Collaboration and the Knowledge Economy: Issues, Applications, Case Studies
Paul Cunningham and Miriam Cunningham (Eds)
IOS Press, 2008 Amsterdam
ISBN 978–1–58603–924-0

When Little Brother is Watching You It Is Time to Ask: Who Has the Right to Mediate Personal Data?

John Sören PETTERSSON
Centre for HumanIT, Karlstad University, Karlstad, 651 88, Sweden
Tel: +46 54 700 2553, Fax: + 46 54 700 1446, Email: john_soren.pettersson@kau.se

Abstract: The focus of this presentation is on the commercialisation of various register data exemplified by some cases of mass distribution of personal data in Sweden. Even if many people use such web services, other people find faults with them. The critics want to restrict data dissemination but this is hard when there are data aggregators such as credit-ranking institutes benefiting from mediating personal data. This paper proposes that the mediating could be done by the subject as there is means to let the data be supplemented by proofs of the authentic origin in banks, tax registers, etc., of the data. By this mode of operation, every (computerised) citizen would be informed about the data basis for decisions that concerns them and is thereby in a better position to augment data giving a misleading picture.

1. Introduction

Interests in personal data about neighbours, friends, or famous people seem to be quite wide-spread, to judge from facts revealed during a debate in Sweden last year. When certain web sites started to publish personal data about every citizen these sites attracted a lot of attention. What ordinary gossip columnists writing their chronicles of scandal in colourful magazines cannot provide is this personalised service, which gives civil status and economic reports about exactly the individuals that each reader likes to hear about. So much better then that some web publishers feel the responsibility to offer such services… Well, in fact, it is not good that personal data is easily available in this manner as it is a clear threat to everyone's privacy. The focus of this presentation is on the commercialisation of various register data exemplified by some cases of mass distribution of personal data in Sweden.

The paper raises the question how to remedy these cases. It is proposed that the EU Directive's 'right of access' to personal data by the data subject should be replaced by an exclusive 'right to mediate' granted to the e-citizen.

2. Objectives

This paper aims to discuss how citizens (in particular, Internet users) can be empowered to control personal data about themselves. The discussion is based on an account of how sensitive economical data has been made available for free or for small fees by web sites. The incentives for the data providers have been to sell advertisement space. In the concluding section, a proposal based on the individual data subject as a mediator is suggested as a solution to the problem of mass distribution of personal data in electronic form.

3. Personal Data Mediated by Commercial Web Services

3.1 Some Swedish Cases

A couple of years ago, certain credit-rating agencies in Sweden began exploiting the act of the freedom of press to make sensitive information available on websites. Credit-ranking information is normally electronically accessible only by employers and credit institutes, but now websites were registered with named persons as publisher – this is enough to be covered by the laws on freedom of the press and freedom of speech (the latter law covers registered radio stations, etc., nowadays including Internet-based publishers). Such web sites can publish anything and this fact was used to publish information usually used for credit ranking on individual citizens. Such requests should normally be followed by information to the one concerned (i.e., the 'data subject' in legal texts).

In spring 2006 there was a debate in Sweden about this as the web services took only a small fee from their customers, which made many people signing up for such services. Newspapers published articles on this fact, and although many citizens were shocked, the debate made more people aware of these services and possibly spurred the use of these services. Also the national data protection authority and foreign news media commented on the matter (see, e.g., [1] and [2]). The Orwellian 'Big Brother Is Watching You' had turned into a threat from Little Brother – your friends, foes, neighbours, colleagues, employees, old partners and prospective ones could make a check of your economic status. During the following year there were three important developments:

- In November 2006, there was a service (ratsit.se) providing the data for free attracting lots of people and selling advertisement slots on its web pages.
- In March 2007, the National Tax Board declared its intention to deliver information only in printed form and not electronically to credit information agencies which passed information on to websites. (There were further issues: ratsit.se did not register as a publisher until March so the legality of its data dissemination activities between November and March was in doubt. This aspect will not be discussed here.)
- From June 11, 2007, there is an agreement within the credit-rating branch. When individuals order information, a copy will be sent to the one concerned including data about who made the request, while a company may inquire without any copy being sent.

The June-11 agreement contains a further restriction that for a request from an individual "a legitimate need must exist". Companies could be thought of having a legitimate reason, such as checking job applicants or customers placing large orders or landlords checking prospective tenants. At least in older 'paper-based' times it would be expensive for company managers to misuse the possibility to check individuals, and for many years only larger companies had electronic access to credit-ranking data.

One might think that this agreement should stifle data supervision by 'little brothers'. Who could have a legitimate reason to get credit-ranking data for his/her neighbour or boss? Furthermore, the demand that a copy is sent to the data subject also brings with it costs, so it is difficult to have gratis services any longer. One euro per data request must be charged to cover postage and the paper-based process of sending a copy (the copy has to be in print as there are not legally valid e-mail addresses for people in general; only physical addresses can be used). One may moreover note that if customers of these web services have to pay, they will be identified by their physical address (invoice) or credit card numbers. Thus, the information about who requested the data will be certified in an implicit manner (at least in most cases).

In principle, this should be the end of unwarrantable supervision by hundreds of thousand little brothers (by the time of the agreement, ratsit.se claimed to have more than 600.000 registered customers and that more than 14 million inquires had been done;

Sweden has 9 million citizens). But this is only 'in principle' as shown by the following two points concerning the site upplysning.se:

- Testing upplysning.se there were no requests for information about the need for the data requested, but later the paper copy to the person being investigated contained a sentence "If you have questions about why John Sören Pettersson has taken this information about you, you can turn directly to him at the address [Pettersson's address]."
- For the limitation that only a company may inquire without copies being sent out, the only check is that the company is registered at the address given. Many persons have their own registered companies and the limitation of anonymity to only companies does not seem to be an important restriction.

As a commentary to the second bullet, it can be noted that, upplysning.se seems really keen to point out that for registered companies nothing has really changed and one will still be totally anonymous. In an e-mail message sent out about a week before the agreement would be effective, they noted this, ending with: "no copy will be sent out and one will be fully anonymous!" (Sic, the clause ends with an exclamation mark!) This e-mail message was sent to all registered customers, not only company customers. Also ratsit.se makes it very clear that companies can inquire without any copy being sent.

The ease with which companies nowadays are registered makes the differentiation between companies and persons questionable when the issue is who gets information. To round off the discussion, we can note that ratsit.se tried to keep to their gratis branding by still offering information about companies free of charge because still no copy needs to be sent if it is a company that is the object of an inquiry. This kind of differentiation between companies and physical persons should be uncontroversial because a company is an economical entity first and foremost.

3.2 Incentives to serve Little Brother

In [3] we speak about 'webification' of data processing. A particular feature of the webification is not only the easy access people have, but also the ease with which new distribution spots, i.e. web servers, are set up, registered, etc. It is also easy to set up the economical infrastructure needed to motivate the web site owner to at all bother for publishing data about individuals. Solutions for credit card payment, or other electronic payments nowadays available (e.g., paynova), are easily installed. Also the other major economic source, advertisement, has found easily implementable forms, both technically speaking and economically. For the business perspective, it is noteworthy that organisations interested in advertising have an efficient means of doing cost-benefit analysis: they do not have to pay for the advertisement itself but for each view of it or click on it. This makes it safe to invest in advertisements – the organisation only pays if the web ad has some effect. There are marketing companies such as Google selling advertisement slots on a huge variety of web sites – the organisation only has to tell what types of site should host its advertisement and then the ads are put at the relevant web sites more or less automatically.

As pointed out in [3], the webification concerns more than databases with personal data. The webification of payment and advertisement infrastructures makes these means for income available to everyone – it is easy to set up a 'professional' hobby site. Google's way of handling adverts has been accused for stimulating the setting up of empty web sites with domain names that look like popular web sites' addresses to fish for users who misspell addresses [4]. Advertisements on these sites will inevitably be clicked resulting in a small revenue for the site owner. We will not deal with this issue here. Rather, we wish to highlight the kind of advertisement-driven sites that try to attract visitors by providing a real but improper content. A single person could set up a site for the dissemination of personal data and hope the adverts will generate a positive return on the (minimal) investment without charging the users anything, at least if personal data is easily accessible

electronically. An example of this was a recent site, tubo.se, which tried to fill the vacuum left when the credit-ranking information sites no longer can provide information totally free of charge. Tubo made available all salaries in public organisations, because this information is publicly available as are all other official records of public organisations in Sweden. The web site claimed a serious goal, namely to analyse salary differentials revealing, e.g., gender discrimination. However, what stroke the eye when entering the site was, besides the adverts, the Search box where the user immediately and conveniently can type in a name of a person and in a drop-down list select the organisation the person works for and the salary would promptly appear together with some other data. Now, this limited service was perhaps not too successful as in spring 2008 it was shutting down after six months.

3.3 And Finally: the Privacy of Users of the Web Services

To the problems for the data subjects that low-fee, public available databases entail, there is another privacy problem looming in the shadow, namely the customer registers of the web services selling personal data. Who would admit that he has done a hundred searches covering friends, neighbours, colleagues, ex-girlfriends, etc.? Considering the way credit card numbers and other things are available on the black markets of Internet, it would not be surprising to find web servers offering searches in stolen customer registers. That the inclusion in such registers really is sensitive has been proven in the Swedish case – there have been disputes between some customers and services on the fee charged, but such victims do not want to be identified in news media with their names [3].

4. Put More Technology to Work!

The problems for individuals' privacy have been demonstrated in the preceding section. The present section takes a positive stance to the development of data processing in our digitally connected society, but argues for even more technology, namely data processing based on electronic certificates to enhance transparency and privacy. The arguments come from development work conducted within a large EU project (see e.g. [5, 6]) but in particular from a visionary pilot study conducted 2007 ([7, 3]).[i]

4.1 Checking Information About Oneself

It is easy to be critical to the existence of web sites providing personal data. In the same time it should be acknowledged that there are positive sides of the free flow of information allowed in the Swedish example: any data subject can very quickly check what information about him is available to employers, landlords, and prospective partners. In [3] we noted also for the American site Intelius.com selling information on court cases and address history on individuals[ii], that in addition to the questionable state of affairs, that the person being searched does not know he is investigated, people might even get the wrong information about him by mistaking one John Smith for another one; in Sweden such mistakes are less probable as all personal data handling is based on the unique 'personal number' given to every citizen and person in the census register. But just as in the Swedish cases, any American data subject can very quickly check what information about him (and his namesakes) is available to employers, landlords, and others, by paying the 8 to 50 dollars that Intelius wants to have for information about individuals.

What would happen if this possibility is not available? One can compare with the citizens' questions put to the German data protection authority ULD (see [8] with data from the Datenschutz Schleswig-Holstein). A question such as the following could presumably be answered very quickly by the individual himself had he lived in Sweden: "The telco provider told me that they won't offer me a mobile phone contract. What may be the reason for that?" It is likely that the German telephone company screened applicants based on credit-rating data and then found that this individual had a bad ranking. If this person could

have checked what economic data about him is available, he would most probably have found the answer to his question. What is more, he might even be able to explain his present situation better to the telephone company than what these data do lagging a year or so behind as they often do.

4.2 Legal Support Not Enough

So, when taking the data subject's interest in getting to know what information about him or her is available to companies, these web services seem to provide a really useful service. One may object, though, that such checking on oneself should be available anyhow without allowing neighbours and other people to look on one's data. In Europe, the EU Directive 95/46/EC and its implementation in national laws grant this 'right of access' to information on data concerning oneself. The possibility to identify oneself by electronic identity cards now exists and should give swift web access to relevant data.[iii] However, there are two reasons for why this legal support is not enough.

First, as noted in [13], the formulation found in the EU Directive is not appropriate in our digitally connected era: there is room for each member state to set restriction as to how often such inquires can be forced upon the data controllers. Traditionally, there is an economic burden connected to the processing of such requests as they have to be answered in the paper medium. In Sweden, e.g., a data controller can limit the free access to data to once per annum, which may leave the citizen with too old information if he has already accessed his information less than a year ago. In a world with e-IDs such restrictions should not exist (in Germany, this restriction was removed before electronic ID cards [13]).

Second, to really evaluate the contribution from sites such as Intelius.com and upplysning.se one important aspect has to be added: The essence of what these sites do (or the companies delivering data to them) is to collect data from different sources which makes it much easier for the inquirer to get a relevant picture of a certain individual or firm. Thus, a really useful function for checking data about oneself cannot solely be based on e-IDs. There is a need for assistance functions aiding the user to the right compilation of requests, in the same way as Hansen et al. [5] describe assistance functions for ordinary Internet users for exercising their legal rights to access and correct personal data (cf. [7]).

A 'right of access' is a good thing, but there must be guidance how to access relevant data. That is, there must be organisations well informed of what credit-ranking institutes deliver to their customers and these organisations must make this information public (and preferably machine-readable in order to let users' computer systems process it automatically) so that the user will make the right combination of requests. The same would hold for other strands of life, such as what prospective employers look for.

4.3 Extension of the 'Right of Access' to an Exclusive 'Right to Mediate'

It has just been noted that the possibility to identify oneself by electronic identity cards now exists and could potentially give swift web access to relevant data. One can add that it should also ensure unique access by the one concerned, blocking other citizens from watching his or her data. We will round off the discussion of composition of data requests by elaborating the idea of unique access by the data subject.

It should not be controversial to force 'normal' users of credit data (organisations of all kinds) to ask the data subject before data is released. The release could in fact be done by the subject him/herself because there are means to let the data be supplemented by proofs of the authentic origin in banks, tax registers, court records, etc., of the data.[iv] If the individual does not release data, he will not get the loan, employment, apartment he wants. (A non-user, i.e. a citizen without digital equipment, would then have to ask to get the information in paper or give consent already at the time of application, which often is the case when one subscribe to certain services.) Such an order of things would allow customers of credit-

ranking agencies to go directly to the individual which would potentially restructure the whole business of credit-ranking. There would not be any need for agencies amassing data about people outside the sources for such information. And the many Little Brothers of our modern society would not be so easily served; by law, it could even be mandatory to request each individual's consent for electronic release of data as there would be little need for any such processing that is not actively supported by the individual in question.

Naturally, there still has to be some open records for such things as the property register. But for other things, such as court and tax registers, it is time to demand a return to solely paper-based routines for all inquires that are not made by the one concerned.

This prospect for very transparent data transfers would need further refinement regarding the citizen's ability to consent to data requests. A person who is really keen on an apartment or for an object that is subject to instalment purchase, or a person in need of a loan, may be prone to agree to excessive data requests from the other party. The assistance functions "aiding the user to the right compilation of requests" mentioned in 4.2, should warn the user against data requests that are excessive in relation to the purpose of the request. Many people would probably allow excessive data requests in certain situations, so some sort of cautious guidance to data collection and mediation is surely needed.

Noteworthy, the assistive system on people's computers could in fact also inform the data protection authorities and consumer organisations about breeches against good standards for credit ranking of individuals. This could be done in anonymous formats if the individual thinks his case is sensitive. This use of the assistance functions will in general make it easier to develop useful market standards and to follow up liability issues.

5. Conclusions and Recommendations

Above, we have presented an account of the debate in Sweden spring 2006 – summer 2007 about the existence of web services selling or giving away personal data that credit-ranking agencies normally would sell only to credit-giving institutions or to certain other legal entities, such as employers. The public availability of economic data and the possibility to register web sites so that they are protected in the same way as mass media institutions are protected by the act of the freedom of press, has made it possible to present personal data to every individual who wants to take part of other people's circumstances.

We noted the inappropriateness of providing access to register data about ordinary citizens on the web but admitted that this accessibility also makes it possible for every registered person to very swiftly and cheaply get the same information about himself that various banks and companies have. Then we took the discussion further by discussing why the intermediates are needed at all. It should not be extremely controversial to force also the 'normal' users of register data to ask the data subject before data are released from the source. There are means to embed data in certificates warranting the authentic origin in banks, tax registers, court records, etc., of the data and we concluded that there would not be any need for agencies amassing data about people outside the sources for such information. The many Little Brothers of our modern society would not be served. Such an order of things would allow secondary users of register data to go to the individual concerned which would increase the transparency and also make it possible to enter corrections or additional facts by the individual himself.

Further research is needed on the question whether users will be able to act as mediators for data about themselves which would stifle data collection (and dissemination) by web sites. This is both a technical issue and a usability question. It also raises questions concerning how and by whom assistance is given because the more automatic the assistance is, the more liability issues are influenced. Naturally, it is also a question of changing business behaviour. We are confident that with the availability of new technology business processes change under the pressure of legislation and the public opinion. As for the latter,

which can drive both legislation and business change, we refer to the latest *Flash* Eurobarometer on "Data Protection in the European Union – Citizens' perceptions" where it is stated that 64% of the respondents reported a concern about whether their personal information was protected, and half of these were "very concerned" [15].

References

[1] Datainspektionen (web, 2006-05-15) Lillebror vet allt om dina skulder. ("Little brother knows all about your debts".) Press release in Swedish available at: http://www.datainspektionen.se

[2] *Süddeutsche Zeitung* (web, 2007-07-06) Datenschutz in Schweden: Einblick beim Nachbarn. By Elmar Jung. http://www.sueddeutsche.de/computer/artikel/403/122239/

[3] J.S. Pettersson. Little Brother Is Watching You – commercialisation of personal data through 'webification'. Presented at "Security of the digitized man" (Réflexions prospectives et internationales: «*La sécurité de l'individu numérisé*») the concluding colloquium of project Asphalès, Paris November 22-23, 2007. Will appear in proceedings published 2008 by CNRS with a summary in French.

[4] *Computer Sweden* (2007-11-26) Danny Aerts: "Google gräver sin egen grav". (In Swedish "Danny Aerts (i.e. the CEO of .se): 'Goggle is digging its own grave' .")

[5] M. Hansen, S. Fischer-Hübner, J.S. Pettersson, & M. Bergmann. Transparency Tools for User-Controlled Identity Management. Presented at *eChallenges e-2007*, 24-26 October 2007, The Hague. Published in: *Expanding the Knowledge Economy: Issues, Applications, Case Studies*, ed. by Cunningham & Cunningham. IOS Press, Amsterdam 2007; pp. 1360-1367.

[6] J.S Pettersson, S. Fischer-Hübner, & M. Bergmann. Outlining "Data Track": Privacy-friendly Data Maintenance for End-users. Presented at *The 15th International Conference on Information Systems Development (ISD 2006)*, Budapest, 31st August - 2nd September 2006. Published in *Advances in Information Systems Development, Volume 2*, ed. by G. Magyar, G. Knapp, W. Wojtkowski, G. Wojtkowski & J. Zupancic; Springer, 2007; pp. 215-226.

[7] J.S. Pettersson. Reports from the pilot study on privacy technology in the framework of consumer support infrastructure. Working Reports R1, R2, R3. December 2006-November 2007. Dept. of Information Systems and Centre for HumanIT, Karlstad University. http://www.humanit.org/projects.php?projekt_id=48&lang=en

[8] ULD (2006) Erhöhung des Datenschutzniveaus zugunsten der Verbraucher. Unabhängiges Landeszentrum für Datenschutz, Kiel, 201+27 pages. https://www.datenschutzzentrum.de/verbraucherdatenschutz/. [7], page R2-20, contains English sample translations by Marit Hansen, ULD.

[9] *Computer Sweden* (2007-11-30) Dödläge för e-id. (In Swedish "Deadlock for e-ID".) http://computersweden.idg.se/2.2683/1.133781

[10] *Computer Sweden* (2008-03-26) Hårt tryck på Verva att ta fram nytt e-id. (In Swedish about e-ID) http://computersweden.idg.se/2.2683/1.152277

[11] Verva (2007a) Säkert informationsutbyte och säker hantering av elektroniska handlingar. Verket för förvaltningsutveckling, 2007:13.

[12] Verva (2007b) eID 2007. Elektronisk identifieng och underskrift. Verket för förvaltningsutveckling, 2007:16.

[13] J.S. Pettersson & S. Fischer-Hübner (forthcoming) Transparency as the Key to User-controlled Processing of Personal Data. To be published in *Human IT: Technology in Social Context*, ed. by Ch. Christensen. Cambridge Scholars Press.

[14] E. Bangerter, J. Camenisch & A. Lysyanskaya. A Cryptographic Framework for the Controlled Release of Certified Data. Published in: *Security Protocols. 12th International Workshop, Cambridge, UK, April 26-28*, 2004, ed. by B. Christianson, B. Crispo, J.A. Malcolm & M. Roe. *Lecture Notes in Computer Science , Vol. 3957*, Springer Verlag 2006.

[15] *Eurobarometer 2008*, Data Protection in the European Union, Citiznes' perceptions, Analytical Report. Flash Euroarometer 225: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

[i] The EU 6th Framework project PRIME, *Privacy and Identity Management for Europe*, ran March 2004 to February 2008; project web site at www.prime-project.eu . Fundamental in the architecture elaborated in the PRIME project is the use of *network pseudonyms* to allow users to be anonymous and *digital credentials* to allow users to prove their identity or parts thereof, such as being a Swedish citizen. Other features involve aid to the users to gauge the privacy policies of service providers (that is, data handling polices) and to negotiate about policies.

The pilot study "Privacy technology in the framework of consumer support infrastructure" [7] was in part financed by the Swedish agency for innovation systems, VINNOVA, by grant no. 29644-1.

[ii] The Intelius wait page (when searching) says: "Intelius is searching billions of current utility records, court records, county records, change of address records, property records, business records, and other public and publicly available information to find what you're looking for."

[iii] Presently there is a debate in Sweden about the cumbersomeness of these solutions. The present business model underlying the agreements that public bodies are supposed to make has received sharp criticism. See articles in *Computer Sweden* [9] and [10]. Swedish agency Verva released a pilot study October 2007 [12], cf. [11]. On the other hand, in Norway, the MinSide ("MyPage", a service at http://www.norge.no/minside/) allows Norwegian citizens online access to their data stored at authorities (similar service developing in Denmark at www.borger.dk; see www.modernisering.dk/da/vision_strategi/strategi_for_digital_forvaltning/).

[iv] Some certificate-based mechanism must be used if the source of the data is not directly involved in the data release transactions. However, using traditional certificates (X.509 style) based on signature schemes such as RSA or DSA, it is not possible to select a subset of data from a certified record. For alternatives, see [14] (the present author's gratitude to Dieter Sommer, IBM Zürich, for this reference). Sending only a subset might be desired by the data subject in many mediation scenarios unless it is easy and costless to acquire a new certified record each time which in its content is limited to exactly the desired subset.