The "Transparent Citizen" in Web 2.0

Challenges of the "Virtual Striptease"

DOI 10.1007/s12599-010-0113-9

The Authors

Prof. Dr. Hans Ulrich Buhl (✉)
FIM Research Center Finance & Information Management
University of Augsburg
Universitätsstraße 12
86159 Augsburg
Germany
hans-ulrich.buhl@wiwi.uni-augsburg.de

Prof. Dr. Günter Müller
Institute of Computer Science and Social Studies
University of Freiburg
Friedrichstraße 50
79098 Freiburg
Germany
mueller@iig.uni-freiburg.de

Published online: 2010-06-24

This article is also available in German in print and via http://www.wirtschaftsinformatik.de: Buhl H.U., Müller G. (2010) Der „gläserne Bürger" im Web 2.0. Herausforderungen des „virtuellen Striptease". WIRTSCHAFTSINFORMATIK. doi: 10.1007/s11576-010-0230-6.

The wave of indignation at the threat of a "security peepshow" was great when at the beginning of this year the discussion on upgrading airports with body scanners came up again. In many cases, such a commanded exposure was considered to be an unacceptable violation of human dignity. Drawing the attention away from the real to the virtual world, the U.S. market researcher Hitwise reported in March 2010, at the time when this editorial was written, that – in terms of the number of visits – the online social network Facebook had replaced the search engine giant Google as the most-visited U.S. website. Isn't it remarkable that the majority of our society refuses body scanners, but cannot resist the daily temptation of the common "virtual striptease" in today's "participatory Web"? Here, people (more or less) voluntarily provide more information about themselves than a body scanner could ever "expose". A particular temptation (and risk) emerges from the simplicity and attractiveness of the business models used for current Web 2.0 applications, such as online social networks and weblogs: For the provision of personal data users "buy" the supposedly free access to attractive Internet services. The perfidy of this is that most users are not even aware of this "payment process" and the potential negative consequences.

Some examples may illustrate the issue: The Web 2.0 application Blippy (http://www.blippy.com) is one of many services that are based on the voluntary "virtual striptease". By providing the credit card number and/or the access data to online stores, such as Amazon or Ebay, the service is able to assign all procurement transactions (including relevant details) to the respective user profile. Similar to the Twitter principle we can see what friends and acquaintances spend their money on, and each transaction may – as is typical for the "participatory Web" – be commented on by other users. Other Web 2.0 applications that are currently gaining popularity provide even deeper insights into the activities and the social environment of a user by connecting real and virtual world on the basis of spatial data. Thus, e.g., Foursquare (http://www.foursquare.com) makes use of GPS data to offer a hybrid service to the rapidly growing number of smartphone users which consists of a "friends radar", a local referral service, a virtual game, and a platform for location-based advertising. However, the risk that may result from such a "playful" combination of virtual and real world can be illustrated by Google's latest Web 2.0 application named "Google Buzz" (http://www.google.com/buzz). With Buzz, Google not only offers real time social networking to its more than 140 million Gmail users, but also integrates the functionality of an e-mail program, Twitter service, photo album, video platform, and a news reader among other things. The interesting feature during the launch was the automatic creation of so-called friends lists on the basis of existing Gmail contacts. These "friends" automatically gained insights into the user's private life (including private e-mail contacts) without prior approval by the Buzz member in question. In addition, they could see the user´s blog entries, Twitter messages ("tweets"), and status messages that were mostly published using a pseudonym via a "ticker". Apparently very helpful and practical at first sight – as there was no annoying search for friends and confirmation of contact inquiries –, this could however have far-reaching negative consequences. The case of a young American woman may illustrate the issue. After she was successfully divorced from her violent husband, had obliterated all her traces in real life, and started using a pseudonym on the Internet which suggested anonymity, the identification algorithm in Buzz still classified her former husband as a "friend" based on the regular contact in the past and showed him the new residence and the employer of his former wife as well as current blog entries. Although the Buzz function was revised immediately as a result of this scandal, this prominent example should not be trivialized as an individual case. It is only one among many others, illustrating that the careless disclosure of personal data in the Web might become a stumbling block not only in private life but also for one's professional career.

In addition, new technological developments, such as the automated matching of digital images, which is still being tested, and applications building upon that service, open up more and more unexpected and potentially unpleasant search opportunities. Thus, for example, the identification of strangers via mobile phones seems to be within reach. By linking and enriching this feature with a lot of information from other Web 2.0 applications, strangers would be able to find out more about us in a split second than a body scanner could ever reveal.

Here at the latest, one must ask whether the long-term consequences of generously providing personal data on the one hand and the rapid technological progress in Web 2.0 on the other hand are at all foreseeable for us and our daily lives. For instance, the insurance industry is discussing the issue of charging an additional premium for the users of corresponding Web 2.0 applications who (in-)voluntarily publish their current residence or of rejecting future insurance claims because the insured's duty of care is not fulfilled.

At any rate, the above examples disclose the following: While the almost exponentially growing number of users of especially location-based Web 2.0 applications indicate the (at least temporary) individual benefit, the users neglect the fact that they leave a trace of "digital breadcrumbs", just like Hansel and Gretel did in the fairy tale, which may exist forever and which may be linked with other historical traces almost in real time. In the fairy tale, the breadcrumbs were eaten by birds – in Web 2.0 this will definitely not be the case. Incidents like that of the young American woman exemplify the consequences which the violation of privacy and the linkage of data from different sources may incur.

Therefore, the interesting questions from today's perspective are: What other general trends are identifiable beyond the above mentioned examples? What risks and challenges result from these issues for individuals, companies, and society?

These questions are particularly important as the current developments in Web 2.0 are only a small – albeit important – step towards a digital identification. Thus, in the course of the increasing informatization of the real world, e.g., by RFID and Ubiquitous Computing, by new software applications like "Google Goggles" (http://www.google.com/mobile/goggles) or the controversial "Google Streetview" (http://maps.google.com/help/maps/streetview) huge amounts of data are already stored. Although informatization and networking are assigned a crucial role in solving fundamental problems of future mankind (resource scarcity, climate change, demographic change, uncontrolled migration, traffic gridlock, terrorism, etc.), further sensitive data, the use of which most often cannot be controlled or influenced by us, end up in the hands of a few Internet giants. In future, therefore, in addition to our phone calls, credit cards, e-mail and Internet accounts, even clothing and any kind of ticket will gather information about us.

The implications of the heavily discussed topic of "cloud computing" will be addressed here only briefly: "Cloud computing" and the service orientation seem to develop into new concepts for a global and standardized offer. "Computing on demand" in combination with the potential of new services and service composition reduces – at least in theory – the basic cost of IT to a previously unimaginable degree. For instance, Google already offers e-mail accounts and massive storage capacities for data, videos, and graphics for € 30 per month; an offer even computer centers cannot provide today. Here companies, however, are (still) hesitant as complex applications such as business process systems are not transferable to the extent that organizations would trust a "cloud". The respective importance of the protection of our privacy the associated storage of personal data on virtual giant computers that are operated by private service providers may take the "virtual striptease" to new unimaginable spheres.

One thing becomes clear: By bundling the numerous digital traces we leave in the on- and offline world as time goes by, an ever finer and more detailed mosaic of our real existence results, which turns George Orwell's surveillance fiction "1984" into reality – but in a different way than he imagined.

The actual problem is not the "transparent citizen", who is at the mercy of the "surveillance state", but rather the fact that no state of the world can protect us against the threat of anarchy in the Web. Already the largest data collectors such as Google, Facebook, Microsoft, and many more seem to monitor everything – and yet there still is no really identifiable guardian. While at the time of population census it was the government in this country against which people could successfully defend themselves,

we are now rather dependent on how the Internet giants conceive their responsibilities. Although these declare to be solely interested in the collectivity of user traces (in particular for the identification of trends, tendencies, and patterns), and thus not to be interested in individual data, this may change quickly in the future – especially if it may open up new revenue sources. Of course, we could at this point draw the conclusion that the simplest solution for the protection of individual rights lies in the hands of every individual him- or herself: After all, it appears to be our decision whether we use such Web 2.0 applications and publish personal data in the network. However, this would be too short-sighted. On the one hand, personal data (especially images) are published in the Web indirectly through the "exhibitionism" of other people. Even the search for these data in the network's depths turns out to be a time-consuming and almost hopeless "cat-and-mouse game", not to mention the subsequent deletion of the tracks found. In this context, the German Stiftung Warentest, after conducting a study of the major online social networks, reported that abuses through "faked profiles" have not been satisfactorily resolved by the providers despite insistent pleas of the aggrieved person. Instead, the "petitioners" received standardized e-mails that had nothing to do with their initial request. Furthermore, the providers responded similarly to the request to release the data that was stored about the user's behavior in the OSN, although German providers are bound by law to do so. Whoever, on the other hand, rejects the current developments takes the risk of not tapping the full potentials and to some extent takes leave of an increasingly important part of our society.

Regarding the effect of the increasing generosity with data and networking for companies, in addition to the praised potentials (including the provision of new knowledge pools by staff members involved in social networks, absorption of innovation potential through the integration of customer knowledge into the value chain) also challenges emerge, as many incidents of data theft and abuse as well as incidents of Internet crime illustrate. This antagonism is also subsumed under the term "de-perimeterization". Thus, the usage of both mobile devices and different storage media breaks up the original security boundaries of the corporate IT network, and a balancing act between safety and mobility has to be accomplished. In addition to this challenge, however, companies in recent times face an increased risk through potential defamation resulting from the network. Whereas the flow of information can be controlled directly in corporate or business related Web 2.0 applications, especially the loss of image resulting from a dissemination of (intentionally) distributed negative information in "non-influenceable" applications is generally unpreventable as any commentary enhances the negative message and may even make it more widely known. The possibility of creating anonymous posts not only lowers the inhibition threshold, but also makes it difficult to trace back "cyber bullying", which is also increasing in the private sector and at universities.

Against this backdrop, the decision of the German Federal Constitutional Court in March this year, declaring the previously valid regulation on the retention of data to be unconstitutional and allowing the usage only under very strict conditions, is double edged: On the one hand, the court's decision reduces the (maybe less probable) risk of having an Orwellian surveillance state for citizens and companies. On the other hand, it at the same time increases the probably higher risk of a criminal use of anonymity: by prohibiting the retention of traffic data from telephone, mail, and Internet, a government protection in the Internet by means of retracing is virtually impossible.

Thus, there is an immense social challenge to ward off internal and external threats and at the same time not to endanger the further development of an open society structure. Here, the role of IT is also double-edged: on the one hand, new services are an essential coordination technology in almost every conceivable economic, political, and social context (energy and water supply, production, finance, health, transport, education, e-voting, etc.). These services, however, also threaten – as shown – the social security. On the other hand, IT is also an important "enabler" of social security in terms of the identification and prevention of internal and external threats. It is therefore essential that everyone – whether it is on individual, company, or state level – becomes aware of the foreseeable impact on their area of responsibility: it is vital to develop strategies to reduce the risks discussed without destroying the inherent opportunities through a blind minimization of risks.

What measures should be taken, therefore, to meet the outlined challenges?

- There is a wide social consensus regarding the fact that the basic personal rights and civil liberties of individuals should not be discarded due to the exponentially increasing data traffic of ubiquitous information processing. This is and remains a

fundamental principle, even if the sometimes very extensive provision of personal data is voluntary and people are partly right in sneering at the Data Protection Act as it regulates technology of 30 years ago. At this point, a general social rethinking is necessary which requires not only each individual user, but also the government to keep abreast of the new developments in Web 2.0 technology. It is essential that – next to a discourse on the current challenges and in particular about how data protection and privacy is defined in the age of Web 2.0 – people do not rely on the fact that providers of Web 2.0 applications are aware of their responsibilities and act accordingly. Instead, providers should be requested – in an internationally coordinated way – to take direct action to protect the privacy of their users. Default settings for the use of data during registration to ensure, for example, that newly created profiles are visible only for the users themselves at first, might be an exemplary suggestion. The modification of the automatic transfer of all copyrights to use data only with the expressed consent of the user is another issue for which – as long as no alternative is agreed upon – the principle must apply that the users retain ownership of their data.

- Even if the rapid speed of technological development in Web 2.0 and the enormous complexity of the issue lead to the fact that usually aberrations are detected very late, often too late, we must ensure that the users of these Web 2.0 applications – especially young people – become aware of embedded risks. This is important as the users' carelessness regarding their personal data may involve unpleasant consequences even years later since the Internet does not forget and there unfortunately are no birds that eat up our "digital breadcrumbs". We must ensure that even schools and universities impart fundamental media literacy for the wise and responsible use of the WWW in general and Web 2.0 services in particular. Moreover, the companies behind these applications are requested to make a significant contribution by at least sufficiently elucidating the general risks of new applications prior to registration.

Besides these aspects, in particular the interdisciplinary field of Business and Information Systems Engineering (BISE) is obligated to answer current and future questions in terms of the heavily discussed issue of "security" in the context of "de-perimeterization". From an information technology based point of view, this in particular includes the effective prevention and control as well as the reduction of weaknesses in order to ensure compliance with the objectives of availability, integrity, and confidentiality of information systems. In addition, from today's perspective further challenging changes are emerging. Thus, the so-called "five E" (Economy, Employment, Energy, Elderly Society, Education), which can be offered more economically and to a greater number of consumers as a result of the cost reduction of IT, are being increasingly placed into the center of attention as a priority area of life for the use of new IT services. In Germany, these "five E" will in future be extended by both the issue of health and – transversely to the functional perspective – by the growing digital identification of the individual and the control of services that are used by an individual in a future society. Job card, health record, and digital identity card together with the proposed system ELENA – with which the German government has already collected sensitive data from more than 40 million employees since the beginning of the year – only represent first precursors of this development. In which way similar developments influence our society can be illustrated by an example from Japan. There, the phone number has become a crucial identification feature of an individual as a result of the almost exclusive use of the mobile phone for almost all areas of life (e.g., for shopping, partner search, communication with employers, etc.). The scope that is offered by the combination of such a legitimation – even for criminal transaction – and the evidence that this number is used by one person over a longer period is enormous.

Not least this example illustrates that the transformation of the public, private and economic environment which accompanies the discussion on "upgrading" through information technology and the related effects on the behavior and interaction of human individuals and business entities, are and will be important tasks, in particular for BISE.

Hans Ulrich Buhl
Günter Müller