International Working Group
on Data Protection
in Telecommunications

675.36.5 4 March 2008

Report and Guidance on Privacy in Social Network Services

- ”Rome Memorandum” -

43rd meeting, 3-4 March 2008, Rome (Italy)

Report

Background

“A social network service focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others, and which necessitates the use of software. Most services are primarily web based and provide a collection of various ways for users to interact […]”[1]. Specifically, many popular sites offer means to interact with other subscribers (based on self-generates personal profiles[2]).

The advent and ever increasing popularity of social network services heralds a sea change in the way personal data of large populations of citizens all over the world become more or less publicly available. These services have become incredibly popular in the past years especially with young people. But increasingly such services are also being offered e.g. for professionals and the elderly.

The challenges posed by social network services are on the one hand yet another flavour of the fundamental changes that the introduction of the Internet in the 90s of the past century has brought with it, by – inter alia – abolishing time and space in publishing information and real-time communication, and by blurring the line between service providers (authors) on the one hand and users/consumers (readers) on the other.

At the same time, social networking services seem to be pushing at the boundaries of what societies see as a person’s individual space: Personal data about individuals become publicly (and globally) available in an unprecedented way and quantity[3], especially including huge quantities of digital pictures and videos.

With respect to privacy, one of the most fundamental challenges may be seen in the fact that most of the personal information published in social network services is being published at the initiative of the users and based on their consent. While ”traditional” privacy regulation is concerned with defining rules to protect citizens against unfair or unproportional processing of personal data by the public administration (including law enforcement and secret services), and businesses, there are only very few rules governing the publication of personal data at the initiative of private individuals, partly because this had not been a major issue in the “offline world”, and neither on the Internet before social network services came into being. Furthermore, the processing of personal data from public sources has traditionally been privileged in data protection and privacy legislation.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

At the same time, a new generation of users has arrived: The first generation that has been growing up while the Internet already existed. These "digital natives"[4] have developed their own ways of using Internet services, and of what they see to be private and what belongs to the public sphere. Furthermore they – most of them being in their teens – may be more ready to take privacy risks than the older "digital immigrants". In general, it seems that younger people are more comfortable with publishing (sometimes intimate) details of their lives on the Internet.

Legislators, Data Protection Authorities as well as social network service providers are faced with a situation that has no visible example in the past. While social network services offer a new range of opportunities for communication and real-time exchange of any kind of information, the use of such services can also lead to putting the privacy of its users (and of other citizens not even subscribed to a social network service) at risk.

Risks for Privacy and Security

The surge of social network services has only just begun. While it is possible to identify some risks associated to the provision and use of such services already now, it is very likely that we are at present only looking at the tip of the iceberg, and that new uses – and accordingly new risks – will continue to emerge in the future. Specifically, new uses for the personal data contained in user profiles will be invented by public authorities (including law enforcement and secret services[5]) and by the private sector.

The following list of risks can only represent a snapshot which may need to be revised and updated as social network services develop.

Risks associated to the use of social network services identified up to now include the following:

1. *No oblivion on the Internet:* The notion of oblivion does not exist on the Internet. Data, once published, may stay there literally forever - even when the data subject has deleted them from the "original" site, there may be copies with third parties (including archive services and the "cache" function provided by a well-known search engine provider). Additionally, some service providers refuse to speedily comply (or even to comply at all) with user requests to have data, and especially complete profiles, deleted.

2. *The misleading notion of "community":* Many service providers claim that they are bringing communication structures from the "real" world into cyberspace. A common claim is that it is safe e.g. to publish (personal) data on those platforms, as it would just resemble sharing information with friends as it used to be face-to-face. However, a closer look at some features in some services reveals that this parallel has some weaknesses, including that the notion of "friends" in cyberspace may in many cases substantially differ from the more traditional idea of friendship, and that a community may be very big[6]. If users are not openly informed about how their profile information is shared and what they can do to control how it is shared, they may by the notion of "community" as set out above be lured into thoughtlessly sharing their personal data they would not otherwise. The very name of some of these platforms (e.g. "MySpace") creates the illusion of intimacy on the web.

3. "*Free of charge" may in fact not be "for free"*, when users of many social network services in fact "pay" through secondary use of their personal profile data by the service providers, e.g. for (targeted) marketing.

4. *Traffic data collection by social network service providers*, who are technically capable of recording every single move a user makes on their site; eventually sharing of personal (traffic) data (including users' IP-addresses which can in some cases also resemble location data)

with third parties (e.g. for advertising or even targeted advertising). Note that in many jurisdictions these data will also have to be disclosed to law enforcement and/or (national) secret services upon request, including maybe also foreign entities under existing rules on international cooperation.

5. *The growing need to refinance services and to make profits may further spur the collection, processing and use of user data*, when they are the only real asset of social network providers. Social network sites are not – while the term "social" may suggest otherwise – public utilities. At the same time, Web 2.0 as a whole is "growing up", and there is a shift from start-ups sometimes run by groups of students with less financial interests to major international players entering the market. This has partially changed the rules of the game, as many of these companies noted on national stock markets are under extreme pressure from their investors to create and maximise profits. As for many providers of social networks user profile data and the number of unique users (combined with frequency of use) is the only real asset these companies have, this may create additional risks for unproportional collection, processing and use of users' personal data. Note that at present, many providers of social network services follow the concept of externalisation of privacy costs to users[7].

6. *Giving away more personal information than you think you do:* For example, photos may become universal biometric identifiers within a network and even across networks. Face recognition software has been dramatically improved over the past years, and will continue to reap even "better" results in the future. Note that once a name can be attached to a picture, this can also endanger the privacy and security of other, possibly pseudonymous or even anonymous user profiles (e.g. dating profiles, which normally have a picture and profile information, but not the real name of the data subject published). Additionally, the European Network and Information Security Agency points to an emerging technology called "content based image retrieval" (CBIR), which creates additional possibilities for locating users by matching identifying features of a location (e.g. a painting in a room, or a building depicted) to location data in a database[8]. Furthermore, "social graph" functionalities popular with many social network services do reveal data about the relationships between different users.

7. *Misuse of profile data by third parties*: This is probably the most important threat potential for personal data contained in user profiles of social network services. Depending on available privacy (default) settings and whether and how users use them, and as well on the technical security of a social network service, profile information, including pictures (which may depict the data subject, but also other people) are made available to – in the worst case – the entire user community. At the same time, very little protection exists at present against copying any kind of data from profiles, and using them for building personal profiles, and/or re-publishing them outside of the social network service[9].

   But even "normal" uses of (user) profile data uses can encroach upon users' informational self-determination and, for example, also severely limit their career prospects[10]: One example that has gained public attention is personnel managers of companies crawling user profiles of job applicants and/or employees, which seems to emerge as a steady feature: According to press reports, already today one third of human resources managers admit to use data from social network services for their work, e.g. to verify and/or complete data of job applicants[11]. Law enforcement agencies and secret services (including from less democratic countries with low privacy standards) are other entities likely to capitalise on these sources[12]. In addition, some social network service providers make available user data to third parties via application programming interfaces, which are then under control of these third parties[13].

8. *The Working Group is especially concerned about* further increased risks of identity theft fostered by the wide availability of personal data in user profiles[14], and by possible hijacking of profiles by unauthorised third parties.

9. *Use of a notoriously insecure infrastructure:* Much has been written over the (lack of) security of information systems and networks, including web services. Recent incidents include well-known service providers like Facebook[15], flickr[16], MySpace[17], Orkut[18] and the German provider "StudiVZ"[19]. While service providers have taken measures to strengthen the security of their systems, there is still room for improvement. At the same time, it is likely that new security leaks will keep emerging in the future, and is unlikely that 100% security will ever be realised at all given the complexity of software applications at all levels of Internet services[20].

10. *Existing unsolved security problems of Internet services* add to risk of using social network services and may also in some cases raise the level of risk, or develop "flavours" specific to social network services. A recent position paper by the European Network and Information Security Agency (ENISA) inter alia lists SPAM, cross site scripting, viruses and worms, spear-phishing and social network-specific phishing, infiltration of networks, profile-squatting and reputation slander through ID theft, stalking, bullying, and corporate espionage (i.e. social engineering attacks using social network services)[21]. According to ENISA, "social network aggregators" pose an additional security threat[22].

11. *The introduction of interoperability standards and application programming interfaces* (API; e.g. "open social" introduced by Google in November 2007) to make different social network services technically interoperable entails additional new risks: They allow for automatic evaluation of all social networks websites implementing this standard. The API delivers literally the entire functionality for automatic evaluation implemented in the web interface. Possible applications with potential repercussions on user privacy (and possibly also on the privacy of non-users whose data are part of a user profile) may include: Global analysis of (professional and private) user relationships, which may well cross "borders" between different networks where user act in different roles (e.g. professionally oriented vs. more leisure-oriented networks). Interoperability may also further foster download and third-party re-use of profile information and photos, and creation of profiles about change histories of user profiles (including making available of information a user has deleted from his profile).

Guidance

Based on the above said, the Working Group makes the following (preliminary) recommendations to regulators, providers and users of social network services:

<u>*Regulators*</u>

1. *Introduce the option of a right to pseudonymous use – i.e. to act in a social network service under a pseudonym[23] –,* where not already part of the regulatory framework.

2. *Ensure that service providers are honest and clear about what information is required for the basic service so that users can make an informed choice whether to take up the service*, and that users can refuse any secondary uses (at least through opt-out), specifically for (targeted) marketing. Note that specific problems exist with consent of minors[24].

3. *Introduction of an obligation to data breach notification for social network services*. Users will only be able to deal especially with the growing risks of identity theft if they are notified of any data breach. At the same time, such a measure would help to get a better picture of how well companies secure user data, and provide a further incentive to further optimise their security measures.

4. *Re-thinking the current regulatory framework with respect to controllership* of (specifically third party-) personal data published on social networking sites, with a view to possibly attrib-

uting more responsibility for personal data content on social networking sites to social network service providers.

5. *Improve integration of privacy issues into the educational system.* As giving away personal data online becomes part of the daily life especially of young people, privacy and tools for informational self-protection must become part of school curricula.

Providers of social network services

Providers must have a vital self-interest in preserving security and privacy of personal data of their users. A failure to make swift progress in this field may result in loss of user confidence (which is already now considerably shaken by recent security and privacy incidents), and may well result in an economic backlash comparable to the crisis that hit the digital economy in the late 1990s.

1. *Transparent and open information of users* is one of the most important elements of any fair processing and use of personal information. While the need for such a mechanism is recognised in most national, regional and international regulatory instruments for privacy, the present form in which many service providers inform their users may need to be revisited: At present – and in many cases in line with existing regulatory frameworks – privacy information form a part of sometimes complex and lengthy "terms and conditions" of a service provider. In addition, a privacy policy may be provided. Some service providers suggest that the percentage of users actually downloading this information is very low[25]. Even if this information is displayed on the screen when a user signs up to a service, and can also be accessed later if the user so wishes, the goal to inform users about potential consequences of their actions during the use of a service (e.g. when changing privacy settings for a collection of – say – pictures) may be better served by built-in, context-sensitive features, that would deliver the appropriate information based on user actions.

   User information should specifically comprise information about the jurisdiction under which the service provider operates, about users' rights (e.g. to access, correction and deletion) with respect to their own personal data, and the business model applied for financing the service. Information must be tailored to the specific needs of the targeted audience (especially for minors) to allow them to make informed decisions.

   Information of users should also refer to third party data: Providers of social network services should – on top of informing their users about the way they treat their (the users') personal data, also inform them about the do's and don'ts of how they (the users) may handle third party information contained in their profiles (e.g. when to obtain the data subjects' consent before publication, and about possible consequences of breaking the rules). Especially the huge quantities of photos in user profiles showing other people (in many cases even tagged with name and/or link to the other persons' user profile) are an issue in this context, as current practices are in many cases not in line with existing legal frameworks governing the right to control one's own image.

   Candid information should also be given about remaining security risks, and possible consequences of publishing personal data in a profile, as well as about possible legal access by third parties (including also e.g. law enforcement, secret services).

2. *Introduce the creation and use of pseudonymous profiles as an option*, and encourage its use.

3. *Living up to promises made to users:* A *conditio sine qua non* for fostering and maintaining user trust is clear and unambiguous information about how their information will be treated by

the service provider, specifically when it comes to sharing personal data with third parties. However, with some service providers there are at present ambiguities with respect to those promises. The most prominent example is the popular statement "we will never share your personal information with third parties" in relation to targeted advertising. While this statement may be formally correct in the eyes of the service provider, some providers fail to clearly communicate the fact that e.g. for displaying advertisements in the browser window of a user, the IP address of these users may be transmitted to another service provider delivering the content of the advertisement, in some cases based on information processed by the social network service provider from a users' profile. While the profile information itself may indeed not be transmitted to the advertisement provider, the users' IP address will[26] (if the social network provider does not e.g. use a proxy mechanism to hide the user IP address from the provider of the advertisement). The problem is that some providers of social network services erroneously assume that IP addresses are not personal data, while in most jurisdictions they in fact often are. Such ambiguities may mislead users and may spur an erosion of trust when users learn about what happens in reality, which is neither in the interest of the users, nor in the interest of the service provider. Similar problems exist regarding the use of cookies.

4. *Privacy-friendly default settings* play a key role in protecting user privacy: It is known that only a minority of users signing up to a service will make any changes to default settings – including privacy settings. The challenge for service providers here is to choose settings that offer high degree of privacy by default without making the service unusable. At the same time, usability of setting features is key to encourage users to make their own changes. In any case, non-indexibility of profiles by search engines should be a default.

5. *Improve user control over use of profile data:*

   - *within the community*; e.g. allow restriction of visibility of entire profiles, and of data contained in profiles, as well as restriction of visibility in community search functions. Tagging of photos (i.e. the addition of links to an existing user profile or the naming of depicted persons) should be bound to the data subject's prior consent.

   - *create means allowing for user control over third party use of profile data* – vital to especially address risks of ID theft. However, there are at present only limited means to control information once it is published. The experience of the movie and music industries with digital rights management technologies suggests that possibilities may in this respect stay limited. Nevertheless, services providers should strengthen research activities in this domain: Existing and maybe promising approaches include research on the "semantic" or "policy-aware web[27]", encrypting user profiles, decentralise storage of user profiles (e.g. with users themselves), the use of watermarking technologies for photos, the use of graphics instead of text for displaying information, and the introduction of an expiration date to be set by users for their own profile data[28]. Service providers should also strive to discourage secondary use especially of pictures by offering a function allowing users to pseudonymise or even anonymise pictures[29]. They should also take effective measures to prevent spidering, bulk downloads (or bulk harvesting) of profile data. Specifically, user data should only crawled by (external) search engines if a user has given his explicit, prior and informed consent.

   - *Allow for user control over secondary use of profile and traffic data;* e.g. for marketing purposes, as a minimum: opt-out for general profile data, opt-in for sensitive profile data (e.g. political opinion, sexual orientation) and traffic data. Many existing legal frameworks contain binding rules on secondary uses for marketing purposes, which must be observed by providers of social network services. Consider letting users decide for themselves, which of their profile data (if any) they would like to be used for targeted marketing. In addition, the introduction of a fee should be considered as an additional option at the choice

of the user for financing the service instead of use of profile data for marketing.

- *Comply with user rights recognised in national, regional and international privacy frameworks;* including the right of data subjects to have data – which may well be entire profiles – erased in a timely manner.

- *Address the issues that may arise in cases of a takeover or merger of a social network service company*: Introduce guarantees for users that new owner will maintain present privacy (and security) standard.

6. *Appropriate complaint handling mechanisms* should be introduced (e.g. to "freeze" contested information, or pictures), where they do not already exist, for users of social networks, but also with respect to third party personal data. Timely response to data subjects is important. Measures may also include a penalty mechanism for abusive behaviour with respect to profile data of other users and third party personal data (incl. removing users from site as appropriate).

7. *Improve and maintain security of information systems.* Use recognised best practices in planning, developing, and running social network service applications, including independent certification.

8. *Devise and/or further improve measures against illegal activities, such as spamming, and ID theft.*

9. *Offer encrypted connections for maintaining user profiles,* including secured log-in.

10. Social network providers acting in different countries or even globally should respect the privacy standards of the countries where they operate their services.

Users of social networks

1. *Be careful*. Think twice before publishing personal data (specifically name, address, or telephone number) in a social network profile. Think also about whether you would like to be confronted with information or pictures in a job application situation. Maintain your profile information. Learn from CEOs of big companies: These people know about the value of their personal information and control it. This is why you will not find a lot of personal information about them on the web.

2. *Think twice before using your real name in a profile*. Use a pseudonym instead. Note that even then you have only limited control over who can identify you, as third parties may be able to lift a pseudonym, especially based on pictures. Think of using different pseudonyms on different platforms.

3. *Respect the privacy of others*. Be especially careful with publishing personal information about others (including pictures or even tagged pictures), without that other person's consent. Note that illegal publication especially of pictures is a crime in many jurisdictions.

4. *Be informed*: Who operates the service? Under which jurisdiction? Is there an adequate regulatory framework for protecting privacy? Is there an independent oversight mechanism (like a Privacy Commissioner) that you can turn to in case of problems? Which guarantees does the service provider give with respect to handling your personal data? Has the service been certified by independent and trustworthy entities for good quality of privacy, and security? Use the web to educate yourself about other people's experience with the privacy and security prac-

tices of a service provider you do not know. Use existing information material from providers of social network services, but also from independent sources like Data Protection Agencies[30], and security companies[31].

5. *Use privacy friendly settings*. Restrict availability of information as much as possible, especially with respect to indexing by search engines.

6. *Use different identification data* (e.g. login and password) than those you use on other websites you visit (e.g. for your e-mail or bank account).

7. *Use opportunities to control* how a service provider uses your personal (profile and traffic) data. E.g. opt out of use for targeted marketing.

8. *Pay attention to the activity of your children in the Internet*, especially on social network websites.

Closing remark

The Working Party calls upon Consumer and Privacy Protection Organisations to take appropriate measures to raise awareness with regulators, service providers, the general public, and notably young people[32] about privacy risks regarding the use of social networks and responsible behaviour with respect to one' own personal data, as well as those of others.

The Working Group will closely monitor future developments with respect to the protection of privacy in social network services and revise and update this Guidance as necessary.

Notes

[1] Quoted from Wikipedia at http://en.wikipedia.org/wiki/Social_network_service [viewed on 5 February 2008]
[2] This report does not cover chat, blogging, and ranking sites.
[3] A German researcher recently identified in a selection of popular social network services about 120 single personal attributes contained in user profiles in social network services, like for example age, home address, favourite movies, books, music etc., and also including political opinions and even sexual preferences. Cf. „Berliner Morgenpost“ of 23 January 2008, S. 9: „Mehr Informationen als die Stasi“; http://www.morgenpost.de/content/2008/01/23/wissenschaft/942868.html (in German language)
[4] A term attributed to Marc Prensky, a US speaker, writer, consultant, and game designer in education and learning. Cf. e.g. http://www.ascd.org/authors/ed_lead/el200512_prensky.html [viewed on 5 February 2008]
[5] Already now, secret services from the United States (namely the “Open Source Center”, a service attached to the US “Director of National Intelligence”) seem to be using data from what is called “open sources”, which seem to include inter alia YouTube, but also social media like Myspace, and blogs; cf. http://www.fas.org/blog/secrecy/2008/02/open_source_intelligence_advan.html [accessed 7 February 2008]
[6] While some service providers have tried to create limited areas within their services to give users more control over how they share their (personal) information, others make such information or parts thereof available to a bigger audience, which can in some cases be the entire community – and thus millions of perfect strangers: “it stays between us”, yes, but “us” may well be 50 million+.
[7] Cf. the statement of John Lawford from the Canadian Public Interest Advocacy Center in a speech given 3 October 2007 at the OECD-Canada Technology Foresight Forum “Confidence, privacy and security”; cf. http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf [accessed 6 February 2008], p. 35
[8] Cf. ENISA Position Paper No.1: “Security Issues and Recommendations for Online Social Networks”, October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf
[9] Note that some social network services allow search engines to crawl user content, and that search engine services have emerged recently specialising in offering personal profiles drawn together from different sources. On the other hand, service providers seem to have at present little or no control over the actions of spiders on their websites who do not respect the “robots.txt” protocol.
[10] “APRIL 26--A Pennsylvania woman claims that her teaching career has been derailed by college administrators who unfairly disciplined her over a MySpace photo that shows her wearing a pirate hat and drinking from a plastic cup. In a federal lawsuit, […] charges that Millersville University brass accused her of promoting underage drinking after they discovered her MySpace photo, which was captioned "Drunken Pirate". Quoted from http://www.thesmokinggun.com/archive/years/2007/0426072pirate1.html [accessed 11 February 2008]. Cf. also The Guardian, January 11, 2008: “Would-be students checked on Facebook”; http://education.guardian.co.uk/universityaccess/story/0,,2238962,00.html
[11] Cf. e.g. “Employers Use "Facebook" and "MySpace" to Weed Out Applicants”; http://www.wtlv.com/tech/news/news-article.aspx?storyid=64453 [accessed 12 February 2008]. Finland seems to be the only country so far to ban such practices.
[12] Other examples to emerge in the future may well include use by immigration authorities when travelling abroad.
[13] Cf. e.g. “Facebook API Unilaterally Opts Users Into New Services”, by Ryan Singel, 25 May 2007, http://blog.wired.com/27bstroke6/2007/05/facebook_api_un.html; cf. also Chris Soghoian: “Exclusive: The next Facebook privacy scandal”, 23 January 2008, http://www.cnet.com/8301-13739_1-9854409-46.html?tag=blog.1 [accessed 12 February 2008]
[14] Cf. as a telling example for instance the recent “Natalie”- and “frog-” experiments conducted by the Security company Sophos; cf. “Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Research highlights dangers of irresponsible behaviour on social networking sites”, August 2007; http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html and “Der Fall 'Natalie'. Online Communities zunehmend IT-Sicherheits-Risiko. Experten warnen vor massivem Anstieg von Datendiebstahl und -missbrauch auf Social Network Websites“, 21 January 2008 (in German language)
[15] Cf. “Secret Crush Facebook App Installing Adware, Security Firm Charges”, Wired of 3 January 2008, http://blog.wired.com/27bstroke6/2008/01/secret-crush-fa.html
[16] Cf. “Phantom Photos: My photos have been replaced with those of another”; http://flickr.com/help/forum/33657/
[17] Cf. e.g. the December 2006 “MySpace XSS QuickTime Worm”; http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708
[18] Cf. PC World: “Worm Hits Google's Orkut” of 19 December 2007, http://www.pcworld.com/article/id,140653-c,worms/article.html , and SC Magazine US: “Google's Orkut hit by self-propagating trojan” of 26. February

2008, http://www.scmagazineus.com/Googles-Orkut-hit-by-self-propagating-trojan/article/107312/ [both accessed 3 March 2008]

[19] Cf. e.g. „Datenleck beim StudiVZ? [Update]"; http://www.heise.de/newsticker/meldung/81373/ (in German language)

[20] In addition, the steep growth of information stored electronically every year is in itself seen as a security risk: At the last RSA Europe Security Conference in London in 2007, RSA president Art Coviello was cited saying that alone in 2006 176 exabytes of data had been generated worldwide, and that such a huge amount of data was in his view unmanageable, and could not be secured effectively; cf. the German Computer Magazine "iX", December 2007, p. 22 "Trübe Aussichten: Große Datenmengen verhindern Datensicherheit" (in German language); http://www.heise.de/kiosk/archiv/ix/2007/12/022/

[21] Cf. ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

[22] Cf. ENISA Position Paper No.1 (footnote 21 supra), p. 12

[23] "Pseudonymous use" in this context means the right to act in a social network service under a pseudonym without having to reveal one's "true" identity to other users of the service, or to the general public, if the user wishes so. Depending on circumstances, this may well include having to reveal one's true identity vis-à-vis the provider of the social network when registering.

[24] Cf. Working Paper "Children's' Privacy On Line: The Role of Parental Consent", adopted at the 31st meeting, Auckland (New Zealand), 26/27 March 2002; http://www.datenschutz-berlin.de/attachments/205/child_en.pdf?1200656702

[25] A representative from facebook stated recently at an OECD conference that the percentage of users visiting a privacy policy may not be more than a **quarter of a percent**; cf. http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf p. 33f. [accessed 6 February 2008].

[26] Depending on circumstances, the advertisement provider may even be able to reconstruct some or all of the underlying profile information based on the kind of targeted advertisement that is to be displayed to a specific user.

[27] Cf. e.g. Daniel J. Weitzner, Jim Hendler, Tim Berners-Lee, Dan Connolly: "Creating a Policy-Aware Web: Discretionary, Rule-based Access for the World Wide Web". To appear in: Web and Information Security, E. Ferrari and B. Thuraisingham (eds), Idea Group Inc., Hershey, PA (forthcoming); http://www.w3.org/2004/09/Policy-Aware-Web-acl.pdf , and Sören Preibusch, Bettina Hoser, Seda Gürses, and Bettina Berendt: Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling; http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/05-Preibusch.pdf [both accessed 12 February 2008].

[28] Cf. e.g. The Royal Academy of Engineering: Dilemmas of Privacy and Surveillance. Challenges of Technological Change. March 2007, at 7.2.1, p. 40

[29] Cf. ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", October 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, p.23

[30] Cf. e.g. the brochure "when online gets out of line" jointly published by facebook and the Information and Privacy Commissioner of Ontario, Canada, at http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf, the US Federal Trade Commission: "Social Networking Sites: A Parent's Guide" at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm and "Social Networking Sites: Safety Tips for Tweens and Teens" at http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm

[31] Cf. e.g. the model privacy settings proposed by Sophos for facebook; http://www.sophos.com/security/best-practice/facebook.html

[32] Cf. e.g. the campaign „dubestemmer" launched by the Norwegian Data Protection Authority; http://www.dubestemmer.no/english.php, the "DADUS"-Project of the Portuguese Data Protection Authority; http://dadus.cnpd.pt, and the initiatives cited in footnote 30 above