Article 11 of the PDPA provides that data controller shall, on its own initiative or upon the request of the Party, delete personal information collected when the specific collection purpose no longer exists, or when the authorization of data use expires, or in cases when the data collection, processing, or data use is in violation of the provisions of this Act. Because the PDPA does not explicitly mention about the withdrawal of data subject's consent as a legal basis for requesting the deletion of personal information, and the Ministry of Justice, which was the authority in charge of the interpretation of the law, only expounded that the data shall not be *further processed* once the consent is withdrawn,[1] it remains an untested hypothesis that the withdrawal of consent would entail the mandatory deletion of personal information even though the data is still processed in a way compatible with its specific collection purpose.

Under the PDPA, the right to request deletion of personal data would be honored when the specific collection purpose no longer exists, or when the authorization of data use expires, or in cases when the data collection, processing, or data use is in violation of the provisions of this Act. However, under the current law, the need for secondary uses of data collected

[1] Ministry of Justice Interpretation Letter No. 10403508020 (July 2, 2015).

originally on grounds other than individual consent may trump individual's right to request deletion of personal data. For example, several individuals jointly filed a law suit requesting the National Health Insurance Administration (NHIA), which is authorized by law to collect personal medical data for the purpose of health insurance payment, to cease processing their data for secondary medical research uses and to delete such data from a research database. As a single-payer mandatory social insurance run by NHIA, Taiwan's National Health Insurance (NHI) provides a universal coverage for its 23 million people. Collection of personal data for each and every NHI service is required by law with a specific purpose of approving insurance claims.[2] The tremendous volume and the centralized nature have made NHI data invaluable treasures for those who are eager to make the best use of large-scale health information and big data analytic tools. Since 2011, the NHIA has begun to provide a copy of its complete NHI data to Ministry of Health and Welfare (MHW) to create a NHI research database in company with other databases held by MHW. While the NHI research data released by MHW for public access is without direct identifiers, data belonging to a specific individual within the NHI database is still linkable among different datasets and to other databases using a universally unique identifier, that is, the scrambled national identity number. Although users of the database are required to take away only the aggregate results of their analyses, the possibility of indirect identification is never completely ruled out. After five-year law suit, the Supreme Administrative Court ruled that individual plaintiffs do not have a right to request deletion since the collection is authorized by law rather than individual consents. A standalone opt-out right would not be granted as long as the data is further used for medical research purposes and is at least pseudonymized (no need to be entirely anonymized).[3] The individual preferences were painlessly outweighed by the ostensible public interest of medical research. The plaintiffs later brought the case for constitutional review on the basis, among other things, that depriving individual's right to request deletion would amount to forced participation in research and thus encroaching on individual's constitutional right to privacy. While the result of constitutional review is still pending thus far, the case poses an important question of whether there is some more critical values undergirding the recognition of the RTBF other than the respect for individual will or choice.

RTBF as the Right to De-indexing on the Web

If the RTBF refers more specifically to the de-indexing of personal data from the results of search engines on the web, PDPA's right to request deletion of personal data may provide only a tenuous ground because indexed information was collected, processed, and retained as information in the public domain where the right to erasure under PDPA is usually not applicable unless the truthfulness of the information is contested. Alternatively, causes of action based on the Civil Codes may provide more appropriate legal grounds against internet service providers (ISPs) when the disclosure or dissemination of the true information is claimed to infringe on the reputation or privacy of a data subject. RTBF, in this sense, is therefore linked to the personality right. For example, a plaintiff in a tort case requested the Taiwan Branch of Google International LLC to remove the search results containing a game-fixing scandal allegedly involving the plaintiff. The plaintiff, a professional baseball team CEO, was prosecuted for breach of trust because he was accused of being involved in a baseball game-fixing scandal. Although the plaintiff in the criminal case was eventually found

[2] National Health Insurance Act, Art. 79 & 80.
[3] Supreme Administrative Court 106 Pan Zi No. 54.

not guilty, news about his involvement in the scandal and other dishonest behaviors remains popular results in google search about the plaintiff. People unaware of the criminal judgement continue to make comments about the plaintiff based on those search results. The High Court in the tort case, without ruling directly on the substantive issue of the RTBF, found against the plaintiff because the court determined that Google Inc., which is the real search engine operator, is a different entity from Google International LLC and is without local presence in Taiwan.[4] Courts in other cases involving the erasure request directed at ISPs, however, were more willing to rely upon the balancing of interests between data subjects and the opposing party or even the general public. In a tort case in which Yahoo Taiwan was requested to remove an allegedly defamatory article posted on a social media forum run by Yahoo Taiwan, the High Court rejected the plaintiff's damage claim for fear that the freedom of speech may be overly suppressed if an ISP is to play the role of a police censoring speech on the internet.[5] Yet in another tort case involving a defendant convicted in a criminal slander case was asked by the plaintiff to be responsible for having Google removed the search results containing the defamatory information, a district court was content with the effort to remove all search results from the domains of google.tw without holding that the defendant be further responsible for removing the same search results processed by extraterritorial data processing servers or non-Taiwanese companies.[6]

In short, the right to request deletion of personal data under the PDPA is implemented but is limited to data collected on the basis of individual consents and is subject to the needs of relatively broad secondary uses. It may not be a proper basis for requesting removal of search results containing personal information from a search engine. Tort laws instead provide an alternative basis for requesting deletion of reputation infringing information on the internet. However, whether the information at issue infringes on reputation is a question that always needs to be settled by court before the removal request would be seriously taken. Also, the jurisdiction limitation to the place where the tortious acts occurred is another obstacle in the implementation of tort laws against extraterritorial reputation infringing acts.

RTBF as the Right of Oblivion

When the modern concept of RTBF was first introduced by Mayer-Schöenberger in 2009, it was closely linked to the right of oblivion. Such an origin sheds light on our understanding of the RTBF as a tool for social rehabilitation, which in turn is crucial for building a more tolerable society as a necessary condition for a democracy.

Because Article 6 of the PDPA treats criminal records as sensitive data, the collection, processing, or use of such information needs to be, among others, based on written consent of the data subject or on specific statutory authorization, or to be necessary for compliance with a legal obligation to which the private controller is subject or necessary for the performance of a task carried out in the exercise of official authority vested in the public controller. However, the erasure of past criminal data for the reason of social rehabilitation is nonetheless not specifically recognized as a legal right under the PDPA. The Juvenile Delinquency Act is the only law that explicitly requires removal of juvenile criminal records certain years after the

[4] Taiwan High Court 104 Shang Zi No. 389 (Civil Division).
[5] Taiwan High Court 102 Shang Zi No. 915 (Civil Division).
[6] Taoyuan District Court 104 Su Zi No. 985 (Civil Division).

execution of sentence or the completion of juvenile protective measures. While under the Juvenile Delinquency Act the legal obligation of removal is imposed solely on government agencies that retain those records, the Protection of Children and Youths Welfare and Rights Act (PCYWRA) provides additional protection for juvenile delinquent from media exposure. The PCYWRA prohibits the media to report personal identifiable information of the minor of a juvenile delinquency case and authorizes the competent authority to order the removal of contents containing such information. Such a provision is less about the right to be forgotten arising after a lapse of certain time than a right not to be socially labeled in the first place.

If the crux of the RTBF is to ensure a "clean slate" for individuals after a certain period of time thus allowing them to come back to a more solidary society, current statutory laws apparently provide insufficient grounds. More specific clean slate legislations are necessary to complement a general idea of RTBF.

RTBF as Independence from Power

As individual behaviors, preferences, physical conditions, and psychological states are all under the scrutiny and study of data technologies through profiling and machine learning, the threat to democracy is lurking behind subjecting one's independence to the algorithmic power. RTBF is in this light regarded by some as a personal resistance to the threat to personal independence in an era of big data and algorithms. Perhaps, only until RTBF is so understood would it be possible to properly strike a good balance between the right to know and the freedom of speech on the one hand, and the the right to control one's personal data.

邱文聰
（中央研究院副研究員）

中文摘要

源起於歐盟的遺忘權在外觀上與刪除權相似，因此常被認為僅是既有資訊權利的新包裝。遺忘權兼具自由權及請求權的特性，也被認為係派生自資訊隱私基本權核心之資訊自主控制。然而，遺忘權所具有的多面向特性，說明其可能具有多重的制度系譜與制度目的。本篇與談評論將指出，若將遺忘權視為僅在保護資訊當事人為其自身利益而展現的自由意志，將可能在「為了私利而改寫歷史」以及「保護言論自由及資訊取得權」二者的對比中，被輕易地妥協犧牲，反將稀釋了遺忘權本來所具有的制度功能。反之，遺忘權應該被理解為促進團結社會而協助特定個人進行社會復歸所需的制度工具，以及在當代資訊科技透過巨量資料與演算法，危及民主體制所賴以維繫之個人獨立性時，賦予個人的抵抗手段。唯有從遺忘權的此等民主維護功能加以理解，方能在其與其他利益相競爭時，獲得更好的權衡結果。