Can Web 2.0 Ever Forget?

DOI 10.1007/s12599-010-0093-9

The Author

Dr. Jürgen Karla (✉)
Institute of Business Information Systems
RWTH Aachen University
Templergraben 64
52056 Aachen
Germany
karla@winfor.rwth-aachen.de

Received: 2009-10-28
Accepted: 2010-01-01
Accepted after two revisions by Prof. Dr. Sinz.
Published online: 2010-02-23

This article is also available in German in print and via http://www.wirtschaftsinformatik.de: Karla J (2010) Digitales Vergessen im Web 2.0. WIRTSCHAFTSINFORMATIK. doi: 10.1007/s11576-010-0215-5.

1 Data Protection on Web 2.0

The Internet is making rapid advances, but its comforts also go hand in hand with a growing threat to the users' privacy protection. In particular, services subsumed under the heading Web 2.0 – e.g. Social Networks or Microblogs – have aggravated this trend, and continue to pose new and increasingly large challenges for the protection of the private sphere. Risks include the misuse of personal information revealed on the Internet. Furthermore, there is a danger of personal information being misinterpreted to the detriment of the person it refers to. The central source of danger to the private sphere on the Internet emanates from the Internet's particular characteristics of being decentral and global as well as from the unlimited storage time of any information published on the Internet, coupled with the difficulty of deleting such information (Sterbik-Lamina et al. 2009, pp. 11 ff; Mayer-Schönberger 2008, p. 10). Introducing an expiry date for personal information on the Internet as an interdisciplinary approach addresses the latter aspects, integrating technical, legal, and sociological research results. The initial purpose of the expiry date is to sensitize users to the problem of the lack of protection of the private sphere on the Internet. Such an approach would mean enhancing information with the metadata "expiry date" and remove or anonymize the information after expiration.

2 Interdisciplinary Approaches for Enhancing the Protection of the Private Sphere

When examining various alternative approaches for enhancing the protection of the private sphere on the Internet, it becomes obvious that in particular interdisciplinary solutions that integrate the users are more likely to succeed. In principle, technical solutions, e.g. anonymization, and sociological approaches, e.g. digital abstinence, can be differentiated. Additionally, interdisciplinary approaches exist – including approaches that integrate the legal dimension. Both the concept of introducing property rights for personal data and the approach of introducing an expiry date for information are examples for innovative approaches; the latter is addressed in this paper.

Table 1 offers a short overview of the different approaches before dealing with the idea of introducing a solution for "digital forgetting" in the following.

3 Digital Forgetting – Expiry Date for Information

The main intention of an expiry date for information is to sensitize contributors for the lack of data protection of the private sphere on the Internet. The concept refers to user experience in daily life (e.g. expiry date for food) and the natural processes of forgetting of the human memory. Finally, the implementation of an expiry date should lead to removing or anonymizing provided information.

The act of forgetting is of core significance for every individual, but also for social and cultural interactions as we know them today (Bannon 2004, p. 6). For the human memory, the process of forgetting is a natural one on account of the human's biological condition. The act of forgetting is recurrent throughout our lives and is regarded as normal in our society. If we take a closer look, we can also see that the act of forgetting is the driving force behind many of our daily, matter-of-course actions. Therefore, it should not be seen as a kind of deficiency or weakness, but rather as a great advantage of the human mind and as a central element of our society and culture.

With the dissemination of digital media and their branching out into almost every area of our lives, data are collected everywhere and stored permanently. Nowadays, data records are not stored according to whether they are important enough to be stored, simply because every information published is stored (Zeger 2009, p. 84). The phenomenon of voluntary disclosure of personal information can be found particularly in the area of Web 2.0 services and their diffusion into the business context described by the term Enterprise 2.0 (Sterbik-Lamina et al. 2009, p. 14; Zeger 2009, p. 31).

It was on the basis of this consideration that the "privacy by design" approach originated in order to develop an expiry date for digital information (Sterbik-Lamina et al. 2009, pp. 34 ff). It is intended to define a time limit for any information published on the Internet. When this limit is reached, the information will be automatically removed (Mayer-Schönberger 2007, p. 19). Control over one's own personal data would lie with the contributor in the case of the expiry date concept, since only the contributor is in a position to react quickly and flexibly enough to the particular circumstances on the Web 2.0. Furthermore, the storage of information, depending on what sort of information it is, requires different periods of time, and only the user who knows the information in question can sensibly decide how long it should be kept on the Internet (Reischl 2008, p. 63). In concrete terms, contributors should automatically be asked via a dialog before they save any information

Table 1 Interdisciplinary approaches

Approach	Characteristic/intention	Assessment
Digital abstinence	Abstention from the Internet; no publication of personal information	Unsuitable because using the Internet is fundamentally anchored; no self-assertion
Perfect contextualization	Enhancement of protection from misusage and misinterpretation by dissemination of personal information on a larger scale; avoidance of fragmented information	Unsuitable because a panoptic society complicates living together; surveillance pressure; Paradoxon: abolition of private sphere for its protection (Solove 2007, p. 746)
Property rights for personal information	Introduction of a privacy DRM; property rights for the user; usage of market mechanisms for allocation (Mayer-Schönberger 2008, p. 14; Lessig 2001, pp. 282 ff; Blanchette and Johnson 2002, pp. 41 f)	Technically and legally complex; regulation is limited on the Internet; leads to perfect technical surveillance

on the Internet, e.g. before they place a photo into a Social Network, how long this information should be valid for.

After reaching the desired expiration date different strategies for handling the appropriate information are conceivable. One possibility is an automatic removal from the platform (Raguse 2007). A notification function would be possible to inform the contributor that the deletion of certain information is approaching. Apart from the hard removal of information, a weaker variation offers the possibility of anonymizing personal information. That means that the original data (e.g. a picture or a discussion contribution) remains available, but, however, can no longer be assigned to a certain contributor or a certain context.

The principal intention of the expiry date implementation is not to create a perfect technical solution. Rather, the focus is on actively involving the user. Because the user is continuously confronted with the question of how long a piece of information should be stored on the Internet, he or she is actively involved in the processes. This active participation makes a user aware of how little protection for personal data actually exists on the Internet, thus raising awareness for this problem and having a sensitizing effect on the user (Mayer-Schönberger 2007, pp. 20 ff; Mayer-Schönberger 2008, p. 15). The eventual market pressure on Web 2.0 service providers to apply the expiry date principle is a desirable effect.

4 Fields of Application for an Expiry Date

Potential fields of application for an expiry date for personal information include private usage of Web 2.0 services as well as corporate usage of such services. Web 2.0 services that are of relevance in this field are also called Enterprise 2.0 (Koch and Richter 2009); these are characterized by sensitive and person-related information to a comparable extent. Imagine, for example, a colleague who no longer wants to have a failed project enlisted in his profile on the company´s own Social Network. Besides, in the context of business and information systems research (BISE) two additional research topics are being addressed: The growing amount of information on the Internet makes searching more difficult and finding relevant information takes longer. Both aspects could be mitigated by the introduction of an expiry date for information.

Today, approaches can be found to implement an expiry date in Wiki systems in the context of active knowledge management. These concentrate on automatic notification of contributors after a certain amount of time inviting them to review their contribution. The focus is primarily set on quality assurance, but could be extended to data protection.

5 Open Questions and Critical Appraisal

Apart from the advantages of expiry dates, resulting from an easy and inexpensive implementation due to the availability of necessary technologies, there are, however, some points of criticism.

- Even though the main intention of the expiry date is to sensitize the user and thus create market pressure, which would force the providers of Internet platforms to rethink their strategies, this can only be achieved if the expiry date can be used with already existing Web 2.0 services. However, this requires the support of legal regulation, in particular as the Web 2.0 platform owners will not voluntarily integrate an expiry date into their platforms (Raguse 2007).
- From a psychological perspective, a point of criticism is that the expiry date offers the option to delete any contribution at will, which itself is counterproductive, since it further lowers the user's inhibition threshold as to publishing personal data on the Internet (Mayer-Schönberger 2007, p. 22; Bannon 2004, pp. 10 ff).
- The implementation of a notification function could result in an enormous amount of messages for heavy users. These might be unable to manage them.
- A further criticism is the issue of the suitability of metadata for technically implementing the expiry date. On account of their function of providing supplementary information for documents, of being accessible to anyone, and not being coded or hidden, metadata can easily be manipulated or bypassed. Furthermore, material which is published on the Internet can be copied, and it is not possible to guarantee that the expiry date embedded in the metadata of the original document will be adhered to. These copies can be published – besides the local storing – in any form on the Internet, without the originally included meta-information on the expiry date having to be taken into consideration. There is of course also the omnipresent possibility of making a screen copy, which completely ignores the metadata.
- Information generated by third parties also poses a problem, since there is no possibility to supervise the implementation of an expiry date.
- Furthermore it must be ensured that, in those areas where Internet-based

contracts are concluded, the relevant contractual information – in which the participants have a legitimate interest – remains available in the future and is not subject to an expiry date. The same applies for legally binding information provided on Internet sites.

6 Future Research Approaches

At this point, it must be pointed out that the original intention of sensitizing contributors towards the expiry date can, in principal, be achieved independently of the problems of manipulation and circumvention of a technical solution. However, there is a danger that a regulation which, as a result of a lack of enforcement or of its function, proves to be practically useless, will be rejected by most users.

Further research can be expected to focus on the integration of existing concepts and methods, e.g. approaches from Digital Rights Management (DRM) or Enterprise Privacy Authorization Language (EPAL) (Ashley et al. 2003), which will be described shortly in the following.

EPAL is a formalized language developed by IBM to enforce the protection of personal data within and between companies. In order to ensure interoperability, EPAL is based on the standardized mark-up language XML. It is EPAL's objective to formalize data protection regulations for the use of personal data so that they are computer readable and can thus be implemented in an automated manner. Every piece of personal information has additional data added to it which regulate user rights. EPAL defines data protection categories, user categories, purposes, groups of actions, obligations, and conditions. With their help, rules can be established which allow or deny the processing of information e.g. depending on date, user, and purpose. EPAL is regarded to be complementary to the P3P standard (Platform for Privacy Preferences), which has already been standardized by the W3C and enables companies to communicate data protection regulations to third parties. EPAL can offset the P3P's deficit of not being able to ensure the enforcement of the communicated data protection policy. EPAL, then, represents the back-end for data protection and P3P the front-end for the user. Therefore, the integration of an expiry date into the data protection regulations enables a processes of forgetting in Web 2.0/Enterprise 2.0. Besides P3P especially PRIME (Privacy and Identity Management for Europe, https://www.prime-project.eu/) and PAW (Policy Aware Web, http://www.policyawareweb.org) should be named as recent further research projects.

The increasing frequency of problems regarding an illegal access to huge amounts of user-generated data from Web 2.0 services generates expectations that users will develop a rising awareness for the topic. Especially in the context of interdisciplinary research further advancement can be expected. For example, as part of the project "Young Scholars' Network on Privacy and Web 2.0", promoted by the DFG, a comprehensive investigation of aspects of data protection in Web 2.0 will be undertaken. Preliminary research showed that possible effects of the constant availability of private information on the Internet is, so far, to a large extent unexplored in the sense of habitualization and socialization effects. The research results to be expected here might deliver input also for further research in the field of BISE.

References

Ashley P, Hada S, Karjoth G, Powers C, Schunter M (2003) Enterprise privacy authorization language (EPAL 1.2). http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/. Accessed 2009-11-26

Bannon LJ (2004) Forgetting as "A feature not a bug" – the duality of memory and implications for ubiquitous computing. CoDesign International Journal of CoCreation in Design and the Arts 2(1):3–15

Blanchette J-F, Johnson DG (2002) Data retention and the panoptic society: the social benefits of forgetfulness. The Information Society 18(1):33–45

Koch M, Richter A (2009) Kollegen im Netz. Wirtschaftsinformatik & Management 1(1):59–63

Lessig L (2001) Code und andere Gesetze des Cyberspace. Berlin-Verlag, Berlin

Mayer-Schönberger V (2007) Useful void – the art of forgetting in the age of ubiquitous computing. http://www.vmsweb.net/attachments/pdf/Useful_Void.pdf. Accessed 2009-07-25

Mayer-Schönberger V (2008) Nützliches Vergessen. In: Reiter M, Wittmann-Tiwald M (eds) Goodbye Privacy – Grundrechte in der digitalen Welt. Linde, Wien, pp 9–15

Raguse M (2007) Verfallsdatum für Daten im Internet – Regulierung gefordert. http://www.datenschutz.de/news/detail/?nid=2382. Accessed 2009-06-05

Reischl G (2008) Die Google-Falle – Die unkontrollierte Weltmacht im Internet. Ueberreuter, Wien

Solove DJ (2007) "I've got nothing to hide" and other misunderstandings of privacy. San Diego Law Review 44:745–772

Sterbik-Lamina J, Peissl W, Cas J (2009) Privatsphäre 2.0 – Beeinträchtigung der Privatsphäre in Österreich. http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a53.pdf. Accessed 2009-11-26

Zeger HG (2009) Paralleluniversum Web 2.0 – Wie Online-Netzwerke unsere Gesellschaft verändern. Kremayr & Scheriau, Wien