The Right to Be Forgotten

More Than a Pandora's Box?

by **Rolf H. Weber,***
Dr.; Chair Professor for International Business Law at the University of Zurich and Visiting Professor at the University of Hong Kong

Abstract: Recently, political voices have stressed the need to introduce a right to be forgotten as new human right. Individuals should have the right to make potentially damaging information disappear after a certain time has elapsed. Such new right, however, can come in conflict with the principle of free speech. Therefore, its scope needs to be evaluated in the light of appropriate data protection rules. Insofar, a more user-centered approach is to be realized. "Delete" can not be a value as such, but must be balanced within a new legal framework.

Keywords: Data protection; delete; free speech; privacy; privacy enhancing technologies; user-centered approach

Recommended citation: Rolf H. Weber, The Right to Be Forgotten: More Than a Pandora's Box?, 2 (2011) JIPITEC 120, para. 1.

A. Introduction

1 In 2010 a first legislative project was developed in France that envisaged the creation of a "right to be forgotten" online.[1] Subsequently, not much concrete information was made available about the proposed law, which was intended to force online and mobile firms to dispose of e-mails and text messages after an agreed-upon length of time or at the request of the individual concerned. In November 2010, the EU Commission took up the idea of introducing a right to be forgotten in the context of the ongoing revision of the Data Protection Directive 95/46;[2] the outcome of the vague proposal is still uncertain.

2 The right to be forgotten in the context of digital memory and/or data retention was only recently proposed as a fundamental right; however, its inherent background concept has been a discussion topic in Continental Europe and in the United States for many years. The main example in court practice and legal doctrine concerned persons who were convicted in court and who wanted to make this information disappear after a certain time period had elapsed.[3] In the United States, the lists of sexual offenders living in the neighborhood that are partly published on the Internet are topics of debate. A specific "case" is described in Mayer-Schönberger's book *Delete: The Virtue of Forgetting in the Digital Age*.[4] Stacy Snyder, a 25-year-old former education student at Millersville University School of Education in Pennsylvania, was confronted with a professor who became aware of a picture of her from a party posted on her MySpace web page, showing her drinking from a plastic cup and wearing a pirate's hat (captioned "drunken pirate"). The professor informed the school authorities dealing with Stacy's file, who thereupon refused to grant the young woman the diploma she had earned, stating that her conduct was "unprofessional" and that she had, albeit indirectly, encouraged young people to drink. Stacy's attempt to reverse the decision in court on the basis of her right of free speech failed.[5]

3 As mentioned, the term "right to be forgotten" has only recently been created. A decade ago, however, a similar term, namely the "right to forget," was already a topic of debate.[6] But viewed precisely, the active and the passive side of the "forget" medal are not identical, and the right *to be forgotten* should not be confused with the right *to forget* as happens frequently in blog discussions:[7] The "right to forget" refers to the already intensively reflected situation that a historical event should no longer be revital-

ized due to the length of time elapsed since its occurrence; the "right to be forgotten" reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them.[8] Therefore, the right to be forgotten is based on the autonomy of an individual becoming a rightholder in respect of personal information on a time scale; the longer the origin of the information goes back, the more likely personal interests prevail over public interests.

4 This contribution looks at the direct and indirect traces that lead from the general personality right to a specific right to be forgotten, it analyzes some key data protection concepts in light of the actual implementation of such a new and fundamental right, and finally it takes possible legal and technological limits of this proposed right into account.

B. Substance of the Right to Be Forgotten

I. Basis in the Right of the Personality

1. Continental Europe

5 In Continental Europe, the right to be forgotten can be considered as being contained in the right of the personality, encompassing several elements such as dignity, honor, and the right to private life. Manifold terminologies are used in the context of the right of personality – mainly the right for the (moral and legal) integrity of a person not to be infringed and for a sphere of privacy to be maintained and distinguished. The (privacy) right to indeed keep certain things secret has already been arguably extended to the right of Internet users not to make their activity trails available to third persons.[9] Essentially, rightholders are relying on their own autonomy to individually decide on the possible use of their own data.[10]

6 In most Continental European countries, there is wide court practice available delineating the extent to which (Internet) media have a right of their own to reveal information about a specific person, who in turn may claim the right to enjoy the protection of private life (privacy).[11]

7 Switzerland is a good example for the development of the right to be forgotten. After a first groundbreaking decision forbidding an artist to present a painting of the famous late Swiss painter Hodler in an art gallery,[12] courts have mainly dealt with situations in which a convicted person wanted to avoid information about earlier criminal records (of an official or unofficial nature) being drawn to public attention:[13] Since criminals do not remain of interest to the public indefinitely, the public should not have access to the respective records after a certain time period.[14] Insofar, court practice acknowledges an individual's right to be forgotten as a criminal.[15] For the courts, the discretion in interpreting the term "substantial amount of time" that has passed since the occurrence of criminal activity, therefore removing the interest of the public in being reminded of these events, is rather broad; obviously the evaluation depends upon the circumstances, such as which information is no longer of public interest and possibly counterproductive to the goal of rehabilitating the person in question.[16] Consequently, privacy concerns might preclude the media from revealing certain truths and previously publicized facts if the information is no longer newsworthy, but when the information about the past is still needed to protect the public in present times, a right to be forgotten cannot be invoked.[17]

8 Similar discussions are also being held in other Continental European countries. In Germany, for example, following the famous *Lebach* decision of the Constitutional Court,[18] several court proceedings have taken place in view of a possible interpretation of the right to be forgotten;[19] court practice has thereby applied a differentiated approach, evaluating the circumstances of the case (push or pull service, importance of criminal activity, etc.). Apart from the question how relevant criminal records should be after the expiration of a certain time period, aspects of involvement in political movements (for example, during World War II or as a member of the ruling party in the former German Democratic Republic) are also debated issues. Furthermore, the Spanish Data Protection Authority (EAPD) recently accused Google of invading the personal privacy of users, arguing that the company was in breach of the right to be forgotten as acknowledged in the laws of Spain.[20]

9 During the last decades, national court practice has been condensed and further developed in the judgments of the Human Rights Court in Strasbourg based on the European Convention on Human Rights (hereinafter ECHR).[21] The Human Rights Court in Strasbourg has rendered many decisions by applying a balance-of-interests test between the fundamental right to privacy (Art. 8 ECHR) and the freedom of speech (Art. 10 ECHR); however, the right to be forgotten has not yet been specifically addressed. In the case of Caroline von Hannover, who (unsuccessfully in Germany) initiated legal actions against photographers who took pictures from her daily life involving activities of a purely private nature, the Human Rights Court at least expressed the opinion in the field of traditional media that the information distribution should be limited by the interest of the concerned person not to make public very personal or even intimate information, and that the state

would be obliged to protect this interest.[22] Closer to the "forgetting" topic, the Human Rights Court recently clarified the relation of the freedom of media vis à vis the rights of privacy in a specific case (relating to Norway) in which a person with a criminal record invoked the presumption of innocence and the "right to be forgotten." The Court concluded that the publication had gravely damaged the person's reputation and honor and had been especially harmful to the person's moral and psychological integrity; the reasoning was based on privacy considerations in general, not on the right to be forgotten.[23]

2. United States

10 In Anglo-American court practice, particularly in the United States, the right of free speech according to the First Amendment has been applied in favor of the dissemination of truthful information relevant to the public interest about convicted persons.[24] Since the First Amendment to the US Constitution plays a particularly important role in court practice and seems to have reached a prevailing level as an entrenched right in comparison with other fundamental rights,[25] US courts rather tend to the statement that restrictions to the right of free speech would "invite timidity and self-censorship and very likely lead to the suppression of many items that would otherwise be published and that should be available to the public."[26] For decades, court practice defined the potential scope of a right to be forgotten in quite a narrow way since the justification for limiting the freedom of speech was tied to the constitutional scrutiny of "highest order" of public confidentiality interest, making it very difficult to satisfy this standard.[27]

11 Theoretically, disclosure could also constitute a tort according to the Second Restatement of Torts;[28] however, the Supreme Court did overturn a decision of a Florida court granting compensatory and punitive damages to a victim of disclosure.[29] Legal doctrine has shed light on the "public significance test" as developed by the Supreme Court and applied under the Restatement's public disclosure tort; however, the interests-balancing test between the right of a democratic society to be informed and the claim of an individual to have a right to be forgotten is usually interpreted in the favor of society and civic values.[30] The privacy right seems to prevail only if sensitive information is disclosed after interventions into the private sphere have been done in frivolous and socially irredeemable forays.[31]

12 This restrictive approach also seems to be the reason why the case of Andrew Feldmar, who had a criminal record because of violating anti-drug laws by taking LSD in his younger years, is discussed at length by Mayer-Schönberger from a US perspective under a data retention angle;[32] if this case had happened in Continental Europe, the appreciation would "naturally" have been done under the aspects of personality rights as described above (and would probably not have caused any specific problems related to the digital memory of the Internet).

II. Limits of the Right to Be Forgotten

13 The EU approach mentioned above (similarly to the earlier French approach) would introduce a right to be forgotten that would allow an individual to have his or her data deleted. However, the proposal so far does not clearly explain how this right could actually be enforced or how the deletion could be done in practice. Various problems in this context must be taken into account:

14 Privacy or a right to keep personal information confidential can be in conflict with other rights, such as free speech, and other privileges related to the free use of the web. Obviously, as already outlined, there is a court practice that balances the interests of privacy advocates against the freedom-of-speech defenders, and trade-offs are also needed in the real world.[33] Nevertheless, in the context of Internet communications, legal doctrine clearly refers to the fact that protection of the right to privacy is so difficult since it would mean "a right to have the government stop you from speaking about me."[34] Furthermore, this traditional concept is increasingly confronted with the fact that social networks such as Facebook are assuming an information-transporting function that might extend the implied consent of the person concerned (like Stacy Snyder) to upload a photo. In addition, the question remains whether the right to be forgotten is actually a "privacy" right since privacy concerns information that is not publicly known. In contrast, the right to be forgotten would turn public information into private information at a certain time by no longer allowing third persons to access such information.[35]

15 A further (practical) obstacle consists in the fact that Internet users consider censorship damaging and go to lengths to circumvent it. As recent experiences with the attempt of many governments to block access to the Internet have shown,[36] interested persons generally find a way to communicate electronically. With improved technology, it is becoming increasingly difficult for governments and private persons to contain certain information.

16 Finally, a cultural aspect must be taken into account: The question needs to be raised to what extent society has changed, as assumed for example by Mark Zuckerberg of Facebook.[37] Many people seem happy to make the trade-off in favor of sharing more about themselves in exchange for services and convenience (or they are at least not aware of the consequences of their behavior).[38] The enforcement problem is also confronted with the (legal) question whether the

government should "punish" those who use information that someone has voluntarily published on the Internet; legally, the time-oriented range of a given consent to publish is at stake.

17 Privacy protection must equally be reflected against the background of disclosure related to data that are, in fact, collected. This approach would require better monitoring by websites; when used correctly, these systems benignly aggregate information about behavior online. Indeed, first attempts have been undertaken to establish a search engine industry that would offer services to "bury" information which an Internet user may want to have forgotten so that it only turns up deep in any search results.[39] Insofar, sophisticated technology could play an important role in the information-gathering spectrum in the future.[40]

18 As shown, the environment for a new fundamental right to be forgotten is complex. Therefore, it is worth evaluating whether or to what extent general data protection principles can contribute to the concretization of such a new right.

C. Right to Be Forgotten as Data Protection Promoter?

I. Origins of Data Protection as Privacy Condensation

19 Some one hundred years ago, Supreme Court Justice Louis Brandeis stated the famous sentence:[41] "Publicity is justly commended as a remedy for social and industrial deceases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman." Some twenty years earlier, Brandeis, together with Samuel Warren, advocated for the right to privacy.[42] This concept, pioneered in 1890, was created to protect an individual's sphere of confidentiality;[43] in particular, the right to privacy was understood as the "right to be let alone."[44] This right focuses on commercial matters, business methods in general, and also on governmental actions.[45] Some years later, Brandeis referred in a dissenting opinion to "subtler and more far-reaching means of invading privacy [that] have become available."[46]

20 The general legal and even philosophical approach of Warren/Brandeis did not immediately lead to legislative actions and was mainly directed against data collections undertaken by governmental agencies and large corporations; the "right to be let alone" did not encompass the right to be forgotten. Moreover, only after World War II and the first economic recovery in Europe did national governments realize that data protection issues must be tackled. Historically, the movement is also linked to the development of the first big computer machines. Furthermore, an obvious tension exists between data protection and information access: The design of the scope of one's area of rights influences the other's area of rights, i.e., an extension of data protection diminishes information access rights and vice versa. The following overview of the release of data protection laws as well as information access laws (as the other side of the information flow coin) shows that this interrelation has often not been properly taken into account.[47]

Country	Data Protection Law	Information Access Law
Sweden	1973	1766
USA[48]	1974	1966
Germany (Brandenburg)	1977	1999
France	1978	1978
Norway	1978	1970
Denmark	1978	1985
Austria	1978	1987
Iceland	1981	1998
Australia (on national level)	1982	1982
Quebec (Canada on national level 1983) level)	1982	1983
United Kingdom	1984	2000
Finland	1987	1951
Netherlands	1988	1991
Ireland	1988	1997
Portugal	1991	1993
Hungary	1992	1992
Switzerland	1992	1993
Belgium	1992	1994
Spain	1992	1992
New Zealand	1993	1982
Italy	1996	1990
Greece	1997	1986

21 As shown, data protection laws have developed over the last 50 years, and the building of coherence with Internet access rights is remote; moreover, seen from a general angle, the release of data protection provisions has gone along with particular technological developments; insofar, four generations of norms can be distinguished:[49]

- *First-generation laws:* The legal provisions were a reaction to the attempt of governmental and private organizations to collect data in central databases, thereby realizing a "big technical risk."
- *Second-generation laws:* Over time, data collections moved from big machines to small, decentralized IT equipment in governments and businesses. This has changed the scope of the

risk potential and caused the legislator to include a broader number of entities in the regulatory framework.

- *Third-generation laws:* Due to increasing data collection activities, the need for the constitution of an individual right to self-determination and participative concepts became apparent.

- *Fourth-generation laws:* In view of the fact that self-determination rights have not worked out as envisaged in reality, the need for sectorial data protection provisions – and in particular of data security rules – gained importance.

22 As a lesson from the historical developments described above, the conclusion can be drawn that reliance on an individual (human) right has proven not to be satisfactory in all respects. In particular, the autonomy of the individual in respect of the use of his/her data cannot be considered as an uncontested principle. Consequently, this experience should be kept in mind with regard to the proposed implementation of a new "right to be forgotten."

II. Data Protection as a Cluster Concept

23 Already 40 years ago, Arthur R. Miller described the risk of an assault on privacy;[50] ten years ago, legal scholars invoked the notion of the "death of privacy."[51] Indeed, privacy is at risk; however, awareness has been rising over the last few years and legislative activities are taking manifold directives. Nevertheless, as Anne Cheung convincingly points out, the Internet "requires us to re-examine privacy as a concept."[52] In order to come to a stable framework for legal provisions and to identify the possible scope of a new fundamental "right to be forgotten," the sociological and philosophical basis of privacy must be evaluated in more detail.

1. Foundation of Privacy Elements

24 According to Lisa Austin, "technology creates privacy issues that appear to fall outside the bounds of our traditional analysis ... we need to sharpen and deepen our understanding of traditional concerns regarding privacy in order to respond to these new situations."[53] Consequently, a multi-dimensional approach is required, and privacy must encompass "the ability to control and limit physical, interactional, psychological and informational access to the self or one's group."[54] (i) The physical dimension refers to how physically accessible an individual is to others; (ii) the psychological dimension looks at an individual's right to decide with whom he or she shares personal information as well as the control of affective/cognitive inputs or outputs (e.g., non-verbal communication); (iii) the social dimension encompasses the ability to control social interactions; and (iv) the informational privacy dimension addresses an individual's right to reveal personal information to another.[55]

25 Recently, Hayden Ramsay identified five forms of privacy and analyzed them from a philosophical angle:[56] (i) The first privacy element refers to the control over the flow of information, in which freedom and individuality are not considered the only values of social life, but also truthfulness and practical wisdom; furthermore, privacy should not be limited to controlling information but extended to the risk of invasion of privacy. (ii) The second privacy element concerns the freedom from interference and observation; insofar, according to Ramsay, the threat of loss of autonomy does not adequately explain the meaning of violation and danger people experience with the most serious attacks on their privacy. (iii) The third privacy element looks at the maintenance of a sphere of inviolability around each person, which can be seen as a substantial moral good contrasting to the lack of respect for the value of persons. (iv) The fourth privacy element constitutes the need for solitude as already discussed by Warren/Brandeis. (v) The fifth privacy element can be identified in the term of "domesticity," asking for safety from observation and intrusion.

26 In light of the many privacy elements described above, data protection constitutes a "complex concept" requiring a consideration of these elements in view of their structural interrelations; consequently, the realization of a "cluster concept" seems to be unavoidable.[57] Such a "clustering" of data protection should concern a concept that ranges over information, access, and expressions. Thereby, autonomy must play an important role, also in view of the possibility to adequately react to new developments. The multi-dimensional nature of such an approach looks at informational privacy, accessibility privacy, and expressive privacy; these three aspects need to be combined and condensed to theories of privacy that include control over information, limited access, and personhood.[58] Informational privacy refers to control over information, accessibility privacy focuses on central observations of physical proximity, and expressive privacy protects a realm for expressing one's self-identity.[59] In view of a new "right to be forgotten," the relevant aspects of this cluster need to be identified, analyzed, and condensed into a rights structure.

2. Need for a More User-Centered Approach

27 The elements described above as a "cluster concept" must be realigned in view of the rights-oriented appreciation that data protection as a condensation of privacy is a "value" that needs to be understood as an aspect of autonomy of individuals containing both freedom from undue demands to conform and freedom to control one's own information.[60] Among the different constituents of privacy, autonomy is a key element.[61] This element advocates for a more user-centered approach encompassing a broad transparency range. When users are online, it must be clear what is happening, who/where personal information is sent to, who is collecting this personal information, as well as if and how such personal information is being transferred to third parties. In particular, users need to be provided with understandable and (in light of the good faith principle) acceptable terms of services, including options to influence the collection of personal information.

28 The more user-centric approach leads to theories looking at default licensing rules of personal information, thus ensuring that individuals retain their control (and power) over their information. This could preserve flexibility based on accepted mechanisms rather than relying on complex (and somewhat rigid) legal tools.[62] Another voice proposed focusing on the context in which information gathering and dissemination takes place; insofar, rights protecting individuals' information power could ensure that this context aspect remains connected to the personal data (a corollary to the purpose limitation principle).[63] Consequently, it is argued that the concept of property is sufficiently flexible and adjustable to work for information privacy.[64] Seen from this angle, privacy is understood as a bundle of interests related to information property that can be shaped through the legal system.[65]

29 Another approach applies a taxonomy based on the transactional scenarios and distinguishes between information collection (surveillance, interrogation), information processing (aggregation, identification, insecurity, secondary use, exclusion), information dissemination (breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion), and invasion (intrusion, decisional interference).[66] This concept begins with the data subject (the individual) from which various entities (other people, governments, businesses) collect information. The qualification of the processing of information depends on the harmfulness of the respective activities. The next step consists in the information dissemination, which brings the potential control of the information even further away from the concerned individual. Finally, privacy could be (illegally) invaded by third persons.[67]

30 More attention should also be paid to the perspective of understanding information privacy in a functional sense as a type of public value since it benefits and shapes society. From this vantage point, information privacy shows characteristics of a commons that requires some degree of social and legal control to construct and then maintain;[68] consequently, data protection approaches are becoming a part of social policy.[69] In this sense, the privacy commons is a multidimensional "territory" that should be ordered through legislation structuring anonymous and semi-anonymous information spaces; therefore, the propertization of personal information should be limited to the extent it undermines the privacy commons.[70]

31 In a nutshell, the different models described rely to a great extent on individual autonomy. Autonomy as such could mean that the individual is entitled to control the information. However, such an approach does not take into account the public interests (such as ordre public, security interests, etc.). Therefore, the application of a balancing test seems to be unavoidable. Before going into the respective details, the theoretical approaches already discussed in this field will be evaluated.

III. Privacy Risks' Mitigation by Data Protection Rules

1. Potential Legal Responses

a. Overview

32 The most extensive attempt to apply data protection principles in the context of the right to be forgotten has been undertaken by Mayer-Schönberger. In his seminal book *Delete*, which is inspiring intensive debate in the United States but is not yet fully appreciated in Europe, Mayer-Schönberger discusses in depth seven potential (legal) responses that could mitigate the ills of digital memory.[71] Six of these responses are described in relatively short comments, while the seventh is explained in far-reaching detail:

- *Digital abstinence:*[72] At first sight, the solution of digital abstinence seems to be simple and straightforward since it is based on choice and autonomy (at least in transparent circumstances): If persons are staying away as much as possible from interactions that require revealing information to others, less "critical" information will be available. However, several problems cannot be overlooked: Digital abstinence is definitely based on individuals' knowledge and preferences not being identical throughout the whole civil society. Consequently, people's be-

havior would have to be influenced. Furthermore, the sharing of personal information offers users values that contradict the limitation of digital memory; indeed, the participation of millions of Internet users around the world in creating content has unleashed innovative and beneficial forms of information production that would not have been possible in a world of digital abstinence.[73] Businesses as well would have to adapt their practices and accept substantial limitations to digital remembering.

- *Information privacy rights:*[74] This approach is based on the notion and concept of informational self-determination: Individuals should have control over every phase and stage of the use of their personal information. As experience has shown in practice, however, the principle of consent to data collection as an expression of self-determination is very difficult to enact; furthermore, a look at court practice also demonstrates that liability claims against data collectors not complying with data protection laws are very rare. Certain procedural measures could obviously be introduced, such as shifting the burden of proof to the data collector that the individual concerned has agreed to the digital remembering. Another approach tries to underlay the right to self-determination with a property rights concept; the elements of this concept have already been outlined.[75]

- *Digital privacy rights infrastructure:*[76] More than 10 years ago, Lawrence Lessig suggested using Digital Rights Management (DRM) infrastructure as a means to protect technical code.[77] DRM was developed for intellectual property rights, mainly by the (Hollywood) entertainment industry in its attempt to prevent the copying of protected works. In the meantime, even DRM's promoters are no longer so convinced that this infrastructure provides an adequate protection measure. Even more questions are justified if DRM is to control personal information. Any system capable of making judgments would have to watch how users handle protected information.[78] Therefore, the risk exists that a technical infrastructure of pervasive surveillance would be created (a panopticon to protect from the Internet society). Further problems concern the related costs and practicability of a new technological infrastructure.[79]

- *Cognitive adjustment:*[80] This approach would not require changing society through the adoption of law or the development and implementation of a novel technical infrastructure, but the necessary changes would take place in the minds of civil society. Whether such a change could be realized is another question; acknowledging cognitive adaptation related to a comprehensive digital memory might be an expectation that is too ambitious.

- *Information ecology:*[81] Advocates for a more stringent and comprehensive information ecology have been raising their voice for many years and asking information processors to slow down the speed of information collection and storage.[82] However, several conceptual weaknesses cannot be overlooked – for example, the problem that mandated information ecology might be a binary tool and that practical experience with norms trying to realize information ecology shows the difficulty of getting them politically enacted. Finally, such norms are confronted with a certain lack of built-in flexibility.

- *Perfect contextualization:*[83] This approach tries to apply the "knowledge" of technical systems in remembering information and in limiting data collection of information not related to the given context. Obviously, a technically perfect contextualization will never be possible. In addition, such systems need sustained attention, which is not always available.

33 Mayer-Schönberger summarizes the above six responses to the demise of forgetting under the headings of "Information Power" and "Cognition" as follows.[84]

	Information Power (incl. information privacy)	**Cognition, Decision-Making and Time**
Individuals	Digital abstinence	Cognitive adjustment
Laws	Privacy rights	Information ecology
Technology	Privacy DRM	Full contextualization

b. Expiration Dates on Digital Data in Particular

34 The seventh response to the demise of forgetting is the already briefly mentioned introduction of expiration dates on digital information:[85] Mayer-Schönberger argues that, technically (design challenges for the most appropriate user interface aside), expiration dates would be relatively easy to implement (just as another type of meta-information associated with a piece of information). Thereby, the role of information processors would become more important, and the development of algorithms that would better approximate what kind of information should still be available for use would become crucial. If expiration dates on information files are not sufficient,

a more fine-grained approach is necessary, described by Mayer-Schönberger as the expiration of information bits.[86] Technologically, this concept looks at cookies as well as the expiration date for web page links and web search queries. The advantages of such measures are that individual users would not be required to become familiar with complex new technologies; they would only need to be aware of how to set expiration dates at any given moment.

35 Furthermore, Mayer-Schönberger also discusses the possibility of negotiating expiration dates.[87] Indeed, particularly in contractual transactions, two parties often have different opinions about the expiration date. In such a case, each individual should independently determine the duration of the digital memory; if the dates do not correspond, a joint understanding must be negotiated just like other contractual issues.

36 The new concept of introducing expiration dates for digital information is a challenging approach. Nevertheless, certain weaknesses cannot be overlooked: The ubiquity of social networking nowadays is so extensive that the introduction of "expiration dates"[88] requiring somebody (who?) to delete the information is difficult to apply in practice. Furthermore, the proposal of "expiration dates" also seems to be inadequate and deficient in and of itself since the approach focuses on self-censorship or a lack thereof, contradicting the human desire to chronicle life (to the smallest and most trivial detail) and to immortalize previously fleeting memories.[89]

2. Potential Technological Responses

37 As already mentioned, technology also plays a role in the triangle between identity, memory, and privacy; as of now, governments and civil societies are still struggling with new technological realities. Indeed, technology can provide solutions which - if embedded adequately - can contribute to overcoming data protection concerns.[90] In practical life, various factors are responsible for the prevailing public uncertainty with technology: Apart from a general reluctance to learn new techniques, the technology is often highly complex, making it difficult or at least cumbersome and time-consuming to apply (for example, in the context of electronic signatures). In addition, the positive aspects of technology can easily morph into negative results (from self-control to being controlled by others).

38 The development and proliferation of devices that provide "Continuous Archival and Retrieval of Personal Experiences" (CARPE) is a good example: In realizing the concept of autonomy, such technologies could improve the control over, the access to, and the record of collective knowledge, but they can also be used by third persons to exert control in their own interest.[91] Such technologies are based on the desire for individual control over the devices, and such individual control might prove determinative in the quest for individual and collective empowerment through these technologies; however, social forces undermine the ability of all netizens to enjoy control equally.[92] In other words, technological parameters that rest on an atomistic concept of relatively autonomous individuals do not reflect the practical reality.[93] Therefore, CARPE devices often do not live up to their perceived potential because they do not operate in a social vacuum.[94] In the end, this question arises: How much privacy are individuals prepared to surrender in order to achieve other purposes (such as social recognition or an increase in security)?[95]

39 The aforementioned evaluation demonstrating some reluctance as far as technologies are concerned does not mean that any single approach should not be implemented. To the contrary, a number of technologies are available to achieve information privacy goals. In particular, Privacy Enhancing Technologies (PETs) can be oriented on the subject, the object, the transaction, or the system. Subject-oriented PETs aim at limiting the ability of other users to discern the identity of a particular organizational entity; object-oriented PETs endeavor to protect identities through the use of a particular technology; transaction-oriented PETs have the goal of protecting transactional data, e.g., through automated systems for destroying such data; and system-oriented PETs are designed to create zones of interaction where users are hidden and objects bear no traces of data streams handling them nor records of interactions.[96] Furthermore, technical developments require assessment capacity and capability, which need to be pooled on a global level; some institutionalized format for pooling available resources of data protection agencies on an international level will have to be found, thus dipping into the resources of technology assessment institutions worldwide.[97]

40 Notwithstanding the fact that technology is able to substantially back up the idea of giving each individual the possibility to autonomously control the life of his/her data, it cannot be overlooked that, in principle, technology should have a serving function; it cannot replace the legislator in designing the scope and limits of a new fundamental "right to be forgotten."

D. Outlook

41 With the increased tendency to make information of all kinds public, privacy is at risk. Notwithstanding existing and planned data protection laws, new fundamental right concepts are being developed as a consequence. Some two years ago, the German

Constitutional Court "invented" a so-called "computer confidentiality and integrity right" designed to avoid third-party interference with the personal electronic communication network.[98] About a year ago, as mentioned, a right to be forgotten was proposed by France and then by the European Union in the context of the revision of the Data Protection Directive 95/46.[99] Nevertheless, as of now there is still no concrete description of the right's scope and contents.

42 In the form proposed by the European Union, the right to be forgotten cannot easily render a substantial contribution to an improvement of data protection. The concept is probably too vague to be successful. History has shown that human rights need to be embedded in strategies, and such strategies have to be actually used.[100] Consequently, a clearer picture of the actual objective of a new fundamental right is necessary. The proclamation of a right to be forgotten as such does not suffice. It recalls the myth of Pandora's box: Impelled by her natural curiosity, Pandora opened the box and all the evils contained in it escaped. Moreover, a concretization of the right to be forgotten might be achieved by more specific codes of conduct, such as the French "Code of Good Practice on the Right to Be Forgotten on Social Networks and Search Engines," encompassing practical commitments that could become the starting point for a future international memorandum or agreement.[101]

43 The right to be forgotten must be complemented with legal instruments to guide individuals and entities on how to apply data protection principles on the basis of the acknowledgement of rightholders' autonomy. Together with such guidelines, accountability mechanisms need to be introduced and audit procedures should be established.[102] Possible means could be privacy marks or seals from a self-regulatory regime, which would then be monitored by established data controllers according to accountability procedures applied by the program or scheme organization. Such an "evaluation" also corresponds to the democratic theory that holds governing bodies accountable in responding to the public's interest.[103] This would enable technical measures to be introduced much faster than legal instruments, and the technical measures would have a global scope of application that is not limited by geography.[104] Returning to Pandora's situation: By the time she managed to close the lid, nearly the entire contents had escaped. Only one last thing lay at the bottom, and that was hope.

■

* The author, who would like to thank Prof. Christine Kaufmann (Zurich) and Prof. Anne Cheung (Hong Kong) for their valuable comments, is engaged as co-investigator in the research project "In Search of a Techno-legal Framework for the Protection of Personal Data," supported by the General Research Fund of the University of Hong Kong.

1 Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche, October 13, 2010, http://www.aidh.org/Actualite/Act_2010/Images/Charte_oubli_La_Charte.pdf.

2 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final of November 4, 2010. This approach has been repeatedly reiterated by members of the European Commission, for example by EU justice commissioner Viviane Reding in a speech to the European parliament on March 16, 2011.

3 For further details, see infra B. I. 1.

4 Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, Princeton and Oxford 2009, pp. 1-3.

5 See http://voices.washingtonpost.com/securityfix/Decision%202008.12.03.pdf.

6 Gregory W. Streich, Is There a Right to Forget? Historical Injustices, Race, Memory, and Identity, New Political Science, Vol. 24/4, 2002, pp. 525-542.

7 Blog discussions about the French and EU approach for introducing a new human right seem to use the two terms synonymously.

8 Substantively, this right concerns data retention and the aspect of the expiration of the data life (see infra C. III. 1).

9 See Franz Werro, The Right to Inform v. the Right to be Forgotten: A Transatlantic Crash, in: Liability in the Third Millennium, Liber Amicorum Gert Brüggemeier, Baden-Baden 2009, pp. 285 et seq.

10 See infra C. II. 2.

11 See Werro, supra note 9, pp. 285-289.

12 Swiss Federal Court, July 20, 1944, BGE 70 II 127; to the right of surviving relatives being entitled to make a claim on behalf of the deceased person, see Swiss Federal Court, December 14, 1978, BGE 104 II 225, C. 5b.

13 The following court decisions correspond to the example of Andrew Feldmar (who had a criminal record due to a violation of anti-drug laws from taking LSD in his younger years), given by Mayer-Schönberger, supra note 4, pp. 3-5.

14 Swiss Federal Court, July 29, 1996, BGE 122 III 449.

15 Swiss Federal Court, October 23, 2003, 5C.156/2003.

16 See also Werro, supra note 9, p. 290.

17 See also Franz Werro/Eva Maria Belser, Le droit à l'oubli et ses limites, medialex 1997, pp. 99 et seq.; for a detailed discussion see Mirjam Teitler, Der rechtskräftig verurteilte Straftäter und seine Persönlichkeitsrechte im Spannungsfeld zwischen öffentlichem Informationsinteresse, Persönlichkeitsschutz und Kommerz, Zurich 2008, pp. 29-98.

18 BVerfGE 35, p. 202.

19 BGH, ZUM 2008, p. 957 (Zerknitterte Zigarettenschachtel); BGH, ZUM-RD 2009, p. 429 (Kannibale von Rotenburg); BGHZ 183, p. 353 (Online-Archive); for further details, see Christoph Alexander, Urheber- und persönlichkeitsrechtliche Fragen eines Rechts auf Rückzug aus der Öffentlichkeit, ZUM 2011, pp. 382-389.

20 Google fights the Spanish privacy order in court: see http://www.bbc.co.uk/news/technology-12239674.

21 See Samantha Besson, Comment humaniser le droit privé sans commodifier les droits de l'homme, in: Franz Werro (ed.), La Convention européenne des droits de l'homme et le droit privé, Bern 2006, pp. 1 et seq.

22 Caroline von Hannover v. Germany, June 24, 2004, No. 59320/00, Sect. 3, ECHR 2004-VI, 40 EHRR 1.

23 A. v. Norway, April 9, 2009, No. 28070/06, Sect. 1.

24 Cox Broadcasting v. Cohn, 420 U.S. 469, 493-496 (1975); Griswold v. Connecticut, 381 U.S. 479, 482-486 (1965).

25 The privacy right under the Fourth Amendment is seen as a right against arbitrary use of data by governments.

26 Cox Broadcasting, supra note 24, p. 496.

27 Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).

28 See 1057 Restatement (Second) of Torts, § 652A-652I (1977).

29 The Florida Star v. B.J.F., 491 U.S. 524 (1989).

30 Jacqueline R. Rolfs, The Florida Star v. B.J.F.: The Beginning of the End for the Tort of Public Disclosure, Wisconsin Law Review 1990, pp. 1107, 1120-1122.

31 Rolfs, supra note 30, p. 1121; Werro, supra note 9, p. 296.

32 See Mayer-Schönberger, supra note 4, pp. 3-5.

33 See above B. II.

34 Eugene Volokh, Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People From Speaking About You, Stanford Law Review, Vol. 52, 2000, pp. 1049-1124, at p. 1051.

35 See L. Gordon Grovitz, Forget Any "Right to Be Forgotten," The Wall Street Journal, November 15, 2010, http://online.wsj.com/article/SB10001424052748704658204575610771677242174.html.

36 Most prominently, this attempt was undertaken in Egypt; however, other countries as well have only been partly successful in avoiding electronic communications among members of civil society by means of social networks (Iran, China, etc.).

37 Tim Cole, A Right to Forget?, http.//blogs.kuppingercole.com/cole/2010/08/07/a-right-to-forget.

38 See John Palfrey/Urs Gasser, Born Digital: Understanding the First Generation of Digital Natives, New York 2008. To the specific data protection problems related to social networks, see Daniel B. Garrie/The Honourable Maureen Duffy-Lewis/Rebecca Wong/Mari Joller/Richard L. Gillespie, Impersonation of Life: The Perils of Social Networking, Convergence, Vol. 5/2, 2009, pp. 236-249.

39 Peter Waldkirch, France and the Right to Forget, http://www.iposgoode.ca/2010/01/france-and-the-right-to-forget.

40 See below C. III. 2.

41 Louis D. Brandeis, What Publicity Can Do, in: Other People's Money: And How the Bankers Use It, New York 1914, p. 92.

42 Samuel D. Warren/Louis D. Brandeis, The Right to Privacy, Harvard Law Review 4, 1890, pp. 193-220.

43 Historically evaluated, one reason for this approach may have been the fact that unkindly reports appeared in the local press about Warren's dinner parties: see Daniel J. Solove/Marc Rotenberg/Paul M. Schwartz, Privacy, Information, and Technology, New York 2006, p. 11.

44 Warren/Brandeis, supra note 42, p. 205; see also Dissenting Opinion of Brandeis, in: Olmstead v. United States, 277 US 438, 478 (1928).

45 See also Christine Kaufmann/Rolf H. Weber, The Role of Transparency in Financial Regulation, Journal of International Economic Law, Vol. 13/3, 2010, pp. 779-780; Neil M. Richards, The Puzzle of Brandeis, Privacy and Speech, Vanderbilt Law Review, Vol. 63, 2010, pp. 1295-1296.

46 Olmstead v. United States, 277 US 433, 471 (1929); see also Susan E. Gindin, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, San Diego Law Review, Vol. 34, 1997, pp. 1153-1154.

47 See Rolf H. Weber, Datenschutz v. Öffentlichkeitsprinzip, Zürich 2010, pp. 16-17.

48 The Federal Privacy Act 1974 only covers the processing of personal information by Federal Agencies; the scope is insofar quite limited as data processing by private actors is not restricted by a nationwide law in the United States.

49 See Weber, supra note 47, pp. 8-9; Viktor Mayer-Schönberger/Ernst O. Brandl, Datenschutzgesetz, 2nd ed. Vienna 2006, pp. 12-13.

50 Arthur R. Miller, The Assault on Privacy: Computers, Data Banks and Dossiers, Ann Arbor 1971.

51 See Simon Garfinkel, Database Nation: The Death of Privacy in the 21st Century, Beijing et al. 2000; A. Michael Froomkin, The Death of Privacy?, Stanford Law Review, Vol. 52, 2000, pp. 1461-1543.

52 Anne S. Y. Cheung, Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd, Journal of Media Law, Vol. 2, 2009, p. 192.

53 Lisa Austin, Privacy and the Questions of Technology, in: Law and Philosophy, Vol. 22/2, 2003, pp. 119-166, at p. 164.

54 Judee K. Burgoon/Roxanne Parrot/Beth A. Le Poire/Douglas L. Kelley/Joseph B. Walther/Denise Perry, Maintaining and restoring privacy through communication in different types of relationship, Journal of Social and Personal Relationships, Vol. 6, 1989, pp. 131-158, at p. 132.

55 Ulrike Hugl, Approaching the Value of Privacy: Review of theoretical privacy concepts and aspects of privacy management, AMCIS 2010 Proceedings, Paper 248, p. 4.

56 Hayden Ramsay, Privacy, Privacies and Basic Needs, The Haythrop Journal, Vol. 51, 2010, pp. 288-297.

57 Hugl, supra note 55, p. 4.

58 Judith Wagner DeCew, In Pursuit of Privacy: Law, Ethics and the Rise of Technology, Ithaca/London 1997.

59 Hugl, supra note 55, pp. 4-5.

60 Cheung, supra note 52, p. 209.

61 A part of this sub-chapter is a short version of longer comments, published as Rolf H. Weber, How Does Privacy Change in the Age of Internet, in: Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval (eds.), Internet and Surveillance: The Challenges of Web 2.0 and Social Media, Oxford 2011, forthcoming.

62 Mayer-Schönberger, supra note 4, p. 142.

63 Helen Nissenbaum, Privacy as Contextual Integrity, Washington Law Review, Vol. 79, 2004, pp.119 et seq.

64 Paul M. Schwartz, Property, Privacy, and Personal Data, Harvard Law Review, Vol. 117, 2004, pp. 2055 et seq.

65 Mayer-Schönberger, supra note 4, p. 143.

66 Daniel J. Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, 2006, pp. 477 et seq.

67 Solove, supra note 66, pp. 488-491.

68 Schwartz, supra note 64, p. 2088; Daniel J. Solove/Paul M. Schwartz, Information Privacy Law, 3rd ed., New York 2009, p. 61.

69 See also Colin J. Bennett/Charles D. Raab, The Governance of Privacy. Policy Instruments in Global Perspective, Cambridge Mass./London 2006, pp. 29 et seq.

70 Schwartz, supra note 64, p. 2088.

71 Mayer-Schönberger, supra note 4, pp. 128 et seq.; other authors have looked at the Delete problem as well, but none of the contributions is as groundbreaking as Mayer-Schönberger's book.

72 Mayer-Schönberger, supra note 4, pp. 128 et seq.

73 Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedoms, New Haven 2006, pp. 59-90.

74 Mayer-Schönberger, supra note 4, pp. 134 et seq.

75 See supra C. II. 2.

76 Mayer-Schönberger, supra note 4, pp. 144 et seq.

77 Lawrence Lessig, Code and Other Laws of Cyberspace, New York 1999.

78 Mayer-Schönberger, supra note 4, p. 148.

79 Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, Wisconsin Law Review 2000, pp. 743 et seq.

80 Mayer-Schönberger, supra note 4, pp. 154 et seq.

81 Mayer-Schönberger, supra note 4, pp. 157 et seq.

82 Jack M. Balkin, The Constitution in the National Surveillance State, Minnesota Law Review, Vol. 93, 2008, pp. 1-25, at pp. 1 et seq; David Lazer/Viktor Mayer-Schönberger, Statutory Frameworks for Regulating Information Flows: Drawing Lessons for the DNA Databanks from Other Government Data Systems, Journal of Law, Medicine & Ethics, Vol. 34, 2006, pp. 366 et seq; Rolf H. Weber, Kassandra oder Wissensbroker – Dilemma im "Global Village," in: Jürgen Becker/Reto M. Hilty/Jean-Fritz Stöckli/Thomas Würtenberger (eds.), Festschrift für Manfred Rehbinder, Munich, 2002, pp. 405-421.

83 Mayer-Schönberger, supra note 4, pp. 163 et seq.

84 Mayer-Schönberger, supra note 4, p. 168.

85 Mayer-Schönberger, supra note 4, pp. 169 et seq.

86 Mayer-Schönberger, supra note 4, pp. 178 et seq.

87 Mayer-Schönberger, supra note 4, pp. 185 et seq.

88 As proposed by Mayer-Schönberger, supra note 4, pp. 171 et seq.

89 See Sabrina Gilani, Book Review, Human Rights Law Review, Vol. 10, 2010, pp. 785, 787.

90 Herbert Burkert, Globalization – Strategies for Data Protection, Weblaw Jusletter, October 3, 2005, No. 60, http://www.weblaw.ch/jusletter/Artikel.asp?ArtikelNr=4321.

91 See Jane Bailey/Ian Kerr, Seizing Control? The Experience Capture Experiments of Ringley & Mann, Ethics and Information Technology, 9/2007, pp. 129-139.

92 Bailey/Kerr, supra note 91, p. 133.

93 See also Bennett/Raab, supra note 69, p. 14.

94 Bailey/Kerr, supra note 91, p. 134.

95 Pieter Kleve/Richard D. Mulder, Privacy protection and the right to information: In search of a new symbiosis in the information age, in: S. Kierkegaard (ed.), Cyberlaw & Security Privacy, Beijing 2007, pp. 331, 342 and 346.

96 Pamela Samuelson, Privacy as Intellectual Property?, Stanford Law Review, Vol. 52, 2000, pp. 1124, 1668.

97 Burkert, supra note 90, Nos. 63/64.

98 Decision of the German Constitutional Court of February 27, 2008, 1 BvR 370/07; 1 BvR 595/07; for an evaluation of this decision, see Rolf H. Weber, Grundrecht auf Vertraulichkeit und Integrität, digma 2008, pp. 94-97.

99 See infra A.

100 Burkert, supra note 90, No. 4.

101 See "Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche," October 13, 2010, http://www.huntonprivacyblog.com/2010/10/articles/european-union-1/french-government-secures-right-to-be-forgotten-on-the-internet/.

102 Bennett/Raab, supra note 69, pp. 215/16.

103 Bennett/Raab, supra note 69, pp. 237/38.

104 See already Rolf H. Weber, Datenschutzrecht vor neuen Herausforderungen, Zürich 2000, p. 75.