PART 2. PRIVACY IN THE INTERNET

Ulf-Dietrich Reips*
University of Deusto in Bilbao, Spain
Ikerbasque, Basque Foundation for Science

Privacy and the Disclosure of Information on the Internet: Issues and Measurement

Over the past twenty or so years, the Internet has become an indispensable and ubiquitous feature of daily life in the developed world. As is often the case, the technology is somewhat of a double-edged sword. While it may enhance our lives in many ways, as our world becomes an information society, it also raises new concerns. For much of that information relates to not just things but to people. Information about us is accessed, stored, manipulated, data mined, shared, bought and sold, analyzed and potentially lost, stolen or misused by countless government, corporate, public and private agencies, often without our knowledge or consent. When we communicate, interact or even just go shopping, both online and offline, we leave data trails and digital footprints behind us, generating information about our lives and activities as we go. As the recognition of this pheno-menon grows, the issue of privacy has increased in salience. Research and articles about online privacy are now appearing regularly in the academic and popular press (e.g. Hurtado, 2008; Joinson, Reips, Buchanan, & Paine, 2010; Online ad targeting system, 2009; Paine, Reips, Stieger, Joinson, & Buchanan, 2007).

* Correspondence concerning this article should be addressed to Prof. Dr. Ulf-Dietrich Reips, Departamento de Psicología, Universidad de Deusto, Apartado 1, 48080 Bilbao,Spain. E-mail: reips@deusto.es

Introduction

Consider the following stories:

- in Italy regulators required Internet cafés to photocopy passports and monitor their clients' Internet access in detail (Celeste, 2005);
- on a web site, women identify cheaters (see Figure 1): "It reads like the FBI's Most Wanted list, complete with mug shots, physical descriptions, aliases and modus operandi of alleged perpetrators. But the fugitives listed on www.dontdatehimgirl.com aren't evading law enforcement. They're on the run from wives, girlfriends and lovers." (Hatcher, 2005);
- the results of a study released by University of Cambridge researchers conclude that Web sites that host user-uploaded photos commonly store those photos even after users deleted them. The researchers studied 16 popular Web sites, saved the URLs of uploaded photos, and then revisited those URLs after deleting the photos. On almost half of the sites, the photos remained accessible after 30 days. The researchers found that social networks are particularly slow to fully delete. Researcher Joseph Bonneau of the team says: "This demonstrates how social networking sites often take a lazy approach to user privacy" (Porter, 2009).

This chapter is motivated by the recognition that there are important privacy issues related to Internet activities as mundane as buying your weekly groceries over the Web (e.g. does the retailer store information on your purchases? Is it sold to third parties so they can send you targeted junk mail?), or as specialized as Internet-based psychological research at academic institutions (e.g., is identifying information gathered about participants? Can confidentiality be guaranteed?) or e-teaching at universities (e.g., if Virtual Learning Environments allow student behavior to be tracked, what are the ethical implications? Would awareness of this affect students' willingness to use the technology?).

Furthermore, if these concerns are acted upon – what are appropriate measures? Some measures may resemble overshooting, such as cases where university IT departments tightly limit what Internet scientists can do. It may, for example, be necessary to record participant computers' IP addresses* to identify possible multiple submissions by the same participant (Birnbaum & Reips, 2005). Accordingly, privacy concerns sometimes clash with other values, such as with the need to properly cite resources (some may not wish their identity to be masked, rather be mentioned as authors of their words), or the need to ensure high data quality in research.

* Each computer on the Internet is assigned an Internet Protocol (IP) address that is unique at any point in time. IP addresses often are assigned temporarily, and can be camouflaged via anonymizing services such as http://tools.rosinstrument.com/cgi-proxy.htm

Awareness of these issues may affect people's behavior in a wide range of contexts. It is therefore important to have methods of identifying and quantifying people's privacy concerns, as a tool for research on how people behave both on and off the Internet.

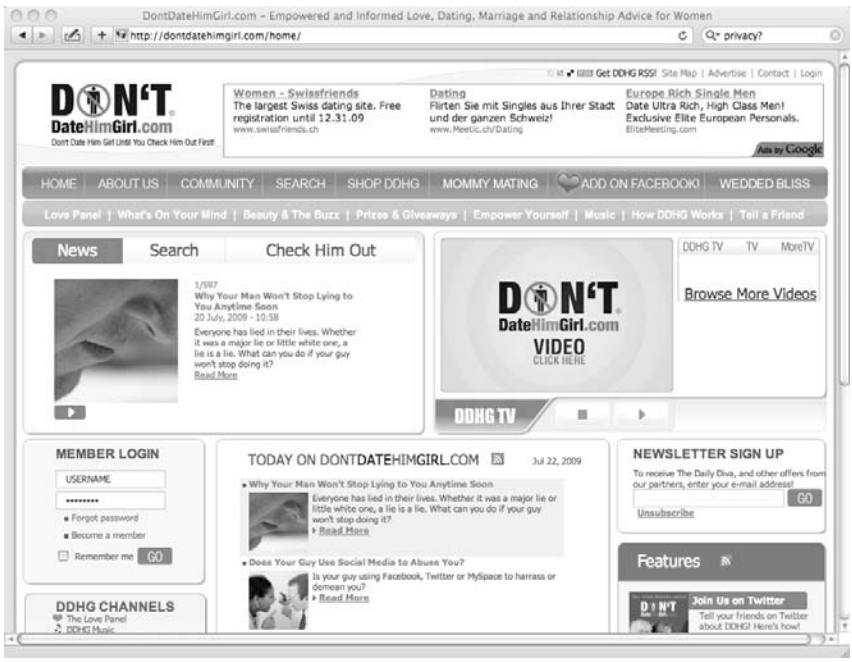

Figure 1. A screenshot from www.dontdatehimgirl.com, where people report on cheating men – whether true or not.

Definitions of Privacy

There have been several attempts to define privacy. In a legal context, privacy has been considered to be largely synonymous with a "right to be let alone" (Warren & Brandeis, 1890). However, others have since argued that privacy is only the *right to prevent the disclosure of personal information to others* (e.g., Westin, 1967).

The British Royal Academy of Engineering (2007) summarizes the many aspects of privacy as follows: "Privacy comes in many forms, relating to what it is that one wishes to keep private:

- privacy as *confidentiality*: we might want to keep certain information about ourselves, or certain things that we do, secret from everyone else or selected others;
- privacy as *anonymity*: we might want some of our actions (even those done in public) not to be traceable to us as specific individuals;
- similarly, we might wish for privacy of *identity*: the right to keep one's identity unknown for any reason, including keeping one's individual identity separate from a public persona or official role;
- privacy as *self-determination*: we might consider some of our behavior private in that it is 'up to us' and no business of others (where those 'others' may range from the state to our employers);
- similarly, we can understand privacy as *freedom* to be 'left alone', to go about our business without being checked on: this includes freedom of expression, as we might wish to express views that the government, our employers, or our neighbors might not like to hear;
- privacy as *control of personal data*: we might desire the right to control information about us – where it is recorded, who sees it, who ensures that it is correct, and so on." (p. 11).

Despite many attempts to create a synthesis of the existing literature, a unified and simple account of privacy has yet to emerge. The highly complex nature of privacy that we can see from the list above has resulted in an alternative way of defining it – through its various dimensions. Burgoon, Parrott, LePoire, Kelley, Walther, and Perry (1989) and DeCew (1997) have developed multidimensional definitions of privacy, and recently attempts were made to empirically capture what people subjectively experience as privacy (Buchanan, Paine, Joinson, & Reips, 2007; Paine, Reips, Stieger, Joinson, & Buchanan, 2007).

The dimension *Informational Privacy* appears in both Burgoon et al.'s and DeCew's definitions. Burgoon et al. (1989) state that informational privacy relates to an individual's right to determine how, when, and to what extent information about the self will be released to another person (Westin, 1967) or to an organization. The dimension *Accessibility Privacy*, as defined by DeCew, overlaps with informational privacy in cases where "acquisition or attempted acquisition of information involves gaining access to an individual" (DeCew, 1997, p. 76). Thus, the repeated cases of others getting access to Hotmail e-mail accounts (Fildes, 2009; Lloyd, 1999) is a clear breach of Informational/ Accessibility Privacy. For example, a victim of the 1999 incident is quoted as saying: "I have a Hotmail account. … This scares the heck out of me. Now anybody and their brother can read my mail." (Lloyd, 1999). These breaches combined with other Hotmail privacy incidents (e.g., Mainelli, 2002) to se-

verely impede on the service's public image. Accessibility Privacy also extends to cases where physical access is at stake (for example, 'intrusions' by spam mail or computer viruses; not access to information about home addresses that people might wish to keep private and so on). This dimension overlaps with Burgoon et al.'s *Physical dimension* of privacy, which is the degree to which a person is physically accessible to others.

Finally, DeCew identified *Expressive Privacy*, which "protects a realm for expressing ones self-identity or personhood through speech or activity. It protects the ability to decide to continue or to modify ones behavior when the activity in question helps define oneself as a person, shielded from interference, pressure and coercion from government or from other individuals" (DeCew, 1997, p. 77). In this way, expressive privacy restricts external social control over choices about lifestyle, and improves internal control over self-expression and the ability to build interpersonal relationships. This dimension overlaps with Burgoon's *Social / Communicational dimension of privacy*, which is an individual's ability and effort to control social contacts (Altman, 1975).

Central to these dimensions is the desire to keep personal information out of the hands of others, or in other words *privacy concern* (Westin, 1967), and the ability to *connect with others without interference*. In a systematic discussion of the different notions of privacy, Introna and Pouloudi (1999) developed a framework of principles that explored the interrelations of interests and values for various stakeholders where privacy concerns have risen. In this context, concern for privacy is a subjective measure – one that varies from individual to individual based on that person's own perceptions and values. In other words, different people have different levels of concern about their own privacy.

The Importance of Privacy in Internet-Based Research

When the interactive WWW became available, a few pioneers of Internet-based research discovered that this technology can be used very well in social and behavioral research. By now we know that much of Internet-based research produces results similar to the one conducted in the laboratory (Dandurand, Shultz, & Onishi, 2008; Krantz & Dalal, 2000; but see Birnbaum, 2001 and Vadillo & Matute, 2009). The first web-based research questionnaires appeared on the Internet in 1994, after the new standard HTML 2 was implemented that allowed users of Web browsers to send back information to the server. Krantz, Ballard, and Scher (1997) and Reips (1997) conducted the first Internet-based experiments in 1995. In 2000, Musch and Reips published results from a survey con-

ducted in October 1998 and April 1999, in which they had reached almost all of the Web experimenters world-wide at that time. Then, 29 Web experimenters answered regarding 35 Web experiments. The number of studies conducted via the World Wide Web has grown ever since, Reips and Krantz (2010) report more than 2000 archived Internet-based research studies in their archives alone.

Examples for such Internet-based social and behavioral studies currently in progress can best be found on designated web sites, the reader may visit studies linked at the following web sites:

- Web experiment list (Reips & Lengler, 2005): http://wexlist.net/
- Web survey list: http://wexlist.net/browse.cfm?action=browse&modus=survey
- Web Experimental Psychology Lab (Reips, 2001): http://wexlab.eu/
- Psychological Research on the Net by Krantz:
- http://psych.hanover.edu/research/exponnet.html
- Online Social Psychology Studies by Plous:
- http://www.socialpsychology.org/expts.htm

Tools to create Internet-based studies or response items for web questionnaires, to recruit participants, to include an Internet-based Big Five personality test with one's own study, to analyze log files, and to learn about Internet- based research can be found at the iScience Server at http://www.iscience.eu/.

When Musch and Reips (2000) conducted their above mentioned survey nothing was asked about the issue of privacy specifically, but one question was concerned with potential problems in Web experiments. Of all problems, ethical problems were considered the least problematic, with a mean rating of 1.5 ($SD = 1.0$) on a scale of 1 ("not problematic at all") to 7 ("very problematic").

In 2001 Frick, Bächtiger, and Reips published the results from an experiment that investigated whether a request to self-disclose personal information (and also incentives for participation) has an impact on data quality and dropout in Internet-based research. Early versus late placement of demographic questions resulted in lower dropout and better data quality, showing that the request of such information (i.e. less privacy) may be necessary for methodological reasons. Participants seem to value a questionnaire more after having given personal information, and subsequently are more compliant. This process can be explained by the *Theory of Cognitive Dissonance* (Festinger, 1957). The theory proposes that people have a motivational drive to reduce dissonance by changing their attitudes, beliefs, and behaviors, or by justifying or rationalizing them. Thus, to avoid an uncomfortable feeling of dissonance between logically inconsistent cognitions of "I am providing privacy-relevant personal information to the current questionnaire" and "The current questionnaire is not worth being answered

fully", participants change their behavior regarding the second cognition once they have already provided personal information.

Following another theory, the *Theory of Planned Behavior* by Ajzen (1991), Yao and Linz (2008) investigated whether self-protections of online privacy could be predicted from psychological processes. Their findings show that individuals' attitude toward online privacy protection was significantly influenced by *subjective norm* (one of the main components of the Theory of Planned Behavior), *need for privacy*, a generalized sense of *self-efficacy*, and a general *fear of crime* (in order of explained variance). They conclude that a favorable attitude toward online privacy protection and a high level of perceived behavioral control regarding online privacy protection strategies are necessary conditions for users to actually adopt these strategies.

From these two examples of research on online privacy issues a core constituency of the relationship of privacy and online research evolves: they are interdependent. We cannot know about the experience of privacy on the Internet without researching it online, but the (level of) participation in such research largely depends on personal factors and factors in the design of the online research (see Reips, 2010). One of the methodological solutions to the problem may be to research privacy issues (including those related to the Internet) comparatively both online and offline.

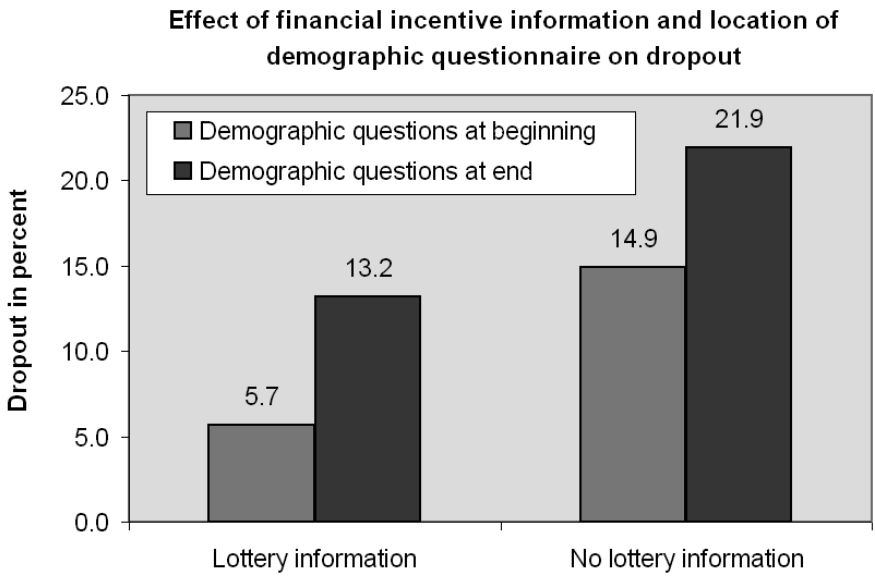

Figure 2. Effect of financial incentive information and location of demographic questionnaire on drop out (Frick, Bächtiger, & Reips, 2001, p. 214; reprint with kind permission).

Measuring Privacy

Now that we know that privacy is best treated as a multi-dimensional construct, we can begin to ask how we then best go about measuring these privacy dimensions. I will first present a classical approach, the *Westin segmentation*, and see why it is helpful yet not sufficient for many purposes. Then I will move on to three short Internet-administered scales measuring privacy related attitudes (*'Privacy Concern'*) and behaviors (*'General Caution'* and '*Technical Protection'*) developed by Buchanan, Paine, Joinson, & Reips, (2007). Finally, I will describe attempts to indirectly measure privacy and self-disclosure via active and passive non-response and a tendency for "blurring".

A Typology of Privacy Concerns

The Westin segmentation (Westin, 1967) is a simple and practical way of categorizing people by their different levels of privacy concerns. Because it is so simple, it lends itself to market research, where there is always the need to capture the most obvious effects quickly.

The market research company *Harris Interactive* since 1995 regularly conducts privacy polls by telephone across the United States. The survey divides the approximately 1000 respondents into one of three categories depending on their answers to three statements. The statements developed by Westin and Harris are:

1. "Consumers have lost all control over how personal information is collected and used by companies."
2. "Most businesses handle the personal information they collect about consumers in a proper and confidential way."
3. "Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today."

For all three statements the respondents are provided with four point scales ranging from "strongly agree" to "strongly disagree". The answers to these items are combined as follows. Participants providing privacy-oriented responses to all three items are categorized as "privacy fundamentalists", privacy unconcerned participants giving non-privacy oriented responses to all the statements are categorized as "privacy unconcerned". Those in between are called "privacy pragmatists". The three categories of respondents can thus be defined as follows (Joinson, Paine, Buchanan, & Reips, 2006, p. 335):

- *"Privacy fundamentalists* – these view privacy as having an especially high value which they feel very strongly about and they usually have high levels of distrust. They tend to feel that they have lost a lot of their privacy and are strongly resistant to any further erosion of it. Currently around a third of all adults are privacy fundamentalists.
- *Privacy pragmatists* – these also have strong feelings about privacy and tend to have medium to high levels of distrust. They are very concerned to protect themselves from the misuse of their personal information by other people and organizations. They weigh the value to them and society of providing personal information and they are often willing to allow people to have access to, and to use, their personal information – where they understand the reasons for its use, can see the benefits for so doing and when they believe care is taken to prevent the misuse of this information. Currently around approximately 55% of all adults are privacy pragmatists.
- *Privacy unconcerned* – these have no real concerns about privacy or about how other people and organizations are using information about them. They usually have low to no levels of distrust. Approximately 10% of all adults are privacy unconcerned."

Joinson, Paine, Buchanan, and Reips (2006) used the Westin segmentation for research into predicting the likely acceptance of various scenarios of implementing ID cards in the UK – a topic that was widely discussed at the time, because the UK government had proposed a scenario that combined high compulsion with a centralized database. Joinson et al. could show that such a scenario leads to the greatest negative shift in attitudes towards ID cards compared to pre-scenario attitudes, while a scenario proposed by others (e.g., the London School of Economics) showed a significantly less negative shift in attitudes. People's pre-existing privacy concerns, as measured with an Internet-based version of the Westin segmentation, indeed also influenced their evaluation of the different implementation scenarios. The research was cited in the debate in the British parliament, which subsequently decided against the government proposal (Whitley & Hosein, 2008).

Measuring Privacy Related Attitudes: Internet-Administered Scales

Naturally, the Westin methodology for the study of privacy attitudes can be seen critically. Just three business-related items may be far from capturing all relevant aspects, Furthermore, the use of the term "fundamentalist" to describe

people who may simply be better informed about privacy threats and making reasoned decisions accordingly, seems a bit overstated.

Consequently, Buchanan, Paine, Joinson, and Reips (2007) set out to develop a more fine-grained and psychometrically sound measurement of online privacy concern and its protection validated for use on the Internet. They developed one attitude scale (Privacy Concern) with 16 items and two behavioral scales (General Caution and Technical Protection), each with 6 items. The scales are displayed in Tables 1 and 2, and Figure 3 shows their Cronbach's Alpha values.

Table 1
Privacy Behavior factor loadings (Buchanan, Paine, Joinson, & Reips, 2007)

	Content	Factor loading	
		1	2
	General Caution		
1	Do you shred / burn your personal documents when you are disposing of them?	.37	.16
2	Do you hide your bank card PIN number when using cash machines / making purchases?	.33	.08
3	Do you only register for websites that have a privacy policy?	.70	.07
4	Do you read a website's privacy policy before you register your information?	.78	-.04
5	Do you look for a privacy certification on a website before you register your information?	.79	-.03
6	Do you read license agreements fully before you agree to them?	.68	-.01
	Technical Protection		
1	Do you watch for ways to control what people send you online (such as check boxes that allow you to opt-in or opt-out of certain offers)?	.19	.41
2	Do you remove cookies?	.26	.60
3	Do you use a pop up window blocker?	.03	.75
4	Do you check your computer for spy ware?	.05	.75
5	Do you clear your browser history regularly?	.15	.62
6	Do you block messages / emails from someone you do not want to hear from?	.21	.45

Note. The instructions accompanying the scales were "*For this part of the survey, we are interested in your privacy related behavior in general and when online. Please answer every question using the full scale provided*". Participants responded using a 5-point scale for each item (never – always).

Table 2
Privacy Attitude factor loadings (Buchanan, Paine, Joinson, & Reips, 2007)

	Content	Factor loadings
1	In general, how concerned are you about your privacy while you are using the internet?	.69
2	Are you concerned about online organisations not being who they claim they are?	.73
3	Are you concerned that you are asked for too much personal information when you register or make online purchases?	.58
4	Are you concerned about online identity theft?	.75
5	Are you concerned about people online not being who they say they are?	.74
6	Are you concerned that information about you could be found on an old computer?	.59
7	Are you concerned who might access your medical records electronically?	.63
8	Are you concerned about people you do not know obtaining personal information about you from your online activities?	.68
9	Are you concerned that if you use your credit card to buy something on the internet your credit card number will obtained / intercepted by someone else?	.74
10	Are you concerned that if you use your credit card to buy something on the internet your card will be mischarged?	.72
11	Are you concerned that an email you send may be read by someone else besides the person you sent it to?	.68
12	Are you concerned that an email you send someone may be inappropriately forwarded to others?	.68
13	Are you concerned that an email you send someone may be printed out in a place where others could see it?	.63
14	Are you concerned that a computer virus could send out emails in your name?	.61
15	Are you concerned about emails you receive not being from whom they say they are?	.63
16	Are you concerned that an email containing a seemingly legitimate internet address may be fraudulent?	.67

Note. The instructions accompanying the scale were "*For this part of the survey, we are interested in any privacy concerns you might have when online. Please answer every question using the full scale provided*". Participants responded using a 5-point scale for each item (not at all – very much).

Validity of the three scales was examined by comparing scores of individuals drawn from groups considered likely to differ in privacy-protective behaviors. Members of one of the groups were technical students and the ones of the other group were nontechnical students. Technical students had significantly higher scores on the General Caution and Technical Protection scales. The groups of students did not differ in Online Privacy Concern.

In Study 3, correlations between the scores on the three scales and two established measures of privacy concern (among them the Westin measure) were exa-

mined. The authors concluded that the scales are reliable and valid instruments suitable for administration via the Internet, and recommended them for use in Internet-based privacy research.

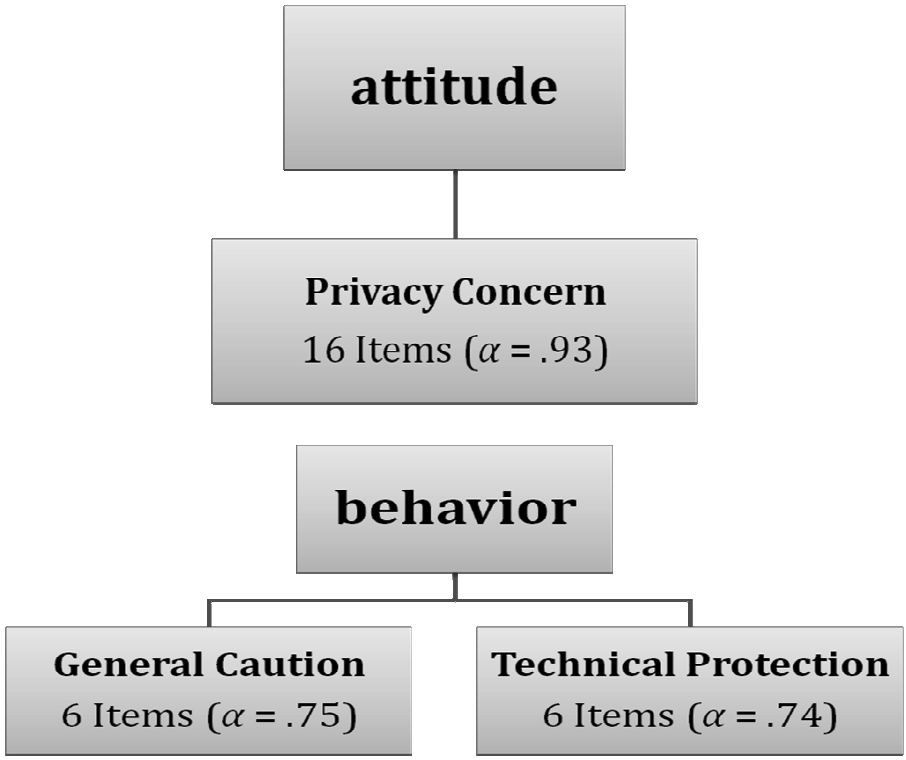

Figure 3. Online measurement of privacy: the three components, with Cronbach's alphas as measured for the subscales.

Following up on Buchanan et al. (2007) Reips, Buchanan, and Oostlander (2010) developed GPCP, a German version of the scale for online privacy concern and protection for use on the Internet. The aim of their paper was to translate the *Online Privacy Questionnaire* from the original English version into German and to validate the translation with a German speaking sample. Like the original, the *Online Privacy Questionnaire* consists of three scales: one attitude scale (Privacy Concern) with 16 items and two behavioral scales (General Caution and Technical Protection), each with 6 items. The validation was based on a sample of $N = 514$. Reips et al. were able to replicate the factorial structure of

the original scale in the German version. For the Privacy Concern Scale and the General Caution Scale Cronbach's alpha was α =.86 resp. α =.75 (α =.93 resp. α =.75 in the original scale). Cronbach's alpha of the Technical Protection Scale was slightly lower with α =.65 (α =.74 in the original scale), probably caused by a ceiling effect that turned up for most items. Following the study of Buchanan et al. (2007) the scale validity of the translation was checked by comparing groups of different technical knowledge. However, the study improved on Buchanan et al. by explicitly measuring technical knowledge via the TECOWI (scale for technical computer knowledge), a subscale of the INCOBI – Inventory of Computer Knowledge, a questionnaire for "objective technical computer knowledge" (Richter, Naumann, & Groeben, 2001).

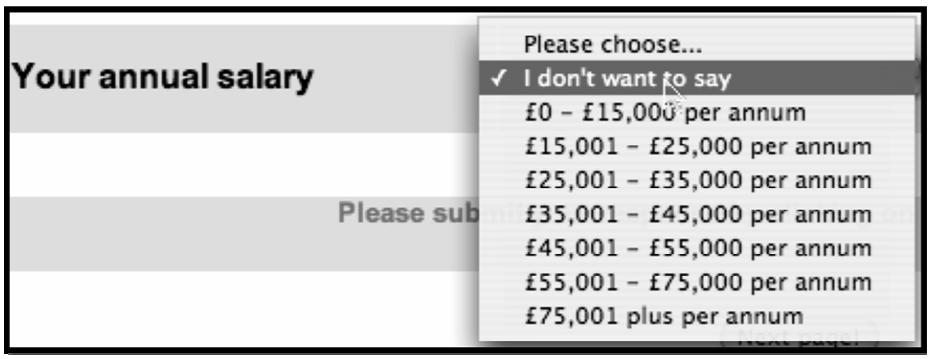

Figure 4. Manipulating default selection, in sensitive ítems to indirectly measure privacy concerns via active and passive non-disclosure.

Alternative Types of Measurement

Apart from using privacy scales, other ways of measuring self-disclosure have been explored. Reips, Buchanan, Joinson, and Paine (2010) systematically studied people's behavioral self-disclosure to web-based forms. These web questionnaires often include sensitive questions, which respondents might prefer not to answer. To avoid answering, users may choose between various strategies of non-disclosure. An *active* strategy results in choosing an option like "I prefer not to say," if available. Following a *passive* strategy means leaving the default option (e.g. "Please choose answer here") untouched. Being motivated to use active and passive non-disclosure strategies is assumed to depend on the sensitivity of the questions asked. For a question about one's income (see example in Figure 4) – a very sensitive question in many cultures – participants were

expected to more frequently use both active and passive non-disclosure strategies than for regular items. Reips et al. investigated in three experiments (Ns of 746, 1075, and 944) how the sensitivity of questions and the design of answer options combine to influence non-disclosure to web-based forms. Type of default selection and location turned out to be of major influence on (non-)response rates to sensitive items. Depending on condition, percentages of participants who non-disclosed ranged from 0 to 34.9%. Due to this large range of non-response, the combined manipulation of sensitivity of questions and the design of answer options seems to be a good alternative to measuring privacy concerns, at least on a group level.

A third possible way of measuring privacy concerns via self-disclosure is described in Joinson, Paine, Buchanan, and Reips (2008). In that paper, "blurring" or increased ambiguity (e.g. answering with „10'000-70'000 €" rather than „25'000-30'000 €") was used primarily by males in response to an income question in a high privacy condition. Furthermore, the use of an "I prefer not to say" option to sensitive questions was again shown to be responsive to the manipulation of level of privacy concern by increasing the salience of privacy issues, and to experimental manipulations of privacy.

Protecting Privacy Online

When doing Internet-based research particular precautions have to be taken to protect participants' privacy (e.g. Buchanan & Williams, 2010). These include measures to avoid collecting personal information and to keep participant data confidential like using secure transmission methods (Reips, 2002). Two developments and recommendations regarding software and steps to be taken by Internet users are described below that may help to better protect privacy online in the future."

Software to Protect Online Users' Privacy

Similar to the creative commons license idea the World Wide Web Consortium (W3C) initiated the *Platform for Privacy Preferences Project (P3P)* It "...enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices

when appropriate. Thus users need not read the privacy policies at every site they visit." (The P3P 1.1 Working Group Note, 2007). The P3P Working Group provides a list of P3P software available from http://www.w3.org/P3P/implementations.html.

The initiative brought together a group of software engineers and decision makers interested in privacy who first met at a workshop in 2002 called "W3C Workshop on the Future of P3P" in Dulles (Virginia, USA) on the Campus of America Online. The workshop materials are still available at http://www.w3.org/2002/p3p-ws/Overview.html. The group notes that there was insufficient support from current Web browser manufacturers for the implementation of P3P 1.1, even though it was ready for it.

As for the usefulness of P3P the group states:

"P3P uses machine readable descriptions to describe the collection and use of data. Sites implementing such policies make their practises explicit and thus open them to public scrutiny. Browsers can help the user to understand those privacy practises with smart interfaces. Most importantly, Browsers can this way develop a predictable behavior when blocking content like cookies thus giving a real incentive to eCommerce sites to behave in a privacy friendly way. This avoids the current scattering of cookie-blocking behaviors based on individual heuristics imagined by the implementer of the blocking tool which will make the creation of stateful services on the web a pain because the state-retrieval will be unpredictable."

Steps to protect one's privacy online

As long as the dream of a "killer app" or software system for privacy protection has not come true (if it ever will be possible), the following steps can be recommended for adjusting one's preferences on social networking sites like MySpace, Xing, Tuenti, and Facebook.

Step 1. In your account settings on the social networking site adjust your password. Swap your existing password for a stronger alphanumeric one. Remove any extra information that is not required, e.g. your maiden or middle names if you included them at registration. Also, you may consider adding some information that really is not true or only half-true, like hobbies that you once had but don't practice anymore.

Step 2. Set your privacy settings, check what you are sharing with whom. If in doubt, then choose the less public option, you can always make changes later. In particular, don't let third parties (like plug-in applications) use your

profile picture in their advertising, which may fool some of your less technology-savvy friends into clicking on unwanted ads believing you somehow invited them.

Step 3. If there are any networks options in the social networking service, then check if you're happy with the sharing settings for any network you may have joined. Consider removing yourself from networks altogether. Also think about unlinking any links you previously established to other services and accounts like twitter, picasa, your personal blog, and so on.

Step 4. If you logged into the social networking site with a mobile phone number, have signed up for any phone-related services linked to the social networking site or listed your number at sign-up, be aware that your phone number will be available for all your "friends" to see (plus networks and possibly advertisers). If you don't want them to call you or send you text spam, alter your settings mobile tab.

Step 5. Check your "friends" regularly. Hackers often seek out a weak link, such as someone who appears to accept friends without really looking at the requests. Having been accepted, the hackers then try to become friends with that person's friends, who assume the newcomer must be ok. In the preferences for your social networking site look for a list of "friends" from which you can purge anyone you don't know well.

Step 6. Do not answer quizzes and tests within social networking services. Most of these request permission to post your answers in your area of the social network (e.g., your Live Feed and your Wall in Facebook). But even if you ignore such requests, commenting on someone else's results could reveal more than you intended to. If you can't resist the temptation to answer a quiz, then again, do not answer everything completely truthfully.

Figure 5 shows Quibble, a service that allows everyone to create quizzes in social networking services. Some of the quizzes here have been answered by tens of thousands or even hundreds of thousands of participants (see "Recently Popular" list in Figure 5). Even though this may be a quick way of gathering data, it is questionable whether the ethics of online privacy is fulfilled with such data grabbing meta services that are not rooted in academic institutions.

Figure 5. Quibble screenshot.

Ethics of Online Privacy

The ethics of online privacy are embedded within general issues of ethics on the Internet. On the Internet, we now see many conflicts arise that will emerge from globalization. Legal and societal values collide on the Internet – for example, it is proper to display swastikas on websites in the USA, but it is not so in Germany. The same website may be legal in one country, and illegal in another. Similarly, for conducting research online, the need and legal status for some practices (e.g. Institutional Review Boards, informed consent, remuneration of participants in the form of raffles) may vary by country (Buchanan & Williams, 2010; Ess, 2007; Reips, 2002, 2007).

A second, very important aspect of online ethics is the Internet's impact on society, in particular in e-commerce. Large companies like Amazon and Google or, lesser known, Akamai, have gathered enormous sets of data from and about human life. "The speed and degree to which e-commerce is infiltrating the very fabric of our society, faster and more pervasively than any other entity in history, makes an examination of its ethical dimensions critical. Though ethical lag has heretofore hindered our explorations of e-commerce ethics, it is now time to identify and confront them." (Kracher & Corritore, 2004). At the root of the new power of e-commerce companies lies users' willingness to provide them with their data, alas to give up privacy.

The online world is a new experience for many, and there is a permanent evolution in technologies. Consequently, users may not understand the implications of their actions. Delio (2002) writes "... many Yahoo customers do not understand the Yahoo privacy policy because they do not understand the new forms of partnerships formed on the Internet." More precisely, "they do not know that the personal information they give at their Yahoo email site is mixed with personal information gleaned from a commercial site affiliated with Yahoo and then sold for marketing purposes." (Kracher & Corritore, 2004). For example, millions of users now use the Voice-over-IP application *Skype* (www.skype.com) for Internet telephony. In this application it is easy to make phone calls that include video contact as well. With a little helper software, *Call Recorder*, one can easily record these communications. Figure 6 shows how easy it is to set up automatic recording, so many users will – often unbeknownst to their call partners – record video messages onto hard disks that may later remain there when the computers are thrown away.

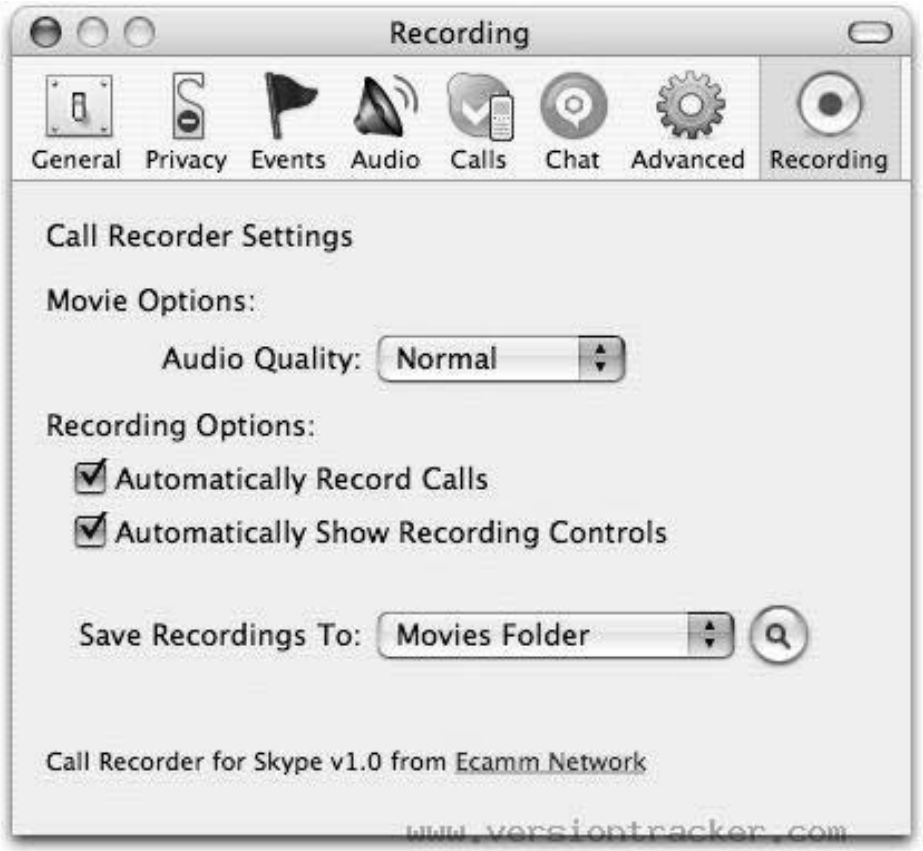

Figure 6. Automatic recording of video calls and calls using Call Recorder in the Voice-over-IP application Skype.

Clicking on a Web application that is seamlessly included with the layout of *Facebook* will grant this application access to all data on the "friends" level, the innermost level with the least privacy protection. The problem of insufficient user knowledge on the technology level is corroborated by too much trust resulting from a higher level of familiarity that user experience online. Paré and Cree (2009) showed that object familiarity was rated higher online than in the laboratory, because the "environment" (Web browser interface) is more familiar online. A feeling of familiarity may become even stronger in social websites, where pictures of friends and family are displayed on the interface. Thus, the danger to reveal (too) much information likely is high in social websites like *Facebook*.

Because many *Facebook* applications recruit new users via the snowball system, these applications quickly gather many data from small social networks.

"X was marked on this picture"

Another privacy problem on *Facebook* and similar is the option (if not invitation) to upload privacy-relevant information about others to the network. Any registered Facebook user can mark people on pictures and enter their names, resulting in a message displayed along with the picture saying "[name] was marked on this picture". It is possible for identifying information to be passed on without an individual's consent. For instance, a user can upload an embarrassing photo of a friend, and this photo can then be tagged directly to a friend's profile. Even people who have never signed up for the service can be tagged and then be found on it by name.

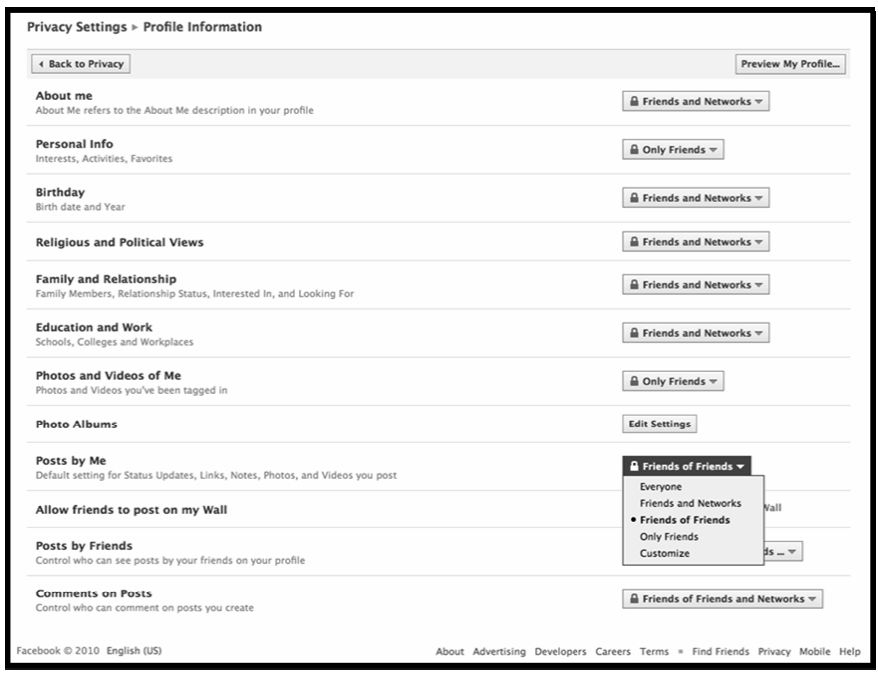

Figure 7. Options for setting levels of privacy in Facebook.

In 2009, and following a lot of complaints, *Facebook* introduced more fine grained privacy settings. Users were now allowed to set the privacy level for

each individual item (see Figure 7, right side) and a clever preview allowed viewing one's pages from another person's perspective (Figure 7, left side). However, these new privacy settings appeared too complicated and difficult to use, as even *Facebook's* CEO seemed to accidentally have opened up access to almost 300 personal photos (Koman, 2009).

"The speed and degree to which e-commerce is infiltrating the very fabric of our society, faster and more pervasively than any other entity in history, makes an examination of its ethical dimensions critical. Though ethical lag has heretofore hindered our explorations of e-commerce ethics, it is now time to identify and confront them." (Kracher & Corritore, 2004).

The Clash of Privacy with Other Values

One of the websites we mentioned earlier, Dontdatehimgirl.com, perfectly illustrates how the need for privacy sometimes clashes hard and directly with other values. Hatcher (2005) writes, the author of the website's aim, "at first, was to provide a public service to women by allowing them to run a background check on men they were considering dating … a forum for women who have been cheated on to exchange ideas, opinions, share their stories and find support." Of course, the database needed to create such a site would then contain many facts, half-truths, and erroneous bits of information about men – all directly invading the men's privacy. So, according to an expert of media law cited by Hatcher the author and users of the website run the legal risk of "being sued for invasion of privacy by the disclosure of private or embarrassing facts".

Again, the British Royal Academy of Engineering (2007) explains very well the general reasons why privacy sometimes cannot be guaranteed and may loose out against other values:

- "accountability for personal or official actions;
- the need for crime prevention and detection and for security generally: our desire to be able to engage in our personal affairs without anyone knowing is always offset against our desire for criminals not to have the same opportunity;
- efficiency, convenience and speed in access to goods or services: this relates particularly to services accessed online, where access might depend on entering personal, identifying information;
- access to services that depend on fulfilling specific criteria such as being above an age limit or having a disability, or being the genuine owner of a particular credit card;
- the need to monitor health risks, such as outbreaks of infectious diseases;

- public and legal standards of behavior which might weigh against some personal choices.

The varieties of privacy and the various values it can be in tension with mean that one cannot appeal to a straightforward, singular right to privacy. Privacy is inherently contingent and political, sensitive to changes in society and changes in technology. This means that there needs to be constant reappraisal of whether data are to be considered private and constant reappraisal of the way privacy dilemmas are handled." (p. 11)

As mentioned before, Introna and Pouloudi (1999) developed a framework of principles that explores the interrelations of interests and values for various stakeholders where privacy concerns have risen or are expected to rise. The framework can be used to navigate the landscape of clashing values and help solving conflicts between the stakeholders' interests, values, and legitimate claims of privacy/transparency being ignored. Introna and Pouloudi use the principles of *access*, *representation*, and *power* to show how they can facilitate the identification of potential privacy and transparency risks.

Privacy issues are on the rise with the continuing development of more and more aspects of life moving online. However, where danger grows the help is also improving. Non-profit organizations begin to monitor the Internet for privacy violations, such as Cotse.net (2009), and legislations become aware of the matter and begin to act.

Privacy Policies: Published and Real

During the 2000s, it became apparent that no major website could exist without a section describing its privacy policy, particularly if the site was collecting data from visitors. If these data were particularly sensitive or for some reason were combined with other data, then such a privacy policy statement was of utmost importance to gain visitor's trust, and for legal reasons. However, hidden in the privacy policy statements one often finds backdoors and sentences that would make it seemingly better to name it "*no privacy policy* statement". The following excerpt is from the TomTom website (http://www.tomtom.com/legal/privacy/), a provider of navigation devices in vehicles and on mobile phones.

"This Privacy Policy outlines the guidelines we have established with respect to the information TomTom collects when you interact with TomTom, such as when you visit our Website, when you use the products and services offered by TomTom, like the TomTom Plus services or TomTom HOME, or when you subscribe to our newsletter or when you call our Customer Support. ..."

In this beginning section TomTom clarifies that it may combine data from several of its services, including continuous location information (driving) and information collected at the Website, e.g. personal information. They move on to state the "using equals accepting" clause, which will not hold in the jurisdictions of several European countries (e.g. Germany). Also, a unilateral "change of privacy rules" clause is introduced. Furthermore, they state that they may move the data to jurisdictions with less protection of privacy – potentially opening the door for the removal of all protection (by moving the data to a country with no established privacy laws). The presentation of these three heavily questionable messages (from the point of privacy protection) are then followed by the request that mirrors the first message: "accept or leave".

"... In accessing the Website or related Communication Channels you accept all the terms and conditions of this Privacy Policy. You also agree that TomTom may amend and/or revise this Privacy Policy at its discretion and you agree to be bound by these revisions and amendments. Your Personal Information may be processed in the country where it was collected as well as in third countries (including the United States) where laws regarding processing of Personal Information may be less stringent than the laws in your country.

If you do not agree with the terms and conditions of this Privacy Policy we request that you immediately cease using and accessing the Website or related Communication Channels as well as the products and services for which you need to provide Personal Information. ..."

Under the subheader "Collection of Personal Information by TomTom" the company then emphasizes the potential benefits for the user that may come from the company's collection of personal data and moves on to a description of the types of personal information that are collected.

"... The Personal Information we gather from you helps us learn about our visitors and customers. We use this information to provide you with our products and services and the products and services of our carefully selected partners, to develop new products and services, to better tailor the features, performance and support of our products and services, and to offer you additional information and opportunities.

We collect Personal Information that you submit to us voluntarily through our Website or related Communication Channels and your use of our products and services. The types of Personal Information we collect are:

If you set up a "MyTomTom" account, we will collect your contact details such as name, address, gender, email address and country as well as, if appreciated, the information you provide us with in order to receive the newsletter of your preference.

If you buy items from our webstore, we will collect your full name, the name of your company (if applicable), your postal address (each for shipping and billing purposes), email address, phone number, and all the information we need to process your payment of the purchase amount.

If you request customer support services for TomTom products and/or services, we will collect Personal Information to enable us to provide such customer support services to you, including your name, mailing address, phone number, email address, and contact preferences. We will also collect other information about the TomTom products you own, such as the serial numbers, date of purchase and information related to a support or service issue, some of which might be Personal Information.

By using a bulletin board or a chat room at our Website, you should be aware that you are sharing all information you post on such bulletin boards or chat rooms with other users, including any Personal Information that you may choose to share. Please choose the information that you share carefully and accordingly. TomTom is not responsible for any use of information you provide on a bulletin board or in a chat room by any third party.

You may also be requested to provide Personal Information about a person other than yourself (for example if you want to purchase a gift for someone and this Personal Information is required for the fulfillment of the delivery of your purchase, or if you use the TomTom Buddies service), such as name, address, email address and/or location data. This Personal Information is used only for the purpose for which you provide it to TomTom.

TomTom may collect Personal Information through surveys for market research purposes to gain a better understanding of our customers, to improve our products and services, and to develop new products and services. The information we collect in such instances depends on the survey, but might include your name, address, age, information about your use of our services and products and the like.

If you request TomTom Plus services such as traffic information, TomTom may collect location data from your TomTom device in order to provide you with the services requested.

If you send us an email to apply for a position with TomTom, we will collect your email address and the full content of your email, included attached files, such as resumes, and other information necessary to process your application. ..."

At the end of this section the company again "smuggles in" a one-sided user obligation, a responsibility to update the collected information at all times:

"... Any Personal Information which you supply to TomTom shall be true, complete and accurate in all respects. You agree to notify TomTom immediately of any changes to your Personal Information via our Website or related Communication Channels. ..."

The privacy policy also contains information on cookies and other "Information Collected Via Technology" that predominantly explains what is happening when these technologies are used. However, hidden in the explanations are statements that data collected via the technologies may be combined with personal information. Also, "accept or leave" messages are reiterated, now in a version that says that things may not work, if one doesn't accept the data collection with the privacy compromise attached to it.

"... This Website uses Cookies to allow TomTom to collect data about the visitors of the Website and users of our service (that we may associate with Personal Information that we have collected from you) and to customise and personalise our Website and related Communication Channels for its viewers. ... If you choose to disable Cookies, some areas of the Website or related Communication Channels may not work properly.

As you navigate our Website or related Communication Channels, certain Anonymous Information may also be collected passively, including your Internet protocol address, browser type, and operating system. We also use Cookies and data like Uniform Resource Locators (URL) to gather information regarding the date and time of your visit and the information for which you searched and viewed. ...

TomTom may gather Anonymous Information from your TomTom device when you are using it or when you are connecting it to a computer by using TomTom HOME. This Anonymous Information may include information on how long it took you to travel certain routes, traffic patterns and on any technical glitches you may have encountered. ..."

The company then briefly states that it will combine the user's personal information with other information it receives from other sources:

"... We may receive Personal Information about you from third parties that provide us with data from their databases. We may add this information to the information we have already collected from you for the purposes described in this Privacy Policy.

... TomTom is entitled to contract third parties to perform its direct marketing activities. TomTom may use your Personal Information to conduct market research, to improve our products and/or services, to provide more responsive customer service and to improve our Website, products and services.

TomTom may provide, distribute or disclose your Personal Information to third parties where TomTom reasonably believes that it is required to do so to conform to legal requirements or litigation, to protect and defend the rights or property of TomTom or other third parties, to enforce this Privacy Policy or act to protect the interests of its users. TomTom is also entitled to disclose your Personal Information for the purposes of national security or other issues of public importance, at TomTom's discretion."

The company then informs the reader that all user information is stored in a central database that is shared by all "TomTom entities", and that these entities may be based in countries within and outside the EU. Furthermore, there is information about anonymization of data and what would happen in case TomTom is bought by another company.

TomTom then restates (in a section ironically termed "Your Choices regarding your Personal Information") its "take it or leave it" policy, reiterating that privacy preferences cannot be changed individually on a service-by-service base. And they conclude with a statement that basically says that user preferences may be ignored even if explicitly stated:

"... Despite your indicated e-mail preferences, we may send you service e-mails regarding our products and services or notices of any updates to the terms and conditions or Privacy Policy. ..."

As can bee seen from this example, companies have a lot of leeway in collecting and handling their client's data, which is particularly troubling for a company that collects continuous location data and combines it with personal data from other services. A privacy policy statement at least provides the clients with information about what may happen.

Resistance

Given that many privacy practices and policies had become more public, more people became aware of the issues and so resistance mounted, in particular with social networking sites, where naturally more personal information is collected and where the user base is very large. In 2009, pressure from non-profit organizations, users, and regulators had mounted so much that *Facebook* decided to implement a new privacy policy. Upon login, each user was provided with information and asked to adjust his or her own privacy preferences following a new set of categories that from then on could also be adjusted in detail, i.e. item by item. However, for many users the options are too complicated, and possible implications of setting the options in a certain way are beyond many users' imagination. Furthermore, some of the information was defined publicly available

by (new) definition: “Your name, profile picture, gender, current city, networks, Friends List, and all the pages you subscribe to are now publicly available information on Facebook. This means everyone on the web can see it; it is searchable.” (Kirkpatrick, 2010).

Following a series of widely published instances of breaches of privacy on Facebook in 2010 that were discovered after Facebook made its changes even the US Senate began investigating the matter. In one of the instances, all e-mail addresses of Facebook users had become visible, even if they had indicated they wanted them to be kept confidential (O’Connor, 2010). In another instance (“Instant Personalization”, the one that triggered action by the senate) changes in third party site integration with Facebook remained unannounced, so users of the social network didn’t even know that instead of opting in they had to opt out of their information being given to Facebook’s business partners. Opsahl (2010) illustrates some of the problems using “cooking” in an article for the Electronic Frontier Foundation, one of the oldest civil liberties groups monitoring issues on the Internet: “Previously, you could list „cooking” as an activity you liked on your profile, but your name would not be added to any formal „Cooking” page. (Under the old system, you could become a „fan” of cooking if you wanted). But now, the new Cooking page will publicly display all of the millions of people who list cooking as an activity. Cooking is not very controversial or privacy-sensitive, and thus makes for a good example from Facebook’s perspective. Who would want to conceal their interest in cooking? Of course, the new program will also create public lists for controversial issues, such as an interest in abortion rights, gay marriage, marijuana, tea parties and so on. But even for an innocuous interest like cooking, it’s not clear how this change is meant to benefit Facebook’s users. An ordinary human is not going to look through the list of Facebook’s millions of cooking fans. It’s far too large. Only data miners and targeted advertisers have the time and inclination to delve that deeply“.

Soon after the series of incidents and changes in Facebook’s privacy policy privacy advocates and political organizations like MoveOn.org began to rally against Facebook’s murky privacy policies and activities, see for example the chart in Figure 8 that was published by MoveOn.org Civic Action (2010).

Figure 8. Chart published by MoveOn.org.

A radical approach to online privacy management is advocated by *Moddr*, a New Media Lab in Rotterdam (http://moddr.net/). The service they offer is called "The Web 2.0 Suicide Machine" (http://suicidemachine.org). It advertises its service as: "Tired of your Social Network? Liberate your newbie friends with a Web2.0 suicide! This machine lets you delete all your energy sucking social-networking profiles, kill your fake virtual friends, and completely do away with your Web2.0 alterego. The machine is just a metaphor for the website which moddr_ is hosting; the belly of the beast where the web2.0 suicide scripts are maintained. Our service currently runs with *Facebook*, *Myspace*, Twitter and *LinkedIn! Commit NOW!*"

Schonfeld (2009) describes the site: "On Facebook, for instance, it removes all your friends one by one, removes your groups and joins you to its own "Social Network Suiciders," and lets you leave some last words. So far 321 people have used the site to commit Facebook suicide." Figure 9 shows the "SNS-Social Network Suiciders" group in Facebook. Users' face pictures are replaced by icons showing a hanging rope.

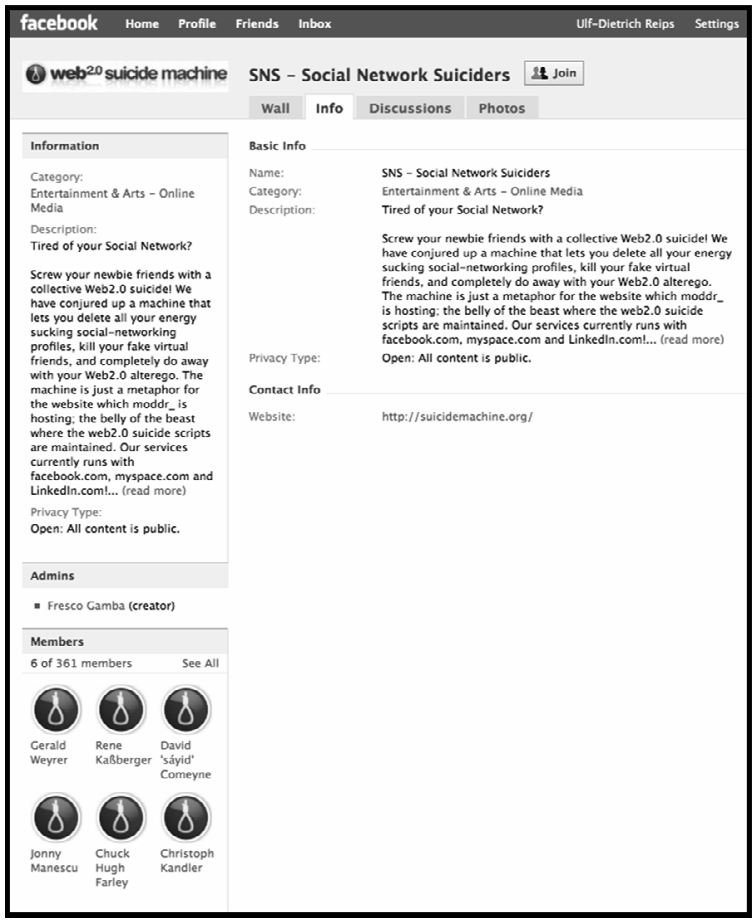

Figure 9. The "SNS- Social Network Suiciders" group on Facebook.

According to McNamara (2010) the site was blocked by Facebook soon after thousands of Facebook profiles had been deleted, and legal action was taken against the art group that started the project.

Future Developments

Privacy issues like identity theft and disclosure of sensitive information on the Internet are particularly on the rise with the increasing popularity of social networking sites such as MySpace, Facebook, Xing, StudiVZ and LinkedIn. Ho, Maiga, and Aimeur (2009) propose a Privacy Framework consisting of four privacy settings or type of data (healthy, harmless, harmful and poisonous) and four privacy levels (best friends, normal friends, casual friends, visitors). The idea is to combine an analysis of subjective privacy preferences with the objective categorization of privacy dangers in social networking sites. However, the nature of privacy issues in networks seems to be built-in. Basically it boils down to the point: "It is important to note that there is no real "Full Privacy" in Social Networking Sites (SNS) because the purpose of SNS is sharing information. If no one is allowed to see user data, there is no reason to use the SNS." (p. 276). Furthermore, harmless data may become harmful if combined, and the status of friends may change.

Consequently, for a long time, there will be significant challenges in the domains of end-user privacy and security management.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179-211. doi:10.1016/0749-5978(91)90020-T

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks/Cole.

Birnbaum, M. H. (2001). A Web-based program of research on decision making. In U.-D. Reips & M. Bosnjak (Eds.), *Dimensions of Internet Science* (pp. 23-55). Lengerich, Germany: Pabst Science

Birnbaum, M. H., & Reips, U.-D. (2005). Behavioral research and data collection via the Internet. In R. W. Proctor & K.-P. L. Vu (Eds.), *The handbook of human factors in Web design* (pp. 471-492). Mahwah, New Jersey: Erlbaum.

Buchanan, T., Paine, C., Joinson, A., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*, 157-165. doi:10.1002/asi.20459

Buchanan, T., & Williams, J. E. W. (2010). Ethical issues in psychological research on the Internet. In S. Gosling & J. A. Johnson (Eds.), *Advanced methods for conducting online behavioral research* (pp. 255-271). Washington, DC: American Psychological Association.

Burgoon, J. K., Parrott, R., LePoire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships, 6*, 131-158. doi:10.1177/026540758900600201

Celeste, S. (2005, October 4). Want to check your e-mail in Italy? Bring your passport. An antiterror law makes Internet cafe managers check their clients' IDs and track the websites they visit. *The Christian Science Monitor.* Retrieved from http://www.csmonitor.com/2005/1004/p07s01-woeu.html

Cotse.net (2009). Cotse.net: Your shield from the Internet. Retrieved from http://www.cotse.net/privacy/

Dandurand, F., Shultz, T. R., & Onishi, K. H. (2008). Comparing online and lab methods in a problem-solving experiment. *Behavior Research Methods*, 40, 428-434. doi: 10.3758/BRM.40.2.428

DeCew, J. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Ithaca, NY: Cornell University Press.

Delio, M. (2002, April 2). Yahoo's opt-out angers users. *Wired News*.

Ess, C. (2007). Internet research ethics. In A. N. Joinson, K. Y. A. McKenna, T. Postmes, & U.-D. Reips (Eds.), *The Oxford handbook of Internet psychology* (pp. 487-502). Oxford, UK: Oxford University Press.

Festinger, L. (1957). *A theory of cognitive dissonance*. Evanston, IL: Row, Peterson.

Fildes, J. (2009, October 5). Phishing attack targets Hotmail. *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/technology/8291268.stm

Frick, A., Bächtiger, M. T., & Reips, U.-D. (2001). Financial incentives, personal information and drop-out in online studies. In U.-D. Reips & M. Bosnjak (Eds.), *Dimensions of Internet Science* (pp. 209-219). Lengerich: Pabst.

Hatcher, M. (2005, September 28). On website. Women identify Cheaters. *Miami Herald,* p. 1, A4.

Ho, A., Maiga, A., & Aimeur, E. (2009). Privacy protection issues in social networking sites. *IEEE/ACS International Conference on Computer Systems and Applications*, 271-278. doi:*10.1109/AICCSA.2009.5069336*

Hurtado, A. (2008, January 22). Buscadores de Internet y privacidad. *El Pais*. Retrieved from http://www.elpais.com/articulo/sociedad/Buscadores/Internet/privacidad/elpepisoc/20080122elpepisoc_2/Tes

Introna, L., & Pouloudi, A. (1999). Privacy in the information age: Stakeholders, interests and values. *Journal of Business Ethics, 22*, 27-38.

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the Internet. In A. N. Joinson, K. McKenna, T. Postmes, & U.-D. Reips (eds.), *The Oxford handbook of Internet psychology* (pp. 237-252). Oxford: OUP.

Joinson, A. N., Paine, C., Buchanan, T., & Reips, U.-D. (2006). Watching me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. *Journal of Information Science, 32(4),* 334-343. doi:10.1177/0165551506064902

Joinson, A. N., Paine, C., Buchanan, T., & Reips, U.-D. (2008). Measuring self-disclosure online: Blurring and non-response to sensitive items in Web-based surveys. *Computers in Human Behavior, 24*, 2158-2171. doi:10.1016/j.chb.2007.10.005

Joinson, A. N., Reips, U.-D., Buchanan, T., & Paine, C. (2010). Privacy, trust and self-disclosure online. *Human-Computer Interaction, 25,* 1-24. doi:10.1080/07370020903586662

Kirkpatrick, M. (2010, January 9). Facebook's Zuckerberg says the age of privacy is over. *ReadWriteWeb*. Retrieved January 11, 2010, from http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php

Koman, R. (2009). Facebook backs off as founder's pictures go public. newsfactor.com. Retrieved Dec. 30, 2009, from http://news.yahoo.com/s/nf/20091212/tc_nf/70579

Kracher, B., & Corritore, C. (2004). Is there a special ecommerce ethics? *Business Ethics Quarterly*, 14, 71-94.

Krantz, J. H., Ballard, J., & Scher, J. (1997). Comparing the results of laboratory and World-Wide Web samples on the determinants of female attractiveness. *Behavior Research Methods, Instruments, & Computers, 29*, 264-269.

Krantz, J. H., & Dalal, R. (2000). Validity of Web-based psychological research. In M. H. Birnbaum (Ed.), *Psychological experiments on the Internet* (pp. 35-60). New York: Academic Press.

Lloyd, R. (1999, August 30). Status of Hotmail privacy unclear. *CNN.com*. Retrieved October 9, 2009, from http://edition.cnn.com/TECH/computing/9908/30/hotmail.06/

Mainelli, T. (2002, May 18). Hotmail policy raises privacy concerns: New view of passport data leaves some customers unhappy with what they see. *PCWorld.com*. Retrieved October 9, 2009, from http://www.pcworld.com/article/100084/hotmail_policy_raises_privacy_concerns.html

McNamara, P. (2010, January 4). Facebook blocks 'Web 2.0 Suicide Machine'. *Buzzblog*. Retrieved January 9, 2010, from http://www.networkworld.com/community/node/49470

MoveOn.org Civic Action (2010). Did you see what Facebook is trying to do? Retrieved May 15, 2010, from http://civic.moveon.org/facebook/chart/index.html?rc=fb&t=1

Musch, J., & Reips, U.-D. (2000). A brief history of Web experimenting. In M. H. Birnbaum (Ed.), *Psychological experiments on the Internet* (pp. 61-88). San Diego, CA: Academic Press.

O'Connor, M. (2010, March). Facebook revealed private email addresses last night. Gawker.com. Retrieved from http://gawker.com/5505967/facebook-revealed-private-email-addresses-last-night

New Scientist (2009, April 25). Online ad targeting system breaks EU privacy rules. *New Scientist, 2705*, p. 17.

Opsahl, K. (2010, April 19). Updated: Facebook further reduces your control over personal information. *Electronic Frontier Foundation Deeplinks Blog*. Retrieved from http://www.eff.org/deeplinks/2010/04/facebook-further-reduces-control-over-personal-information

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65*, 526-536. doi:10.1016/j.ijhcs.2006.12.001

Paré, D. E., & Cree, G. S. (2009). Web-based image norming: How do object familiarity and visual complexity ratings compare when collected in-lab versus online? *Behavior Research Methods, 41,* 699-704. doi:10.3758/BRM.41.3.699

Porter, H. (2009, May 21). Privacy and the net. *Henry Porter's blog, The Guardian*. Retrieved July 3, 2009, from http://www.guardian.co.uk/commentisfree/henryporter/2009/may/21/privacy-and-the-net-facebook

Reips, U.-D. (1997). Das psychologische Experimentieren im Internet [Psychological experimenting on the Internet]. In B. Batinic (Ed.), *Internet für Psychologen* (pp. 245-265). Göttingen: Hogrefe.

Reips, U.-D. (2001). The Web Experimental Psychology Lab: Five years of data collection on the Internet. *Behavior Research Methods*, 33, 201-211.

Reips, U.-D. (2002). Standards for Internet-based experimenting. *Experimental Psychology*, 49, 243-256.

Reips, U.-D. (2007). The methodology of Internet-based experiments. In A. Joinson, K. McKenna, T. Postmes, & U.-D. Reips (Eds.), *The Oxford Handbook of Internet Psychology* (pp. 373-390). Oxford University Press.

Reips, U.-D. (2010). Design and formatting in Internet-based research. In S. Gosling & J. Johnson, *Advanced Internet Methods in the Behavioral Sciences* (pp. 29-43). Washington, DC: American Psychological Association.

Reips, U.-D., Buchanan, T., Joinson, A., & Paine, C. (2010). Internet Questionnaires in e-health contexts: Non-response to sensitive items. Manuscript submitted for publication.

Reips, U.-D., Buchanan, T., & Oostlander, J. (2010). GPCP: A German version of the scale for online privacy concern and protection for use on the Internet. Manuscript in preparation.

Reips, U.-D. & Krantz, J. (2010). Conducting true experiments on the Web. In S. Gosling & J. Johnson, *Advanced Internet Methods in the Behavioral Sciences* (pp. 193-216). Washington, DC: American Psychological Association.

Reips, U.-D., & Lengler, R. (2005). The Web Experiment List: A Web service for the recruitment of participants and archiving of Internet-based experiments. *Behavior Research Methods, 37*, 287-292.

Richter, T., Naumann, J. & Groeben, N. (2001). Das Inventar zur Computerbildung (INCOBI): Ein Instrument zur Erfassung von Computer Literacy und computerbezogenen Einstellungen bei Studierenden der Geistes- und Sozialwissenschaften. *Psychologie in Erziehung und Unterricht, 48*, 1-13.

Schonfeld, E. (2009, December 31). Wipe the slate clean for 2010: Commit Web 2.0 suicide. *TechCrunch*. Retrieved from http://www.techcrunch.com/2009/12/31/web-2-0-suicide/

Strickland, L. S., & Hunt, L. E. (2004). Technology, security, and individual privacy: new tools, new threats, and new public perceptions, *Journal of the American Society for Information Science and Technology, 56*, 221-34. doi:10.1002/asi.v56:3

The P3P 1.1 Working Group Note (2007). Retrieved from http://www.w3.org/P3P/

The British Royal Academy of Engineering (2007). *Dilemmas of privacy and surveillance: Challenges of technological change*. London: The Royal Academy of Engineering.

Vadillo, M. A., & Matute, H. (2009). Learning in virtual environments: Some discrepancies between laboratory- and Internet-based research on associative learning. *Computers in Human Behavior, 25*, 402-406. doi:10.1016/j.chb.2008.08.009

Warren, S., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*, 193-220. doi:10.2307/1321160

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Whitley, E. A., & Hosein I. R. (2008). Doing the politics of technological decision making: Due process and the debate about identity cards in the UK. *European Journal of Information Systems, 17*, 668-677. doi:10.1057/ejis.2008.53

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *CyberPsychology & Behavior, 11*, 615-617. doi:10.1089/cpb.2007.0208