# Timing the Right to Be Forgotten

## A study into "time" as a factor in deciding about retention or erasure of data

Paulan Korenhof, Jef Ausloos, Ivan Szekely, Meg Ambrose, Giovanni Sartor, Ronald Leenes

[P.E.I.Korenhof, R.E.Leenes]@tilburguniversity.edu,
Jef.Ausloos@law.kuleuven.be, Szekelyi@ceu.hu, megLeta@gmail.com
sartor@cirfid.unibo.it

**Abstract.** The so-called "Right to Be Forgotten or Erasure" (RTBF), article 17 of the proposed General Data Protection Regulation, provides individuals with a means to oppose the often persistent digital memory of the Web. Because digital information technologies affect the accessibility of information over time *and* time plays a fundamental role in biological forgetting, 'time' is a factor that *should* play a pivotal role in the RTBF. This chapter explores the roles that 'time' plays and could play in decisions regarding the retention or erasure of data. Two roles are identified: (1) 'time' as the marker of a discrete moment where the grounds for retention no longer hold and 'forgetting' of the data should follow and (2) 'time' as a factor in the balance of interests, as adding or removing weight to the request to 'forget' personal information or its opposing interest. The chapter elaborates on these two roles from different perspectives and highlights the importance and underdeveloped understanding of the second role.

**Keywords.** The Right to Be Forgotten, Data Protection, Privacy, Internet, Time.

## 1 Introduction

Tremendous advancements in information technologies have made it possible to capture, store and process vast amounts of data at marginal costs and in ways previously unimaginable.[1] Much of these data relates to specific individuals and may result in severe consequences. Moreover, the pervasiveness of modern networked communication technologies has given a global scope to these potential effects. Space and time are two key factors in the realm of increased accessibility and use of data, with significant, but different roles in the new digital world versus the old analogue world. Space and time are related; data accessible from anywhere but for no amount of time would reach no audience. The same goes for data that are accessible forever, but from

[1] Cf. generally Mayer-Schönberger 2009.

nowhere. The "digital turn" implies an increased reach of information in both space and time, while information generally has a different value depending on the time and place.[2] This 'disconnect' increasingly causes issues. In this article we explore the extended reach of information in one of these two dimensions: time.[3] Time as a relevant factor in extending the reach of information was expressed by Rosen et al. in their article with the telling title "The Web Means the End Of Forgetting"[4] and Mayer-Schönberger in his "Delete: the virtue of forgetting in the digital age"[5]. At the core of concerns in this domain is the potentially growing need of individuals to have certain information taken down or otherwise obscured. Or to use the controversial term that has taken central stage in the debate, to be "forgotten" – a term often used to express individuals' desires to be free of information that already exists in the public domain, but that "with the passing of time becomes decontextualized, distorted, outdated, no longer truthful (but not necessarily false)".[6]

The European Union is engaged in addressing concerns by developing regulation that enables individuals to oppose the persistent digital memory and giving them a right to be forgotten (RTBF). Most notably this right – currently still under construction – is enshrined in the so-called "Right to Be Forgotten or Erasure", article 17 in the General Data Protection Regulation (GDPR) proposal.[7]

The introduction of the RTBF has been the topic of much – heated – debate. Rosen already dubbed the right "the biggest threat to free speech on the Internet in the coming decade".[8] However, next to numerous opponents, there are also many that underline the social necessity of a RTBF to limit access to persistent, personal, networked data.[9] The debate seems deadlocked with the adversaries taking almost absolute positions on the spectrum of forgetting versus remembering. Taking 'time' into consideration may allow for a more nuanced assessment. For instance, is it in the interest of freedom of expression and the marketplace of ideas to keep the opinion of a 14-year old recalcitrant adolescent in a school paper publicly accessible online for 10-years? What about 40-years? We can think of circumstances where we would answer such questions with 'yes', but equally important, we can think of circumstances where we would answer such questions with 'no'. Additionally, the answer that we as a society give to such questions may in return affect the interests at stake; if we decide that no utterance can ever be 'forgotten', debates may be stifled or curbed for fear of future consequences later on in life. Such considerations show that a pivotal role may be

---

2 Cf. Ambrose 2012.

3 As mentioned, time and space are related, but we will primarily focus on time.

4 Rosen 2010.

5 Mayer-Schönberger 2009.

6 De Andrade 2012, p. 127.

7 The provision was introduced in the European Commission's *"Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data"*, COM(2012)11 final of 25 January 2012.

8 Rosen 2012.

9 Cf. De Andrade 2012, Mayer-Schonberger 2009.

given to "time" in the balance of interests in cases where individuals aim to legally challenge persistent online memory. The main question of this chapter is thus:

**What role can "time" play in the decisions and the balancing of different interests with regard to the retaining or removal of online available information?**

This question was the focus of the "Timing the Right to Be Forgotten" panel at the 2014 Computers, Privacy and Data Protection conference in Brussels. The participants of this panel have collaborated to explore an answer to this question, which resulted in this chapter. It provides an analysis from the perspectives of the different panelists. After a brief introduction to the way we use digital information sources from an applied socio-philosophical perspective, we explore 'time' in law, followed by an analysis of discrete decision points in data processing and the data life cycle. Next we discuss how different interests can be balanced over time. The chapter concludes with a reflection on the insights obtained from the different angles. As the chapter discusses different perspectives provided by scholars from different disciplines, the style of the chapter is hybrid, which provides unique insight and broad treatment. All argue, in one way or another, that 'time' is an essential element to understand and manage information persistence in the digital world.

## 2 The external transactive memory and forgetting[10]

Before we explore time as a factor in the balancing of interests regarding data processing, we first need a model of (digital) memory and what 'forgetting' means in this context.

### 2.1 Memory, external memory and transactive memory

Information is key to our functioning in the world – in relation to others and our environment. The ability to remember is a very important asset in this respect and the complex concept of 'memory' has been topic of research and debate in various academic fields.[11] The overarching similarity in these diverse fields lies in three process elements:

"Any memory system – whether physical, electronic, or human – requires three things, the capacity to encode, or enter information into the system, the capacity to store it, and – subsequently – the capacity to retrieve it."[12]

These three elements are intertwined: the way in which information is encoded determines what and how information is stored and this will in return determine what can be retrieved.[13]

---

[10] The line of thought described in this section has been explored previously in Korenhof 2014.
[11] Sutton 2012.
[12] Anderson et al. 2009, p. 5.
[13] Anderson et al. 2009, p. 5.

Because the biological brain is perceptive to failures in its memory capabilities and has limited storage capacity, people make use of external tools to enhance their cognitive abilities and minimize their weaknesses.[14] Such tools can be used to alter, combine, transform and store information in ways that would be too time-consuming or complex to perform with the "naked" brain.[15] An all-familiar example external memory enhancement is an agenda, which complements the brain's limited memory capacity by diminishing the amount of information that it needs to process and store. Instead of remembering all our appointments, we only need to remember where our agenda is.

The praxis of external memory stores is heavily shaped by technology. The technology adopted determines what (written words, drawn pictures, photo's, voice samples) we can store, how much we can store (amount of books you can store in a house versus digital files on a personal computer) and how easily we can find it (searching manually versus search with a computer program in files). The "digital turn" has dramatically affected the praxis. Practical limits of external memory stores have changed: we store increasing amounts of data,[16] can transport the information more easily[17] and are able to copy and distribute it flawlessly.[18] When publicly available on the Web, information is generally easily accessible to anyone with access to the right device and infrastructure, both of which are increasingly common. Search engines, apps and widgets effectively facilitate the retrieval of online information if its location is not already known.[19] With the "digital turn," our abilities to encode, store and retrieve information have thus expanded.

Treated as external memory, the Internet has an important characteristic not shared with other (private) external memories: because everyone can potentially add and retrieve information to and from the Internet, (particularly the Web) can function as a shared and socially interactive memory, a "transactive memory system".[20] Transactive memory concerns the structuring and processing of information within a group.[21] It is "a set of individual memory systems in combination with the communication that takes place among individuals".[22] In the transactive memory, the memory process elements of encoding, storage and retrieval are recognized to have "both internal and external manifestations".[23] The encoding of information within a transactive memory is done by individual agents or their external memory stores thus contributing to the shared memory. Individuals can retrieve information by consulting all available sources in the transactive memory, their own and other individuals' internal and ex-

[14] Clark 2003, p. 74-75.
[15] Clark 2003, p. 78.
[16] Mayer-Schönberger 2009, p. 67.
[17] Van den Berg and Leenes 2010, p. 1112.
[18] Vafopoulos 2012, p. 411.
[19] Sparrow et al. 2011, p. 776.
[20] Sparrow et al. 2011.
[21] Wegner 1986, p. 185.
[22] Wegner 1986, p. 186.
[23] Wegner 1986, p. 188.

ternal memory sources.[24] Using a transactive memory allows individuals to significantly enhance their (external) memory without the need for encoding and storing all information themselves.[25] A transactive memory shapes what a group of people remembers and influences what they individually take to be true.[26] The Internet is regularly used as a transactive memory and "has become a primary form of external or transactive memory, where information is stored collectively outside ourselves".[27] It thus shapes the manner in which we remember, and what we remember.

### 2.2 Forgetting and the external transactive memory

Humans have always used external memories, but with the adoption of information technologies, the mechanics of 'remembering' and 'forgetting' in the external memory process seem to have changed drastically.

Forgetting is a term generally used in relation to the biological brain and is a "fail[ure] to remember",[28] a glitch somewhere in the memory process that either temporarily or permanently fails to retrieve specific information. It can be the result of failures in any of the three memory process elements, partial failures, temporarily failures or of failures in the elements combined.[29]

Forgetting in the human brain arises under the combination of various factors. Simplified, three main factors play a role in the occurrence of forgetting with regard to a specific piece of information: the passing of *time*, the *meaning* of the information and the regularity with which the information is *used*.[30] Meaningful and repeated use of information reinforces the persistence of the information in memory.[31] The passing of time weakens the strength of the memory of a specific piece of information.[32] Meaning, time and use thus jointly influence the persistence of information in memory, but each can also strengthen or weaken the others' influence. For instance, information often loses value for us over time,[33] which increases the chance that it will be forgotten eventually because it will not be used.

Despite the fact that 'forgetting' is generally only used in relation to *human* agents, we think it is worthwhile to try and apply the term to the praxis of external memory stores. When regarding the concept of "forgetting" as a glitch purely on the *process level*, the term can also be applied to the external memory process, in which individuals *encode* and *store* information in the external memory store, and *retrieve* the information when they need it. Extending the term "forgetting" to the process as such can help us clarify and highlight the changes in the memory process mechanics that

---

[24] Wegner 1986, p. 188.
[25] Wegner 1986, p. 188.
[26] Wegner 1986, p. 191.
[27] Sparrow et al. 2011, p. 776.
[28] Concise Oxford English Dictionary, 11th Edition.
[29] Dudai 2004, p. 100-101.
[30] Dudai 2004, p. 100/101.
[31] Dudai 2004, p. 100- 101.
[32] Dudai 2004, p. 100- 101.
[33] Ambrose 2012, p. 390.

are caused by the praxis of external memory stores and provide guidance on how to implement "forgetting" in digital external memory.

Before the "digital turn", "forgetting" usually occurred as the result of a necessary "forgetting-by-selection" decision because of storage space restrictions over time (i.e. one can fit only so many books in a library). People had to select what to keep —to externally "remember"— and what to eliminate from the storage space.[34] The praxis of memory thus transformed from a human memory store that forgot-by-default, to external memory stores that generally remembered-by-default and required active forgetting-by-selection to make room for the most relevant information. With the "digital turn", this necessity to forget-by-selection drastically transformed and diminished, due to the continuous decline in storage space costs for digitally encoded information. In fact, the necessity for forgetting-by-selection has become so void, that often it is cheaper to get new or more storage space than to spend the effort to erase information. As some authors have already explored,[35] this led to a shift in the long-standing paradigm of human history: today remembering is natural, while forgetting has become an expensive and technically complicated business. This is most true for long-term declarative memory, both individual and collective, and more specifically, of data or document-based memory. But above all, this paradigm shift has relevance in the domain of digital memory, or at least computer-assisted memory.

As discussed in the introduction, there is growing opposition to "remembering-by-default" in certain circumstances and a call for some form of "forgetting" in external memories. The problem with fulfilling an individual's needs to "be forgotten" by an external networked memory store, is that it is not *the individual's* external memory store, but a transactive one. It is not the memory of a single agent that is at stake, but the external memory of multiple agents, each with potentially different interests in erasure or retention. The question is then how to balance the interests of these different agents in the decision to "forget" information in the external transactive digital memory. The way "meaning", "use" and "time" affect forgetting in the human brain may provide some guidance here.

"Time" is a factor that correlates with "forgetting" in the biological brain, and therefore a potentially relevant one if we are interested in facilitating "forgetting" in the digital transactive memory. Time is a fundamental dimension of the life of individuals, families, social groups and society as a whole, down to the survival of human culture. It is a fundamental dimension of memory and forgetting, too. Resources are freed up over time (potentially to be re-used[36]) and social needs to forgive and forget also take time into consideration. 'Meaning' and 'use' limit the memory decay which 'naturally' results from time lapse. The "digital turn" has undermined the technical need to forget, but not necessarily the personal and social need.

---

[34] Szekely 2012, p. 349.

[35] For example, Mayer-Schönberger (2009) who was not the first but perhaps the most influential in realizing these changes, or Szekely (2012) who extended the framework of scholarly analysis to literary dimensions.

[36] Hadziselimovic et al. 2014.

## 2.3 Nuancing persistence

Although the "[t]he Internet isn't written in pencil, it's written in ink"[37], and thus information permanence seems the rule, it is important to recognize the nuance of digital persistence. Information itself is not permanent, no matter the format. Digital information is particularly fragile. It requires a great deal of upkeep. Digital content is at the mercy of media and hardware errors, software failures, communication channel errors, network service failures, component obsolescence, operator errors, natural disasters, internal and external attacks, and economic and organizational failures.[38] This fragility has been the focus of digital preservationists who are deeply concerned about the "digital dark ages,"[39] "electronic crisis,"[40] and the "death of the digit."[41] Studies find various rates of decay, but they are dramatic ranging from rapid rates showing significant loss in days to about 10-15% lasting a few years.[42] "If we are to understand the dynamics of the Web as a repository of knowledge and culture, we must monitor the way in which that knowledge and culture is managed. We find that the Web in its 'native form' is a far too transitory medium," stated Wallace Koehler while insisting that initiatives like Internet Archive are vital to cultural preservation.[43]

Having said this, it is apt to explore whether or not the 'natural' decay observed in these studies is sufficient to regulate in the name of permanence.[44] Content persistence in fact proves that the Internet is a lazy historian with no principled practices of preserving or protecting knowledge.[45] If online information is not more thoughtfully maintained as a collection, neither goals of privacy nor preservation will be met in the future. Tinkering about mechanisms to augment the external transitive memory fits this aim.

Psychologists distinguish between short, intermediate and long-term memory, internal and external memory, visual, auditory and conceptual memory, procedural and declarative memory. Relating to these and their different (temporal) characteristics, it is possible to distinguish short, intermediate and long-term forgetting, oblivion, or even amnesia alike. These types of memory and forgetting have their own characteris-

---

[37] "The Social Network" (Columbia Pictures 2010, http://www.imdb.com/title/tt1285016/), quoted in Ambrose 2012 (Mark Zuckerberg is explained how permanent and harmful this aspect of the Internet is by his girlfriend, as she breaks up with him).

[38] Gladney 2007, p. 10.

[39] MacLean et al. 1998.

[40] Rosenzweig 2011.

[41] Feeney 1999.

[42] Ambrose 2013, citing: Gomes and Silva 2006.

[43] Koehler 2004.

[44] A particular problem with relying on natural decay is that data disappears from the Web at the whim of the data controller, not the data subject or the public. Valuable data is lost everyday while innocuous and harmful data remains. *See* Ambrose 2012,

[45] Ambrose 2012.

tic time periods and even their names sometimes reflect the length of their sphere of interpretation. If this is true, why not speak about computer-assisted forgetting?[46]

If we want to – or question whether we should – limit the reach of the digital memory we may need to re-introduce 'time' into the equation (of time-meaning-use). A primary question here is whether time plays an independent role, or whether it affects a balance of interests. We will explore this question from different perspectives, starting with the law because of its importance in regulating behavior, also in the domain of data processing.

## 3 Time in Law

This section briefly sets out the weight and role time has in evaluating a person's right to have certain information taken down. Rather than giving a detailed analysis of the relevant legal provisions and case-law, it provides a *tour d'horizon* in a European context.

### 3.1 Removing Online Content

Individuals who want to have certain information taken down have reached for technological tools and pressed corporations to provide them with concrete deletion options. In many situations, however, these solutions do not result in satisfactory outcomes for the individuals involved and as a result, they are turning to the law to find relief. Although privacy and data protection law might seem the most straightforward legal frameworks in this context, many other legal domains could be relevant (i.e. defamation law, intellectual property law, general tort law, etc.). For the purposes of this section, we focus on the role of time in the context of privacy and data protection law in particular. Not only do these constitute the most relevant legal frameworks with regard to the issues dealt with in this chapter, but also do most of the other legal regimes have specific criteria in place for assessing the legitimacy of a takedown-request (e.g., wrongfulness, public dissemination, harmful intent, etc.) in which time plays a lesser role.

### 3.2 Terminological issues

The term "Right to be Forgotten" is used in the context of privacy and data protection law. It may not come as a surprise that the concept is subject to different interpretations, which – in turn – have led to a great deal of controversy.[47] Without going into details on this, it is worth highlighting one key distinction. The right can either be grounded on the general right to privacy – in which case it can be referred to as the

[46] In fact there exist computer-assisted forgetting tools and technologies, from specific Privacy Enhancing Technologies (PETs) to user-centric identity management systems, however, their capacity and spheres of use differ greatly and they are far from being commonly used.

[47] Ambrose & Ausloos, 2013.

right to oblivion (in French, *droit à l'oubli*) – or it can be based on the data protection framework – in which case it can be referred to as the right to erasure. Time plays a role in both situations.

**Role of time in the general right to privacy**

In the movie Men in Black[48], the protagonists use "neuralizers" to eradicate (short-term) memory of witnesses to alien incidents. It is not hard to see how the right to oblivion seems to be the translation of this technical tool into law. Its terminology suggests an obligation on third parties to remove certain information from their memory. Courts have recognized a 'right to be forgotten' based on the general right to privacy – inscribed in the ECHR (art. 8) and Charter of Fundamental Rights (art. 7) – in a number of cases.[49]

Looking at European case law in particular, the right has mostly been applied in order to shield individuals from being confronted with certain aspects of their past in a disproportionate, unfair or unreasonable way.[50] The textbook example undoubtedly is the ex-convict who sees his/her name popping up in the media years after the facts. This has become particularly relevant in the context of the digitization of newspaper archives. Quite recently, the European Court of Human Rights (ECtHR) has called attention to the concerns related to online availability of more and more information. In *Delfi AS v Estonia*[51], the Court stated that "the spread of the Internet and the possibility … that information once made public will remain public and circulate forever, calls for caution."[52] In *Österreichischer Rundfunk v Austria*[53], the ECtHR specified that the lapse of time since a conviction and release constitutes an important element in weighing an individual's privacy interests over the public's interest in publication (n°68).[54] It may come as a surprise that the ECtHR has also applied the time-element as an argument *against* the RTBF. In *Editions Plon v. France*[55], the heirs of former French President François Mitterrand had opposed to the publication of a book by the ex-President's private doctor. The ECtHR ruled, however, "the more time that elapsed, the more the public interest in discussion of the history of President Mitterrand's two terms of office prevailed over the requirements of protecting the President's rights with regard to medical confidentiality."

In short, the right to oblivion is primarily invoked in situations where an individual's personal life is publicly exposed. A careful balancing exercise with other fun-

---

48 Columbia Pictures 1997, http://www.imdb.com/title/tt0119654/

49 Graux, Ausloos & Valcke, 2012.

50 Ambrose & Ausloos, 2013.

51 *Delfi AS v Estonia*, ECtHR, Application nr. 64569/09, 10 October 2013.

52 *Delfi AS v Estonia*, ECtHR, Application nr. 64569/09, 10 October 2013, N92, p. 108–109.

53 *Österreichischer Rundfunk v Austria*, ECtHR, Application nr. 35841/02, 7 December 2006.

54 Eventually, it was decided though, that the national court had given too much weight to the time-element. n°69 "The domestic courts attached great weight to the time-element, in particular to the long lapse of time since Mr S.'s conviction, but did not pay any particular attention to the fact that only a few weeks had elapsed since his release."

55 *Editions Plon v. France*, ECtHR, Application nr. 58148/00, 18 May 2004.

damental rights will therefore be imperative. In striking this balance, time may play a determinative role, though not necessarily in favor of removing the information.

**Role of time in data protection law**

The application of the Right to Erasure – vested in the European data protection framework – seems much more straightforward, at least in theory. According to Article 12 of the Data Protection Directive 95/46 (DPD), data subjects have "the right to obtain from the controller [...] the erasure of data the processing of which does not comply with the provisions of this Directive".

For the purposes of this section, the right to erasure in Article 12 can be summarized as being applicable whenever the controller either fails to fulfill its obligations or ignores data subjects' rights. Keeping in mind the focus of this chapter, three elements in the data protection framework are relevant here: (a) the need for a legitimate ground, (b) the purpose limitation principle and (c) the data subject's right to object.

First of all, the processing activities will permanently have to be tested against the legitimacy grounds in article 7 of the Directive. Particularly the first and last justifications are interesting in this regard. When the processing activities are based on the data subject's consent, the controller will have to stop further processing upon withdrawal of consent. The Article 29 Working Party has specified, however, that such withdrawal can only be exercised for the future.[56] Only when the controller cannot present any other legitimate ground for *further* processing, can the subject request erasure of the data. The last legitimacy ground, however, constitutes an incredibly wide safety net controllers can fall back on. According to this ground (art. 7f DPD), personal data can be processed for as long as is "necessary for the purposes of the legitimate interests pursued by the controller (or by the third party or parties to whom the data are disclosed), except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject". It goes without saying that this "balance of interests" gives a lot of leeway to the controller and is hard to contest by data subjects. Nevertheless, this balance might oscillate over time, at least in theory.

Second, the purpose specification principle (article 6) constitutes some sort of benchmark against which the processing of personal data will be assessed over time. Besides having to be specific and explicit, the purpose also has to be legitimate. Whereas the specificity and explicit nature will normally only be relevant at the start, the legitimacy requirement will be more susceptible to the passing of time. In its Opinion on Purpose Limitation, the Article 29 Working Party specified that the processing must – at all different stages and at all times – be based on at least one of the legal grounds.[57] This requirement, the Opinion continues, goes beyond the scope of the legitimacy grounds in article 7 and implies the purposes for processing "must be in accordance with all provisions of applicable data protection law, as well as other

[56] Article 29 Working Party, Opinion 15/2011 on the definition of consent 01197/11/EN WP187, at 33. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[57] Article 29 Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP203, pages 19-20.

applicable laws (e.g., employment law, contract law, consumer protection law, etc.)."[58] It concludes by saying that "the legitimacy of a given purpose can also change over time, depending on scientific and technological developments, and changes in society and cultural attitudes." On top of the potentially wavering nature of the legitimacy requirement, the personal data itself might also become unnecessary, irrelevant or inadequate to achieve the original (or a compatible) purpose.

Third, in principle the right to erasure can also be invoked when the data subject has successfully exercised his/her right to object. But, in order to do so, the subject will have to put forward compelling and legitimate grounds. In this regard, 'time' can both be such a ground, as well as a factor that changes the weight of the arguments for or against the right to object.

Although the data protection directive has been the subject of several cases before the Court of Justice of the European Union (CJEU) already, the right to erasure has never really been dealt with directly until the so-called *Google Spain* case.[59] In this case, the CJEU was asked whether or not search engines fall within the DPD's (material and personal) scope of application and/or whether they are subject to the right to erasure with regard to the personal data they refer to. According to the original plaintiff in this case, some of the Google Search results when entering his name are not relevant anymore (i.e. links to an article on his bankruptcy proceedings).[60] The *Audi-*

---

[58] The Working Party further elaborates that legitimacy also has to be tested against: "all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts. Within the confines of law, other elements such as customs, codes of conduct, codes of ethics, contractual arrangements, and the general context and facts of the case, may also be considered when determining whether a particular purpose is legitimate. This will include the nature of the underlying relationship between the controller and the data subjects, whether it be commercial or otherwise."

[59] CJEU C-131/12, still pending at the time of writing. This case involved a Spanish individual that had been subject to bankruptcy proceedings in the nineties. Spanish law required a local newspaper (LaVanguardia) to publish information on the public auction resulting from the bankruptcy. Upon digitizing its archive, links to this information popped up in Google Search results when entering the individual's name. The individual addressed himself to the Spanish data protection authority, requesting the removal of the article and search results. The DPA denied the request vis-à-vis the newspaper (as it had a legal obligation to publish the information in the first place) but did order Google to remove the link from its search results. The search giant appealed and the *Audiencia Nacional* referred some of the questions raised to the CJEU.

[60] Some say that the market may take care of the problems the RTBF seeks to address. Google's Eric Schmidt, for instance, writes that employing the services of an "identity manager" to maintain one's online presence will be "the new normal for the prominent and those who aspire to be prominent" (Schmidt, 2013). Reputation services, as these identity managers are often called, can be paid by data subjects to move search results to pages beyond the effort of most searches. In order to move pages with content detrimental to the data subject to such an obscure rank, reputation services will flood the Web with content about the data subject. We find this solution to the problem unsatisfying for three reasons. The reputation

*encia Nacional* (referring court) acknowledged that today, it is possible to create very detailed personal profiles in just a couple of clicks, with information that used to be difficult to find. The lack of territorial and temporal limitations to the dissemination of information constitutes a danger to the protection of personal data. The Spanish Court further specified that originally lawful and accurate personal data may become outdated overtime in the face of new events. Some of this information might actually generate social, professional or personal harm to the individual concerned. Indeed, one might claim that the impact of search engines (among others) is such that individuals are perpetually overshadowed by certain past events/facts that might not accurately – or in a proportionate way – represent their current capabilities. It could even be argued that with the right search terms, practical obscurity on the Internet is a myth.

Concerns over perpetual storage of (personal) data have also manifested themselves in the context of another legal framework before the CJEU. In *DRI & Seitlinger*[61], the Data Retention Directive 2006/24 was at stake. The Directive specified a data retention period between a minimum of 6 months and a maximum of 24 months. The Court decided that EU legislation exceeded the limits imposed by the principle of proportionality in Articles 7, 8 and 52(1) of the Charter, inter alia, because the retention period is relatively open while it must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

### 3.3 Two roles 'time' can fulfill in law

It is hard to draw clear conclusions regarding the role of 'time' vis-à-vis the RTBF in a privacy and data protection context. What can be said, however, is that the concept seems to play two parts. Either, and commonly, time is a factor adding (or removing) weight to the request to removing personal information or its opposing interest (e.g., public interest), resulting in tipping the balance in either direction. Generally, the older information is, the less valuable retaining it is. The second role time can play is as the marker of the tipping point when the grounds for retention no longer hold and erasure of the data should follow. Passing an agreed retention period for data is a case in point. Sometimes, however, it is not so much time itself that causes the flip, but rather some other conditions being met at some point in time. This is the case where the purpose limitation principle is at play. Once the stated purpose is reached, there is no longer a legitimate ground for data retention, and hence from that moment

service requires that a mass amount of data be presented about an individual, which is a problematic solution for anyone seeking to be 'left alone.' Additionally, these services are constantly battling search engines who do not appreciate their systems being gamed. Finally, this practice represents poor treatment of such a valuable information source. The only option for data subjects should not be to dilute the Internet with fluff.

61 Judgment - 08/04/2014 - Digital Rights Ireland and Seitlinger and Others Case C-293/12 (Joined Cases C-293/12, C-594/12), http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=52531

in time onwards, data retention is no longer legitimate. This second role of time (time as boundary marker) especially comes to the fore in Article 17 of the proposed GDPR. In the Commission's proposal, data subjects will be able to invoke the right when the data are "no longer necessary in relation to the purposes for which they were collected/processed" or when the predefined storage period has expired.

Before we discuss the former role of time (as a weight in a balance of interests), we first explore time in its role as discrete tipping point in the discussion whether personal data should be retained or deleted.

## 4 Law, time and the use of information: specific points in data processing

In this section we explore the life cycle of the creation and use of data and information and we highlight situations in which the decision of whether or not to create/retain/delete data is relatively straightforward. We identify specific points in data processing, which also denote specific points or periods in time, where enforcing of RTBF is reasonable or even necessary. Since data protection law and specific rules concerning data processing, are codified, it is easy to find legal arguments for interpreting these specific points. However, it should be emphasized that such legal arguments can only be interpreted in a constitutional, rule-of-law democracy, or in a narrow sense, in the legal system of the EU. Nevertheless, there are also moral arguments and fundamental values, which may be evoked to support these legal arguments.

### 4.1 (Moment in) time as a discrete boundary for erasure/retention

*(a) Before recording of information takes place*

Prior to the actual collection and further processing of personal data, a decision can be made not to collect the data in the first place. Data that are not collected do not require a decision to delete or retain data later on. The time preceding data collection decision therefore is relevant for our purposes. For example, if someone wants to make a photo or video recording of someone else's activity, and the data subject realizes the preparations, the subject may ask him not to do so. The subject generally has a right and moral arguments to support his demand, although there are situations when this preliminary step cannot be applied: if someone actively participates in a street demonstration, he cannot demand recording of his participation not be made – he has become, even if temporarily, a public figure, performing public functions, and his activity is information of public interest, even if in a formal sense it can be regarded as his personal data. He cannot discriminate certain media either; he cannot distinguish friendly and adverse reporters or television channels.

*(b) Immediately Upon Recording*

If the data subject discovers that his personal information is being, or has just been, recorded, he may demand the immediate deletion of the information, thus preventing the spread of the recorded information. The ubiquity of information recording devices nowadays implies that individuals can be part of such a scene instantly and constantly in particular (but not solely) in public spaces. Although there is pressure from the data industry to record and distribute ever more personal information, the moral right to object to such recordings is acknowledged. For instance, in some non-European countries where legal protection is weaker, the industry has accepted a de-facto norm that recording equipment make a shutter-click noise that cannot be turned off in order to call data subjects' attention.[62]

The mainstream (printed and electronic) media have traditional privileges in recording and distributing personal information. This is partly reflected in the press law, partly in the practice of courts in press-related lawsuits, and partly in the codes of ethics of the media. Typically, the media are allowed to record information on identifiable persons in public spaces, for example as part of a long shot, however, zooming in on individuals and recording this information is allowed only if consented by the persons concerned.[63]

Again, this demand for deletion of the recorded information cannot be applied when the data subjects perform public functions.

*(c) When a legal deadline expires*

Under the data protection regulation, data controllers can lawfully process personal data (provided the other requirements are met, see section 3) as long as they are necessary for specified purposes. This may include being able to prove the existence of a relationship between parties after the primary relationship ended (e.g., contractual obligations completed). After this period there is no legitimate ground for retaining the data. In criminal law, information on prior convictions is kept in official registers until the expiry of the time prescribed by law, after which no detrimental legal effects shall apply on prior convicts. Similar expiry dates apply to minor offences, too. After these dates the data subject may receive a clean certificate of good-conduct. The expiry of such deadlines generally imposes an obligation on the data controller to delete

---

[62] Smartphones manufactured and purchased in Japan or South Korea have this well-known feature, and lawmakers seem to have declared programs disabling the shutter sound illegal, see for example http://www.unwiredview.com/2012/04/20/south-korea-to-ban-cameraphone-shutter-sound-removers/ or http://news.asiaone.com/News/Latest+News/Science+and+Tech/Story/A1Story20111214-316106.html

[63] As a main rule, the media can record such information under *prior* consent of the people concerned, however, there are some exceptions when asking for prior consent would spoil the situation. In such cases consent should be obtained right after the recording is made, on the spot – and if the consent is not given by the subjects, the recording should be deleted immediately. Well-known examples of such a situation are the candid camera type programs, when only those recordings can be seen on television, which the victimized subjects consented to after realizing the fact of recording (and that is why all such broadcasted episodes end with laughter, and not with angry reactions).

the data. The concerned person may also require the deletion of her data forwarded earlier to other data controllers.

*(d) When the conditions of lawful data processing are not met*

In some cases processing of personal data takes place without meeting the conditions of lawful data processing as prescribed by data protection law. Such situations may occur, for example, when a data subject withdraws her consent and her data is retained and used nevertheless, or the purpose of processing does not exist anymore. In these cases, time is not an autonomous factor, but the legitimacy of data processing is limited in time (in hindsight). A complicating factor here is that data subjects may sometimes realize the non-compliant processing only ex post facto.

A special case occurs when a person objects to the processing of her personal data in the area of direct marketing. Many direct marketing laws obligate data controllers (the marketers) not to delete such data, but to put them on a separate list, the so-called Robinson list. The purpose of such a list is to filter out the "Robinsons" and not target them in subsequent marketing runs. As in the previous cases in this category, the legitimacy of processing here is in a sense limited in time. There, however, is no right to erasure after this point, but only a sort of "filtered use" of the subject's data in the future.

*(e) At pre-defined (or default) dates*

Comprehensive user-centric identity management systems like PRIME[64] envision a network of compatible data processors within which rules set by laws and individual contracts, or defined by data subjects themselves, are automatically enforced. For example, if the data subject posts a photo to a social network site for two weeks only, after this date the photo will automatically be deleted (and not only from the primary data processor but also downstream from all systems adhering to the same standard). Despite working prototypes, PRIME(-like) infrastructures on a large scale are still only a dream.

From a different perspective, Mayer-Schönberger suggests a related idea: each piece of personal data should have an expiry date after which it should automatically be deleted.[6566] Such expiry dates may be defined as default characteristics of the data processing system, but may also be defined individually by the data subject. The expiry dates may be changed before the deletion of the data.

*(f) Grey zone: data of the deceased*

Death is the ultimate turning point in people's life, marking the end of being a legal subject, however, not necessarily meaning the end of remembering the deceased person. In most legal regimes the data relating to the deceased are not personal data in

---

[64] Privacy and Identity Management for Europe, http://www.prime-project.eu. See also Camenisch et al. 2011.

[65] Mayer-Schönberger 2009.

[66] A practical application of this notion can be found in the popular social media application Snapchat, where users can upload images ("Snaps") that are visible to recipients for a period from 1 to 10 seconds to be decided by the poster.

the strict sense of the word[67], although the virtually indelible data of the deceased may revolve in web-based services for a long time. In the case of the deceased, the RTBF can only be enforced by surviving relatives. In this case it is not the protection of personal data but the protection against the injury to the memory of a deceased person which may be applied, and the relatives are entitled to file for court action.

We can imagine the history of data relating to a deceased person as an ever fading grey zone, or a virtual trail of a comet, which at the beginning (at the luminous nucleus of the comet) is very close to the personality of the deceased, and through the passing of time becomes mere historical data, gradually losing its personal nature.[68]

It should be noted that data relating to the deceased may also relate to the surviving relatives and hence the decision whether or not to erase the data depends on more factors than just the interest of the deceased.

*(g) Never*

There are cases when RTBF can never be enforced lawfully. This is the case of personal data of persons performing public tasks, generated in connection with their task. These data are strictly speaking personal because they relate to an identified or identifiable natural person, but the person is treated as an institution rather than as an individual and the public interest prevails over the private interest of the individual. Similarly, personal data lawfully published in the media cannot be erased either. It is questionable whether this rule applies to online media, too, since a fundamental purpose of the RTBF is exactly to counterbalance the unintended consequences of using new media.

*(h) Special case: Memory-preserving institutions*

This case represents one of the most controversial domains of RTBF: forgetting in archives and other memory-preserving institutions. The international archiving community has strongly opposed the enactment of art. 17 GDPR.[69] Administrative archives are operating under legal obligations, which are at odds with a right to be forgotten or erasure for data subjects. Historical type archives (in particular the ones collecting documents on recent history) are meant to preserve history for the benefit of the future. Removing personal data from the archives infringes upon this purpose. Hence it comes as no surprise that, according to the draft EU Regulation, RTBF shall not apply to the extent that processing of the personal data is necessary for historical, statistical and scientific purposes.

---

[67] For instance, art. 2a of the Data Protection Directive 95/46/EC limits personal data to natural persons, which ties the scope to legal personality in civil law. In civil law legal personality terminates at death. See also Art. 29 Working Party Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP136, p. 22. The Working Party discusses some special cases where data of the deceased indirectly receive some protection.

[68] In the age of Facebook profiles, avatars and Internet archives this fading of personal nature is less and less obvious, and the questions of post-mortem privacy has become a growing research area, see for example Harbinja 2013 and Edwards & Harbinja 2013.

[69] See the declaration of the Association of French Archivists 2013.

### 4.2 Use and time

This section has elaborated on discrete moments in time in which it is relatively clear whether personal data can be retained or has to be deleted. The interests of the data subject who wants their data be removed are at the core in the cases elaborated. In most cases discussed, only the data subject (or relatives in case the data subject is deceased) and the data controller hold acknowledged interests. The examples have focused on the immediate information needs of these parties. The use of information by third parties seems to only be acknowledged in the special case of the memory preserving-institutions (in which the information already has a context-specific meaning). Remote information needs, be it from archivists who aim to preserve our times for future historians or from predictive analytics which may improve health care, or from entrepreneurs who want to have legal certainty regarding the reputation and creditworthiness of their business partners, also play a role in RTBF decisions. Third parties use the information in the external transactive memory and may rely on it. It is here where a balance of interests needs to take place leading to deleting or retaining certain personal data. Time, as said, plays a role in this balance as a contributing or limiting factor. In the following section we elaborate on the role of time with respect to 'use' and 'meaning'. We will look at the meaning of information in its data life cycle, and the changing balance of different interests in time.

## 5 Balance of interest over time

It has been said that the RTBF "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."[70] In this section we take a closer look at the balance of interests over time, where the passing of time influences the meaning and use of information by different parties, and thereby affects the balance of their interests.

### 5.1 Changing balance of interests: data life cycles

In order to shed some light on the manners in which the balance of interests can change over time, we shall group the interests involved in data protection cases into two sets. On the one hand the *pro-processing interests*, which include all legally relevant interests promoted through the processing of the personal data at issue, and on the other hand the *con-processing interests*, which include all legally relevant interests that may be demoted by the same processing. Pro-processing interests may comprise diverse meanings and usages of information, such as economic and non-economic goals, and right and values, such as economic freedom, efficiency, property interests, security, freedom of expression, freedom of information, transparency, democracy, and equal judicial protection. The most important pro-processing interests are based on the meaning data hold for the public, the values currently secured in the

[70] Weber 2011.

exceptions of Art. 17(3) of the proposed GDPR that allow for retention of data: (a) to protect the right of freedom of expression; (b) for reasons of public interest in the area of public health; (c) for historical, statistical and scientific research purposes; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law.[71] Con-processing interests similarly may include not only privacy and data protection rights strictly understood, but also the rights to private life, identity, self-determination, non-discrimination, a fresh start, protection from unwanted intrusions, dignity, etc.

We model the changing balance of pro-processing and con-processing interests in a graphic form, as in figure 1. The horizontal axis represents the passage of time, from the initial moment when the processing has started ($t_0$). The vertical axis represents the *legal impact* that the processing has with regard to the *pro* and *con* interests. The full curve represents the importance of positive impact on pro-interests and a dotted curve represents the importance of the negative impact on con -interests. The curve over time is the expression of the data's life cycle; "information as it changes value through the full range of its life cycle from conception to disposition."[72]

For instance in figure 1, at $t_0$ the curve corresponding to pro-interests is much higher than the curve corresponding to con-interests. This means that at $t_0$ the positive legal impact which the processing provides by promoting certain interests is much higher than the negative legal impact that the same processing causes by diminishing the data subject's privacy. Therefore, processing at $t_0$ provides a net benefit all things considered. Consequently, a regulation permitting it also has a positive legal impact, all things considered.

We shall here focus on cases where the originally prevailing pro-processing interests are outweighed at a later stage by con-processing interests. This happens in particular when the personal information is distributed online for purposes pertaining to journalism, or more generally to freedom of expression. In such cases, there is generally a continuous diminution in the importance of the distribution of information with regard to both pro- and con- processing interests, up to the tipping point. This is because public interest, more aptly called public intrigue here, is quite fleeting, and thus the public meaning and use of information is equally fleeting. Entering any number of momentary Internet snafus (e.g., Alexandra Wallace, Caitlin Davis, Justine Sacco) reveals spikes in search activity over a matter of weeks and then a sharp drop back to insignificance.[73] The 'newsworthiness' of content generally protects the public's right to access the information.[74] Like data freshly created (e.g., current address, purchases,

---

[71] DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) adopted in the first reading of the Parliament on 12 March 2014.

[72] Hill 2009, p. 57.

[73] See Ambrose 2012, p. 413 for examples taken from http://google.com/Trends.

[74] "Newsworthiness" varies across jurisdictions. *See* e.g., *Time, Inc. v. Hill*, 385 U.S. 374 (1967); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); *Florida Star v. B.J.F.*, 491

body measurements) this information is relatively current, contextualized, and new before it becomes outdated, uncontextualized, and condensed or aggregated. Older personal facts are generally less meaningful for both the public and the data subjects and are thus also less used. In particular, older information about a person usually gives a less relevant clue to what and who a person "is" now, and therefore should in general be less meaningful, both for those who want to know about that person and for the person herself. There are, obviously, deviations from these general trends where certain past information suddenly may become more important to the public and/or more damaging to the data subject.[75] For instance, when data subjects apply to elective political positions, their data concerning any past criminal or inappropriate behavior becomes more meaningful to the public. Here, we shall just consider the more common case when there is a continuous decrease in the importance of impacts on both pro- and con-processing interests. Consider for instance those cases where personal information related to crimes or bankruptcies is distributed and remains accessible after such events took place.[76] This information is most relevant to the public for a short time after its publication because of its actuality, and then progressively loses its meaning and is used less, but continues to have a significant impact on the interests of the concerned person also because it may affect how that person is publicly perceived. In such cases, usually both impacts on freedom of expression and on privacy decrease as time goes by, but the diminution of the impact on freedom of expression proceeds at a quicker pace. Thus while at the beginning the benefit to the public would outweigh the loss to privacy, at a certain point in time, i.e., the reversal time, there is a change: the loss in privacy outweighs the benefit in freedom of expression. This is the point in time where, arguably, the data should be forgotten. In this typical context the pro-processing interests prevail over a RTBF up until a certain point in time, and after that point privacy takes the lead, as shown in figure 1.

U.S. 524 (1989); C. von Hannover v. Germany, ECHR, 26/4/2004, Rec. 2004-VI 40 EHRR 1; Schwabe v. Austria, ECHR, 28/8/1992, A 242-B.

[75] See Ambrose 2012 and Sartor 2014.

[76] Cf. the Google Spain case referred to in section 3 (footnote 59).

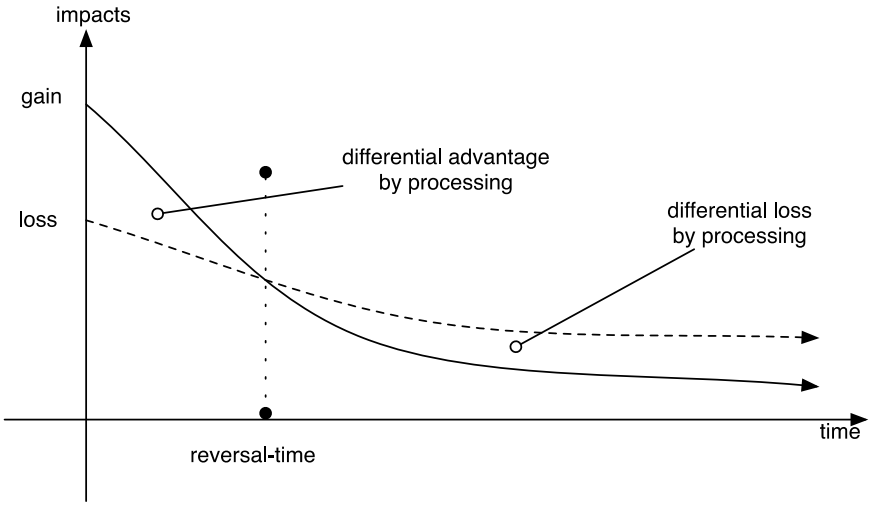


**Figure 1 The impact of processing (line) and non-processing (dotted line) over time**

Figure 2 clarifies this point by representing directly the difference between the differential advantage resulting from the favorable impact on publicity-interests (the publicity-related gain) and the differential disadvantage resulting from the unfavorable impact on privacy-interests (the privacy-related loss) obtained by processing the information. The balance is positive before the reversal-time, it is 0 at that point and then it becomes negative.

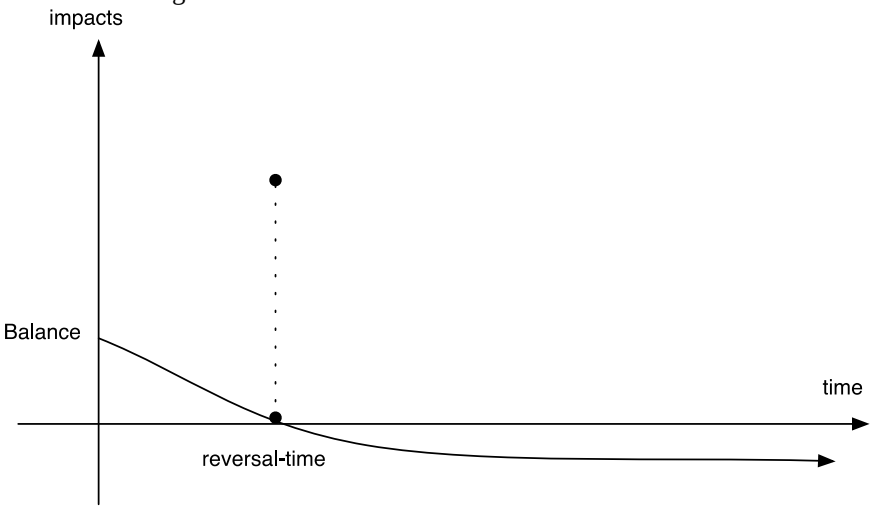


**Figure 2** Net social value of data processing over time.

### 5.2 An increase in pro-processing interests over time

The pro-processing interests are not always declining in time, because the benefits are not always immediate. Public interest in that which is newsworthy may be fleet-

ing, but public interest in history, social science, and cultural preservation last far longer. Think for instance of historical interests or when there is revived interest in the specifics of the content (e.g., an individual decides to run for office), as well as immediate interests met remotely when information is combined, aggregated, or reflected upon revealing previously unknown insights into the past or future.[77] The difficulty is that 'history' may be hard to recognize immediately, the interest very likely grows over time with regard to certain data subjects instead of declines.

However, we may be able to cope with such long-term interests in different ways. Because there is a significant difference between individuals like employers or first dates searching an individual and public interest, the meaning of the information in a context can differ; the employer is looking for a specific person while the public interest generally (not always) will be focused on a certain event in its context. Wikipedia's Biographies of Living Persons Policy draws a distinction between general public interest in the individual or the event or topic of an entry. It reads:

> "Caution should be applied when identifying individuals who are discussed primarily in terms of a single event. When the name of a private individual has not been widely disseminated or has been intentionally concealed, such as in certain court cases or occupations, it is often preferable to omit it, especially when doing so does not result in a significant loss of context... Consider whether the inclusion of names of private living individuals who are not directly involved in an article's topic adds significant value."[78]

Based on this policy, the Star Wars Kid is not named in the entry on the Star Wars Kid.[79] Wikipedia also has a deletion policy that results in five thousand pages being deleted each day, one reasoning being a lack of 'notability,' which requires significant coverage, reliability, sources, independence from the subject, and a presumption that the subject is suitable for inclusion.[80] According to the policy, articles with unclear notability should not be deleted, but those that are clearly not notable should be and useful material preserved on the talk pages,[81] which are not indexed by Google.[82] Like Wikipedia, the right to be forgotten could (but does not) ask the difference between public interest and private searches in order to determine the right course of action when a user seeks to have personal information erased, as opposed to quick deletion or automatic public interest preservation. In some cases public interests may be served just as well by content that is anonymized (interference with the memory process on the level of encoding), as was done with the Star Wars Kid entry on Wikipedia. Moreover, preservation efforts could seek to conserve that personal data that may

---

77 For further discussion of the information life cycle, *see* Ambrose *supra* note 6.

78 "Wikipedia: Biographies of living persons – Wikipedia, the free encyclopedia," http://en.wikipedia.org/wiki/Wikipedia:Biographies_of_living_persons#Presumption_in_favor_of_privacy.

79 "Talk: Star Wars Kid," Wikipedia, http://en.wikipedia.org/wiki/Talk:Star_Wars_Kid.

80 "Wikipedia: Notability," Wikipedia, http://en.wikipedia.org/wiki/Wikipedia:Notability.

81 Id.

82 "Wikipedia talk: Talk pages not indexed by Google," Wikipedia, http://en.wikipedia.org/wiki/Wikipedia_talk:Talk_pages_not_indexed_by_Google.

continue to serve remote needs while offering limited search access where appropriate and in this way enabling a form of "forgetting" on the retrieval level.[83]

### 5.3 Carrots and sticks

To determine how to regulate "digital forgetting", it is not sufficient to consider the interests at stake. We also have to consider the motivations of the parties involved. Let us now focus on cases concerning the publication of publicly relevant information on online platforms.

A simplified representation is provided in the upper part of figure 3 where a linear relationship is assumed between the represented interests and time. In part A of figure 3, the pro-processing curve starts at the higher level, but decreases more rapidly than the con-processing curve, so that at a switch point the two lines cross: from that point on, the damage to con-processing interests is no longer compensated by the benefit to pro-processing ones. Subsequently, processing provides a negative legal trade-off, which apparently justifies its impermissibility, and the provision of sanctions upon the processing parties, i.e., publisher/uploader of the information and the host provider who is storing it in his virtual repository (server/website/forum).

[83] For instance, the Internet Archive does not offer full-text search functionality on the site, but Google has performed a complete crawl of the site allowing the archive to be searched using Google's "site:" feature. The Internet Archive also has detailed instructions for using robots.txt to prevent crawls and removal policy where the technical solution is not possible. "Removing Documents from the Wayback Machine," Internet Archive, at http://archive.org/about/exclude.php.

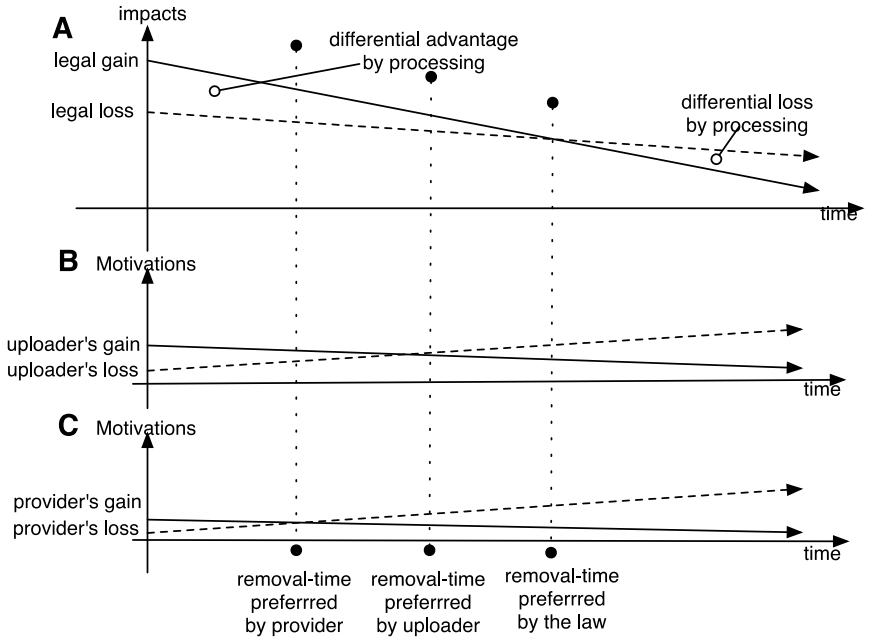


**Figure 3 Impacts of data processing related to interests over time.**

Figure 3 also contains a representation of the motivation uploader (part B) and of the host provider (part C), both of which are also decreasing, but remain positive (assuming that no sanctions are provided).

The meaning that data has for uploaders can differ and thus their motivation to upload. The uploader's motivation includes the economic gains the uploader expects from distributing the information (as is the case for newspapers and websites or host providers getting subscriptions or advertising), but also includes the moral and social importance one attributes to providing such information. Abstracting from different individual attitudes, we may assume that motivation for distributing information is measured by the maximum personal loss one would be ready to sustain for not distributing it, regardless of the grounds that explain this attitude.

Consider, for instance, the situation of a person who has to decide whether to upload on a blog information concerning a political or economic scandal, knowing that this may cause him some personal advantage (e.g., reputation, some chances of having a political role in the future, possible some financial gain resulting from the fact of attracting people to the blog) but larger personal losses (e.g., losing possible contracts, missing career advancements, even putting at risk one's life or freedom, etc.). Knowing also that this information would be highly beneficial to the public, contributing to curb the plight of corruption, while damaging the data subject,the motivation of such a person would likely be measured neither by the mere trade-off of personal gains and losses, nor by adding to this trade-off the full amount of the expected (net) public benefit. It would rather be measured by adding to the trade-off of personal gains and losses a quantity expressing the limited extent up to which the person internalizes the

moral/social merit of his action, i.e., a quantity that indicates what additional personal loss he would be ready to sustain to accomplish that action.

Consider for instance a piece of news being published in an online journal, and assume that after a certain point in time the legal balance becomes negative. At that point in time, the publisher will still have an interest in keeping the news online, since it may still attract readers and thus produce revenue. Thus, if there were no law in place (abstracting from the possibility that the data subject uses private sanctions of incentives), the publisher would probably continue to distribute the information even when the legal trade-off has become negative.

The motivation is assumed to be similar to that of uploaders, while being generally lower, since providers host huge amounts of materials and have a small interest in continuing to distribute a specific single piece of information. Providers have a strong interest in having a legal discipline that does not make them liable for the distribution of illegal information. However, if the battle for a general exemption were lost, they would prefer to comply with removal requests, rather than be subject to sanctions in individual cases.

**Sticks.**

We may assume that sanctions for failure to remove the data may include the compensation of the damage to the data subject, as requested by Art. 23 DPD. This compensation, according to national regulations, such as the Italian one, may also include non-economic damage. In addition, the sanctions may include administrative or criminal fines, as established by national legislation and required by the GDPR.

If such sanctions were always to be imposed upon a processing only after the point in time where the balance between pro- and con-processing interests is reversed, and the processing party knew exactly where this point is located, such a discipline would induce the behavior that maximizes the achievement of legal values. Before the reversal-time uploaders and providers would leave the material on line, since they could enjoy the benefits resulting from the distribution of the information without encountering any legal sanction. After that point, they would take it down, since continuing to distribute the information would expose them to the obligation to compensate damages of the data subject, and to any further sanction established by data protection law.

This analysis however, does not consider that processing parties may be uncertain as to whether distributing certain information at a certain point in time provides a positive or a negative balance between publicity and privacy interests, being therefore lawful or rather unlawful. Or in any case, they may be uncertain as to how the competent decision maker will judge the issue. This uncertainty will very likely lead to premature withdrawal of the material by the parties involved in the distribution, i.e., at times when publicity interests still outweigh privacy interests. This anticipation will be larger when the uncertainty is greater or the motivation to distribute the material is smaller. If we assume, as it seems reasonable that uploaders have a stronger motivation to keep the material on line than providers, the expectation of a sanction will have a stronger anticipatory effect on providers than on uploaders, as Figure 3 shows. Thus, uploaders and host providers would engage in premature self-censorship by

honoring removal requests at times when the benefits of keeping the information on line still exceed the damage to the privacy interests of the concerned data subjects. Note that to have this effect the sanction does not need to be extremely severe: it suffices that the sanction, discounted by the probability of not being punished, overrides the motivation of the uploader. Also a punishment limited to damages (in particular when also moral damages are included) may have such a result. Hence, sanctioning the continued distribution from the point in time when the con-processing legal interests outweigh the pro-processing ones is likely to lead to anticipatory removal. Anticipatory removal would also happen when an unfulfilled request by the data subject was needed to trigger the sanction: anticipated requests would lead to anticipatory removals.

Consequently, a takedown system, where a user can simply request data be removed, requires the data controller to perform this assessment for themselves, which may lead to valuable information being removed, because there is so little guidance on how time should be incorporated into the removal equation.[84] While a RTBF that adheres to a life cycle approach is better than one that does not, data controllers may not be the appropriate source for establishing a standard for interpreting exceptions. In order for the RTBF to account for the interests of the data subject, the data controller, and the public, more guidance that recognizes the digital life cycle (ephemerality of digital content and public interest, as well as the value to remote and immediate users) would certainly bolster the legitimacy and strength of the RTBF.

## 6 Conclusion

In a world where you are what Google says you are and digital dossiers impact automated opportunities beyond view, the RTBF plays an important role in user participation. The complication is that information removal can be just as dangerous as information storage. Digital information sources, and especially the Web, function as very large external transactive memories. Acknowledging the growing wish of individuals to counter the 'remembering-by-default' of this memory requires the implementation of a form of digital 'forgetting'. However, because it is an external *transactive* memory, data controllers and data subjects are not the only parties to be considered, but also the interests of others: the public. Balancing these interests is difficult. We can, however, gain guidance and inspiration from the human memory process in which the factors 'meaning', 'use' and 'time' play important roles. 'Time' is a factor that generally supports 'forgetting' when the passed time increases, while 'meaning' and 'use' generally oppose forgetting when the meaning information and/or the frequency with which it is used increases. This makes 'time' a crucial element to acknowledge in relation to the RTBF. 'Meaning' and 'use' are often in some form or the other recognized by law as being important factors to retain data. For instance, the exceptions mentioned in art. 17 (3) GDPR, inter alia the freedom of expression, scien-

[84] Ambrose 2013.

tific and historical interests, are of such importance to the public that they oppose the 'forgetting' of the information.

However, beyond this general expression of the societal value of data retention in view of time, the exact role that time plays in current privacy or data protection law is not clear. Generally, 'time' can play two parts in law. On the one hand, 'time' can play a role as a weight in a balance of interests, as a factor adding or removing weight to the request to 'forget' personal information or its opposing interest, resulting in tipping the balance in either direction. On the other hand, 'time' can play a role as the marker of a discrete moment where the grounds for retention no longer hold and 'forgetting' of the data should follow.

In section four the important points in time in data processing are identified, where time functions as a marker of a discrete moment in the information process. The identification of these points show that the 'time'-cycle of data processing highly depends on the use of the data; the conditions under which the data are acquired, the purposes for which they are collected, and whether they are necessary. The analysis of the specific points in data processing shows the importance of the point in time with regard to the use of information in data processing for the invoking of a RTBF. Generally at the stages in the process where the information loses relevance for its use (at least for the initial purpose for which it was collected), the chance for a successful appeal on a RTBF is increased.

The role of time as a factor in a balance of interests is more complex. Important for this balancing is to recognize that information has a lifecycle and its value (also to the different interested parties) changes over time. Data is generally created to meet the current state of affairs in the world and has the most meaning and value in that context. The 'newsworthiness' of content is thus often fleeting, and information can easily become outdated, uncontextualized, and condensed or aggregated. Next to immediate needs, information can serve remote needs as it is combined, aggregated, or reflected upon revealing previously unknown insights into the past or future. Despite the fact that these information needs are important, there is very likely a point in time where the added value of personal data retention has diminished so far that the interests of the individual to be 'forgotten' prevail.

Utilizing time can help to inform appropriate decisions about the value of information. Because 'time' generally is an important force opposing memory processes and enabling forgetting, it should be of importance for the implementation of a right to be (digitally) forgotten. 'Time' could play a pivotal role, because at an operational level, it provides a tool for assessing the value of data or content, which is necessary in order to apply the exceptions and weigh rights and interests. However, the 'time' in relation to information life cycles will need to be researched more closely before it can be shaped into a usable tool. The role that times plays is very complex. A specific time span can mean something completely different for the data subject (lifetime perspective), the data controller (processing and use time) and for third parties (public interest, transactive memory use). The passing of ten years in time has a different meaning in relation to the lifetime of an individual than it has in relation to historical interest of the public. The awareness of different time spans can tell us something about the time span that should be used for the implementation of the RTBF. Over the

course of creation to storage to aggregation to edits to maintenance activity or death, digital data may serve or fail to meet immediate or remote needs. Both information needs are important and should be protected, but personal data at some point, may serve neither. This is the point in the information life cycle where a RTBF may be viable without triggering an exception. But how long and how little interest or use decreases the value of information enough to be overpowered by the interests of the data subject? And how does this time span relate to the lifetime of an individual? Many questions still remain to be answered, but what is clear is that approaching the RTBF from a time span that transcends the lifetime of a data subject defies its own use, because the rationale behind the RTBF is that individuals can achieve greater control of their (informational) *life*.

The changing role of time in this –already complex– balance of interests requires more specific research. Several issues will need to be explored like the balance between accountability and erasure and the balance between preservation and privacy. The point we stress in this paper is that we should not overlook or disregard the importance of 'time' when we are shaping policy mechanisms like the RTBF that aim to introduce 'forgetting' into data processing. Taking the passing of time into consideration can help assess the information landscape at issue for the RTBF and account for the changing values of information as it ages, establishing the balance all rights must find with other interests.

**Acknowledgments.** This paper originates from the "Timing the Right to Be Forgotten" panel-discussion at the Computers, Privacy and Data Protection conference (CPDP) in Brussels 2014[85] organized by the Tilburg Institute for Law, Technology, and Society (TILT). We therefore would like to express our gratitude to TILT and CPDP for supporting and making this discussion possible. Paulan Korenhof her research is conducted within the Privacy and Identity Lab (PI.lab) and funded by SIDN.nl (http://www.sidn.nl).

[85] The video recording of the panel discussion and the presentations of the participants are available on the conference website, http://www.cpdpconferences.org/

## References


Ambrose, M.L. (2012). It's about time: Privacy, information lifecycles, and the right to be forgotten. *Stanford Technology Law Review, 16*, 369-422.

Ambrose, M.L. (2013). Speaking of Forgetting: Analysis of Possible Non-EU Responses to the Right to be Forgotten and Speech Exception. In *TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy*.

Ambrose, M. L., & Ausloos, J. (2013). The Right to be Forgotten Across the Pond. *Journal of Information Policy, 3*.

Anderson, M., Eysenck, M.W., Baddeley, A. (2009). *Memory*, London: Psychology Press.

Andrade, De, N.N.G. (2012). Oblivion, the right to be different from oneself. Reproposing the right to be forgotten. *VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet", IDP. Revista de Internet, Derecho y Política, 13*, 122-137.

Association of French Archivists (2013). The European Parliament: Adjourn the adoption of the regulation about personal data. Retrieved from https://www.change.org/petitions/the-european-parliament-adjourn-the-adoption-of-the-regulation-about-personal-data

Berg, Van den, B. & Leenes, R. (2010). Audience segregation in social network sites. *Social Computing (SocialCom), 2010 IEEE Second International Conference on Social Computing/Second IEEE International Conference on Privacy, Security, Risk and Trust). Minneapolis: IEEE*, 1111-1117.

Camenisch, J., Leenes, R.E. & Sommer, D. (Eds.), *Digital Privacy: PRIME – Privacy and Identity Management for Europe*. Heidelberg | Dordrecht: Springer.

Clark, A. (2003). *Natural-born cyborgs: Minds, technologies, and the future of human intelligence*, Oxford: Oxford University Press.

Draft Report (2012). 2012/0011 (COD). Retrieved from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

Edwards L., & E. Harbinja (2013). Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased In A Digital World. *Cardozo Arts & Ent LJ, 32*, 83-377.

Feeney, M. (Ed.) (1999). *The Digital Culture: Maximising the Nation's Investment* (A Synthesis of JISC/NPO Studies on the Preservation of Electronic Materials). London.

GDPR (2012). Proposal for a General Data Protection Regulation, COM(2012) 11 final, 25.1.2012. Retrieved from http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf.

Gladney, H. M. (2007). *Preserving digital information* (pp. I-XXIII). Berlin: Springer.

Gomes, D. & Silva, M. J. (2006). Modelling Information Persistence on the Web, in Proceedings of the 6th International Conference on Web Engineering. ICWE'06.

Graux, H., Ausloos, J., & Valcke, P. (2012). The Right to Be Forgotten in the Internet Era. T*he Debate on Privacy and Security over the Network: Regulation and Markets*, 93-106.

Hadziselimovic, N., Vukojevic, V., Peter, F., Milnik, A., Fastenrath, M., Fenyves, B. G., ... & Stetak, A. (2014). Forgetting Is Regulated via Musashi-Mediated Translational Control of the Arp2/3 Complex. *Cell*, *156*(6), 1153-1166.

Harbinja, E. (2013). Does the EU data protection regime protect post-mortem privacy and what could be the potential alternatives? *SCRIPTed*, Vol. 10, Issue 1. Retrieved from http://script-ed.org/?p=843

Hill, D. G. (2009). *Data protection: Governance, risk management, and compliance*. CRC Press.

Husovec, M. (2014). ECtHR rules on liability of ISPs as a restriction of freedom of speech. *Journal of Intellectual Property Law & Practice*, *9*(2), 108-109.

Koehler, W. (2004). A longitudinal study of Web pages continued: a consideration of document persistence. *Information Research*, *9*(2).

Korenhof, P. (2014) Forgetting bits and pieces: an exploration of the "right to be forgotten" as implementation of "forgetting" in online memory processes. In *IFIP Advances in Information and Communication Technology series*, volume 0421. Springer.

MacLean, M., & Davis, B. H. (Eds.). (1998). *Time & bits: managing digital continuity*. Getty Publications.

Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton: Princeton University Press.

Rosen, J. (2012). The right to be forgotten. *Stanford law review online*, *64*, 88.

Rosenzweig, R. (2011). *Clio Wired: The future of the past in the digital age*. Columbia University Press.

Sartor, G. (2014). The right to be forgotten: dynamics of privacy and publicity. In L. Floridi (Ed.), *The protection of information and the right to privacy*. Springer.

Schmidt, E. (2013). New Digital Age, *John Murray Publishers.*

Sparrow, B., Liu, J., & Wegner, D.M. (2011). Google effects on memory: Cognitive consequences of having information at our fingertips. *Science 333.6043*, 776-778.

Szekely, I. (2012). The right to forget, the right to be forgotten; Personal reflections on the fate of personal data in the information society. In S. Gutwirth, R. Leenes, P. De Hert and Y. Poullet (Eds.), *European data protection: In good health?* (pp. 347-363). Dordrecht: Springer.

Vafopoulos, M. (2012). Being, space, and time on the web. *Metaphilosophy 43.4*, 405-425.

Weber, R. (2011). The Right to be Forgotten: More than a Pandora's Box? In *2 JIPITEC 120*, 121. Retrieved from http://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf.

Wegner, D.M. (1986). Transactive memory: A contemporary analysis of the group mind. In B. Mullen & G. R. Goethals (Eds.), *Theories of group behavior* (pp. 185-208). New York: Springer-Verlag.