

Internet users' perceptions of 'privacy concerns' and 'privacy actions'

Carina Paine^a, Ulf-Dietrich Reips^{b,*}, Stefan Stieger^c, Adam Joinson^a, Tom Buchanan^d

^a*Institute of Educational Technology, The Open University, Walton Hall, Milton Keynes MK7 6AA, UK*

^b*Department of Psychology, University of Zurich, Switzerland*

^c*Core Unit for Medical Education, Medical University of Vienna, Austria*

^d*Department of Psychology, University of Westminster, Regent Street, London WC1, UK*

Received 17 January 2006; received in revised form 29 November 2006; accepted 22 December 2006

Communicated by E. Motta

Available online 19 January 2007

Abstract

A consistent finding reported in online privacy research is that an overwhelming majority of people are 'concerned' about their privacy when they use the Internet. Therefore, it is important to understand the discourse of Internet users' privacy concerns, and any actions they take to guard against these concerns. A Dynamic Interviewing Programme (DIP) was employed in order to survey users of an instant messaging ICQ ('I seek you') client using both closed and open question formats. Analysis of 530 respondents' data illustrates the importance of establishing users' privacy concerns and the reasoning behind these concerns. Results indicate that Internet users are concerned about a wider range of privacy issues than surveys have typically covered. The results do not provide final definitions for the areas of online privacy, but provide information that is useful to gain a better understanding of privacy concerns and actions.

© 2007 Elsevier Ltd. All rights reserved.

Keywords: Privacy; Internet; Survey Methodology; Instant Messaging

1. Introduction

The Internet forms a part of many people's daily life, from doing the grocery shop, communicating with friends and relatives, through to conducting specialist research, teaching and working. The increased use of the Internet, together with rapid advances in technology, has changed the way in which information about users is gathered, stored and exchanged. Accordingly, concerns about the privacy of Internet users have grown in importance. Academic research and press articles about Internet users' privacy concerns and behaviours appear regularly (e.g. Klein, 2004; Vise, 2005). However, privacy is a changeable concept that encompasses a variety of meanings.

1.1. What is privacy?

There have been many attempts to define privacy. In a legal context, privacy is largely synonymous with a 'right to be let alone' (Warren and Brandeis, 1890). Others have argued that privacy is only the right to prevent the disclosure of personal information to others (e.g. Westin, 1967). Within the psychological literature, Westin's (1967) and Altman's (1975) theories of privacy both feature prominently. Since these earlier theories, many researchers have referred to the difficulties involved in trying to produce a definition (e.g. Burgoon et al., 1989) and despite various attempts to create a synthesis of existing literature (e.g. Parent, 1983; Schoeman, 1984) a unified, single account of privacy has yet to emerge.

This difficulty in producing a single definition of privacy has resulted in multidimensional approaches to defining it. For example, Burgoon et al. (1989) distinguish four dimensions of privacy and define it using these dimensions as "the ability to control and limit *physical, interactional, psychological* and *informational* access to the self or one's group" (Burgoon et al., 1989, p. 132). DeCew (1997) also

*Corresponding author.

E-mail addresses: c.b.paine@open.ac.uk (C. Paine), u.reips@psychologie.unizh.ch (U.-D. Reips), stefan.stieger@meduniwien.ac.at (S. Stieger), a.n.joinson@open.ac.uk (A. Joinson), buchant@wmin.ac.uk (T. Buchanan).

reflects the multidimensional nature of privacy in her definition which consists of three dimensions: *Informational*, *accessibility* and *expressive* privacy.

Technology and the Internet pose unique privacy issues that differ from those previously addressed by privacy research (e.g. Smith et al., 1996). For instance, when doing the grocery shopping online, users may be concerned about whether a retailer stores information about their purchases, and whether this information may be sold to third parties who will then send them unwanted mail. In particular, the more traditional ways of understanding and defining privacy do not account for the unique problems technology has introduced (Solove, 2004). Technology and the Internet requires us to rethink the traditional definitions of privacy: “Technology creates privacy issues that appear to fall outside the bounds of our traditional analysis... we do need to sharpen and deepen our understanding of traditional concerns regarding privacy in order to respond to these new situations” (Austin, 2003, p. 164). For the purposes of this paper, we will assume a *multidimensional view of privacy*.

1.2. Privacy concerns

Central to the definition of privacy is the issue of privacy concern (Westin, 1967). Over the recent years, the concept of privacy concern has been regularly applied to the Internet (e.g. Cranor, 1999) and there have been reports that offline privacy concerns appear to be magnified online (Privacy Knowledge Base, 2005).

Numerous studies have consistently concluded that the overwhelming majority of people are ‘concerned’ or ‘very concerned’ about threats to their privacy while online, and are willing to act to protect it. For example: Harris et al. (1998) reported that 87% of Internet users are ‘concerned’ about threats to their privacy while online, with 56% being ‘very concerned’; Jupiter (2002) reported 70% of American consumers worry about online privacy; Harris (2004) report that 65% of respondents say that they had declined to register at an e-commerce site because of privacy concerns; a PC world survey (2003) of 1500 Internet users found that 88% were concerned about websites sharing their e-mail address, and 91% were concerned about being tracked while using the web; Statistics Canada (2006) reported that 57% were wary of using credit cards online (for recent survey results, see also <http://www.epic.org/privacy/survey/>).

The majority of studies that have examined privacy concerns have been conducted using a survey methodology, where users’ attitudes toward privacy are assessed by asking them to indicate on a fixed scale the degree to which they agree with specific privacy statements. For example, the Internet Users’ Information Privacy Concerns (IUIPC) survey (Malhotra et al., 2004) was designed to reflect Internet users’ concerns about information privacy. Participants are asked to respond to ten items using a 7-point likert scale from *strongly agree* to *strongly disagree* such as

“I’m concerned that online companies are collecting too much personal information about me” and “It is very important to me that I am aware and knowledgeable about how my personal information will be used”. However, surveys such as this tend to make assumptions about privacy. By only allowing users to respond on a fixed scale no additional information regarding the reasoning behind participants’ responses can be gained.

In addition, the majority of studies tend to view privacy as a *one-dimensional* construct, focusing only on the dimension of informational privacy. As indicated previously, privacy is *multidimensional* in nature (Burgoon et al., 1989; DeCew, 1997). Furthermore, these studies also make numerous assumptions about how users perceive privacy: they require responses to a number of specific privacy related concepts—although it is not clear how these concepts were collected, or why they were used. As described in Section 1.1, the concept of privacy is highly complex, therefore, it is unlikely that surveys can accurately reflect respondents’ true concerns.

Harper and Singleton (2001) reviewed 23 privacy surveys and found an almost universal use of questions which prompted for certain results and as such probably distorted or manipulated the responses provided. Harper and Singleton also criticised the surveys they reviewed for not separating ‘privacy’ issues. For example, topics such as security, credit card fraud, spam and any other crimes and inconveniences, were often combined under the heading of ‘privacy’ which makes it difficult to identify precise concerns.

Following their review Harper and Singleton described how the use of an unprompted survey can provide the most accurate data. For example, where respondents are not provided with any response options and are simply asked to list issues of concern to them. Of the 23 surveys they reviewed, only one apparently asked a significant number of unprompted questions about the respondent’s attitudes to online commerce. This was the Harris Interactive/Privacy Leadership Initiative survey (2002) which asked respondents to answer open questions such as why they did not spend more time on the Internet. Respondents’ answers showed little concern with the traditional notions of privacy and more concern for crime issues (e.g. credit card theft), the desire to see the product before buying it, or problems with convenience or selection in buying online.

Finally, as well as concerns about privacy, it is also important to consider any actions people may take to protect their privacy. There is the issue that users who are concerned may take actions to protect their privacy, which in turn could reduce their level of concern.

1.3. The present study

While many studies have measured online privacy concerns, these have tended to focus on only the magnitude of concern, typically requiring responses on a fixed scale to items about violations to informational privacy. However,

given the many dimensions of privacy it is important to take a step back and to investigate what meanings of privacy are involved in the practice of being online and to study people's online concerns in detail. In particular, it is important to detail what individuals are reacting to when asked about privacy concerns online and not to simply assume what users perceive about privacy. Due to the limited opportunity for open responses in the previous surveys conducted in this area, the present study aims to explore Internet users' perceptions of privacy concerns and any actions they take to guard against these by openly asking them.

2. Methodology

The study employed the use of a Dynamic Interviewing Programme (DIP) to survey ICQ-users automatically. ICQ ('I seek you') is an online, real time chat programme from which users can send and receive instant messages. ICQ was introduced at the end of 1996 and now has over 180 million users in all countries (www.icq.com).

DIP was developed by Stieger and Reips (2005, 2007) for automatic online interviewing on top of a freely available ICQ client. DIP randomly selects an ICQ-number from the online address book at <http://www.icq.com/people/>. DIP then sends a chat request to the user's ICQ programme saying "Hello I am DIP. I am an "dynamic interviewing program". I would like to ask you 10 short questions about your online behaviour. Would you like to participate? Please use the options in the brackets. [YES/NO/INFO]". The ICQ user then responds positively by typing "YES" if he or she is interested in participating in the survey (Fig. 1 shows the beginning of a conversation with DIP). If the respondent answers "NO" DIP stops asking. If the respondent types "INFO" DIP responds with the message "Please select one option of the words in brackets if

appropriate or visit my homepage <http://homepage.univie.ac.at/stefan.stieger/dip/> for further information".

DIP can ask two sorts of questions—with or without pre-defined answers required. A question without a set of required pre-defined answers (open format) shows only a minimal set of 'steering answers' in the square brackets: [DECLINE/EXIT/INFO]. Questions that may only be answered with one of the options listed (closed or multiple choice format) are recognisable via the additional possible answers in the square brackets, e.g. [YES/NO/DECLINE/EXIT/INFO].

DIP is able to adaptively choose questions depending on the respondent's answers (dynamic branching), similar to branched testing in diagnostic assessments. This type of sensitive automated interviewing spares the respondent from having to answer superfluous questions (with demotivating effects) and saves time for a deeper investigation of the specific respondent's opinion.

To meet the respondent's need for general information about DIP and the research project a URL is provided at the beginning of an interview. For information about the specific question asked, DIP offers an INFO response option. By typing "INFO" the respondent is presented with a question specific information text that explains the question in more detail. For the earlier questions in the interview respondents were provided with detailed information. For example, when asked "how many hours per week do you use the Internet?" by typing INFO respondents would be told "please type the number of hours you actively use the Internet in an average week, for example "12" if you use the Internet for approximately twelve hours per week". For the later items in the survey, regarding privacy concerns and privacy actions, respondents were provided with only basic information. For example, when asked what their main privacy concerns online were, by typing INFO respondents were simply told to "please detail what

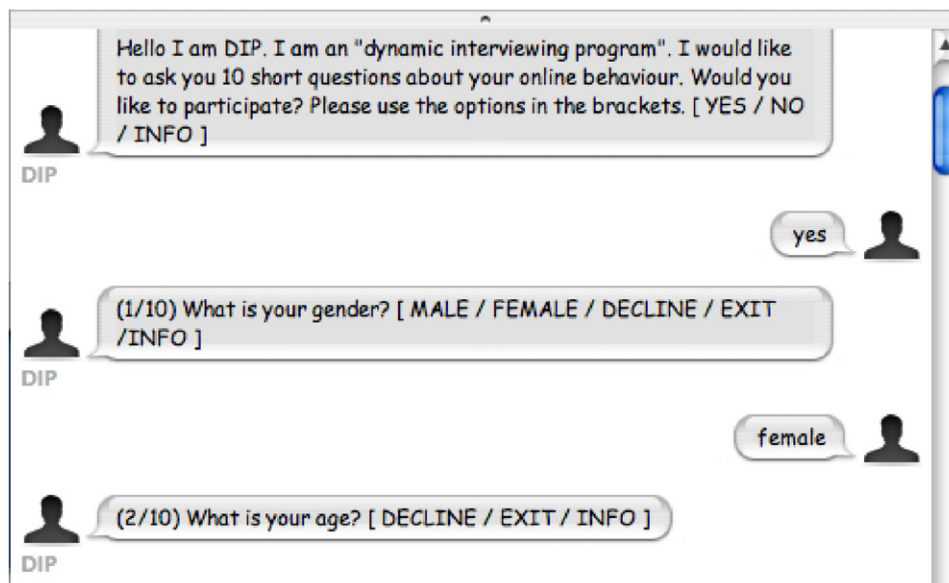


Fig. 1. Beginning of an automated interview via Instant Messaging with DIP (Stieger and Reips, 2005, 2007). (Figure adapted from Reips, 2006.)

your major concerns about privacy are when you are using the Internet". This was to ensure we did not lead respondents with any particular definitions of 'privacy'.

Full details of the response options are shown in Fig. 1. DIP can be accessed and "chatted with" at ICQ number 153155077 (see <http://homepage.univie.ac.at/stefan.stieger/dip/> or via the *iScience Server* at <http://psych-iscience.unizh.ch/>).

2.1. Materials

The questionnaire was developed in order to achieve the aims detailed in Section 1.3. The final version consisted of 10 questions that were a mixture of open, multiple choice and closed formats.

For each question participants were asked to use the response options provided or to answer the open question. Regardless of format, every question included the options DECLINE (for respondents who do not want to answer a

particular question), EXIT (for respondents who want to leave the questionnaire and do not want to return to it later) and INFO (for respondents who need more information. This information is included in the questionnaire design to enable DIP to send tailored information about the particular question). At the end of the questionnaire users were thanked for their time. The complete questionnaire can be seen below in Fig. 2.

2.2. Participants

An interview request was sent to 79 707 randomly selected ICQ users from the online address book at ICQ.com. From 1507 owners of the contacted ICQ numbers came some kind of response. The response rate was 1.9%, with response defined as responding to a minimum of one question. Following data cleaning (described in Section 3.1 below) responses from 530 participants were fully analysed.

Hello I am DIP. I am a "dynamic interviewing program". I would like to ask you 10 short questions about your online behaviour. Would you like to participate?
Please use the options in the brackets [YES / NO]

What is your gender? [MALE / FEMALE]

What is your age?

Which country are you located in right now?

On average, how many hours per week do you use the Internet?

Approximately how long have you been using the Internet?

Where do you most frequently use a computer to access the Internet? [HOME / UNIVERSITY / COMPANY PREMISES / INTERNET CAFE / ELSEWHERE]

Do you have any concerns about your privacy while you are using the Internet?
[YES / NO]

If answered YES
Please outline what your major concerns are

If answered NO
Please outline why you are not concerned

Do you take any action(s) to protect your privacy while you are using the Internet?
[YES / NO]

If answered YES
Please outline some of the actions you take to protect your privacy

If answered NO
Please outline any reasons for not taking action to protect your privacy

Thank you for your time.

Fig. 2. Questionnaire.

Of these respondents, 75.1% ($n = 398$) reported to be male, 22.8% ($n = 121$) reported to be female (missing data = 2.1%). The mean age of the sample was 24.6 years, (range: 12–76 years, $SD = 8.4$). The majority of the respondents (75.3%) were 30 years of age or younger. Although we cannot be sure that the demographics reported by users are correct, Stieger and Göritz (2006) found that in online interviews conducted via different Instant Messaging programs, the false response rate for sex was below 6%. A direct comparison of data from an online questionnaire and data from an online interview of the same respondents showed no difference in sex and age.

Respondents were located in countries all over the world, with the largest number located in Russia (20.6%), followed by Germany (9.2%). The majority of users reported accessing the Internet from a computer at home only (63.8%). About 22.7% reported only accessing the Internet from a computer at their Company premises and 8.7% from both a computer at home and a computer at their Company premises. The remainder of respondents reported accessing the Internet from a computer at university or Internet café or elsewhere (e.g. using mobile phone).

In terms of Internet experience, the mean number of years respondents had been using the Internet was 6.2 years ($SD = 3.9$ years) ($n = 468$). The largest number of respondents had used the Internet for over 5 years but less than 10 years (32.9%). Respondents reported spending an average of 33.2 h/week using the Internet ($SD = 32.0$) ($n = 488$), with the greatest number (38.7%) spending over 30 h a week. Most respondents who had been using the Internet for just 1 year reported spending between 1 and 5 h a week online. Whereas, most respondents who had used the Internet for over 2 years reported spending over 30 h a week online.

3. Results

3.1. Data cleaning

For each question participants were asked, non-responses, selection of the DECLINE option, unrelated responses (e.g. attempts to “chat” to DIP) and inappropriate responses (e.g. swearing, derogatory remarks, complaints) were removed. Respondents’ use of the INFO option was calculated (see Section 3.2) before the remaining responses to each question were collated and entered into a statistical analysis package (SPSS). Responses to closed and multiple choice questions were quantified. Detailed responses for open questions were considered before a smaller set of categories were created by using the terminology employed by respondents. All responses were then sorted into the smaller set of categories.

3.2. Respondents use of INFO

As described, respondents were able to type “INFO” in response to any question in order to gain more information

about that question. In total, 216 respondents used the INFO option at least once, and the majority of these only used it once ($n = 166$). As would be expected, asking respondents if they would like to participate in the survey resulted in the highest occurrence of INFO responses (90 respondents who completed the survey requested further information). When asked the closed item regarding privacy concerns using the Internet, only 27 respondents typed INFO and only 28 respondents responded with INFO when they were asked to detail their concerns in the follow up open item. A lower number of respondents used the INFO response when asked about their privacy actions ($n = 4$ to the closed item and $n = 7$ to the follow up open item).

The remainder of the results section is organised by the questions participants were asked. The number of respondents to each question (written as n) varies throughout for the reasons indicated above.

3.3. Respondents privacy concerns

This section first describes the percentage of respondents who reported being concerned about their privacy whilst online. It then goes on to consider the respondents reported age, gender, Internet experience and location. Statistical tests are conducted to determine whether any differences observed are statistically significant. Finally, respondents detailed privacy concerns are described.

3.3.1. Do respondents have any concerns about privacy while they are using the Internet? ($n = 497$)

The majority of respondents (56%) stated they do have concerns about privacy when they are online. This pattern was true for both males and females. A χ^2 statistical test showed that the relationship between privacy concern and gender of respondent was not statistically significant.

Respondents were split into four groups on the basis of their reported age (20 years and under; 21–30 years; 31–40 years; over 40 years). Fig. 3 shows the percentage of participants who were concerned about privacy online in each of the four age groups.

From Fig. 3 it can be seen that for all age groups above 20 years of age, the percentage of respondents who were concerned about privacy online was higher than the percentage that were not. However, for the age group ‘20 years and under’, a lower percentage of respondents were concerned about privacy online than those who were not. The relationship between privacy concern and the age of respondent was found to be statistically significant [$\chi^2 = 15.144$, $df = 3$, $p < .005$].

There was no difference between those respondents who were concerned about privacy and those who were not concerned when considered in relation to: where they accessed the Internet from; the mean number of hours spent using the Internet per week; or the mean number of years spent using the Internet.

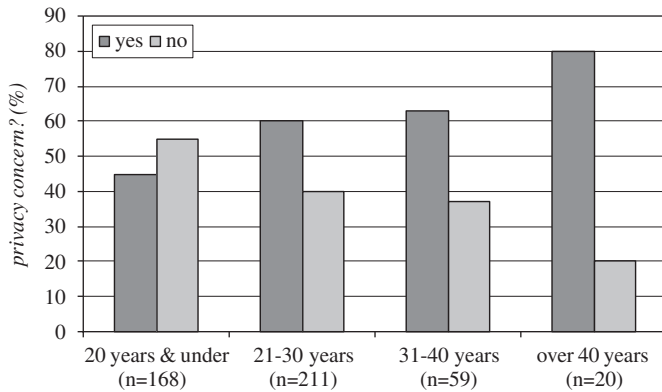


Fig. 3. Percentage of participants concerned about privacy online, organised by reported age.

Finally, respondents were split into groups on the basis of the country they reported being located in. The percentage of respondents who were concerned about their privacy online did not depend on their location.

3.3.2. Statistical analyses

A statistical procedure known as ‘Discriminant Analysis’ was used to enable us to determine whether the information we had about the participants (their age, the number of hours per week they spend on the Internet and the number of years they have been using the Internet) could allow us to discriminate between whether or not they are concerned about their privacy when they use the Internet. A discriminant analysis was performed with *Privacy Concern* (yes or no) as the dependent variable and *Age*, *Number of hours spent per week using the Internet* and *Number of years spent using the Internet* as the predictor variables.¹ Overall, the discriminant function successfully predicted outcome for 57.4% of cases, with accurate predictions being made for 51.2% of users who are not concerned about privacy and 62.1% of users who are.

The results of the discriminant analysis suggest that Age is the best predictor of whether people are concerned about their privacy whilst they are using the Internet, and the older users are, the more likely they are to be concerned.

3.3.3. What were respondents’ major concerns about privacy?

Of the respondents who stated that they do have concerns about their privacy when online, 58% detailed their concerns ($n = 162$). Participants’ concerns were placed into a number of categories which were developed

¹A total of 399 participants’ responses were analysed. Univariate ANOVAs revealed that the privacy concerned and privacy non-concerned differed significantly on the predictor variable of age [$F_{(1,397)} = 11.831$, $p < .001$]. A single discriminant function was calculated. The value of this function was significantly different for privacy concerned and privacy non-concerned [$\chi^2 = 11.937$, $df = 3$, $p < .01$]. The correlations between the predictor variables and the discriminant function suggested that age was the best predictor of privacy concern. Age was positively correlated with discriminant function value.

using the terminology employed by the majority of respondents. The most common concerns listed by respondents are shown in Table 1.

From Table 1 it can be seen that the top two concerns listed were ‘viruses’ and ‘spam’. Respondents also reported that they were concerned about ‘hackers’ and number of respondents simply stated the term ‘security’ as a main privacy concern for them when they are online. Other concerns included people getting ‘access to personal information’ and some respondents specifically used the term ‘Identity theft’.

Although some users were concerned about privacy online, more detailed observations of their open responses illustrated that they were concerned about some issues, but not about others. For example, one respondent stated that they were “concerned about spam and spy ware”, but that they had “very few concerns regarding online financial transactions”.

The respondents who were not concerned about their privacy when online were asked to outline why they were not concerned. About 56% of respondents detailed why they were not concerned ($n = 121$). Participants’ responses were categorized as described above. The most common reasons provided by respondents are shown in Table 2.

From Table 2 it can be seen that the top reason provided by respondents for not being concerned about their privacy online was that they had some information technology (IT) experience and so had already carried out the appropriate actions to protect themselves online. For example, “I know what I am doing”; “I have installed software”. The remaining reasons provided by respondents for not being

Table 1
Respondents main concerns about privacy when online

Common concerns	% of respondents	<i>n</i>
Viruses	16.1	26
Spam	10.5	17
Spyware	9.9	16
Hackers	8.0	13
Access to personal information	6.8	11
Security	5.6	9
Identity theft	3.7	6
Trojan	3.1	5
Deception/honesty	1.2	2

Table 2
Respondents reasons for not having concerns about privacy when they are using the Internet

Common reasons for no concerns	% of respondents	<i>n</i>
IT experience	23.1	28
Not caring	17.4	21
Nothing to hide	15.7	19
Not knowing	11.6	14
Asking ‘Why? Should I be?’	4.1	5
Had no problems before	3.3	4

concerned were simply not caring: “I don’t care, I’m just not [concerned]”. Some respondents were not aware of any online risks, stating they were not concerned about online privacy because they “just chat, nothing else”. The remaining respondents stated that they have “nothing to hide” or that they have not had any problems before: “I’ve never had a problem before, and neither has any of my family members or close friends”.

3.4. Respondents privacy actions

This section first describes the percentage of respondents who reported taking action to protect their privacy on the Internet. It then goes on to consider the respondents’ reported age, gender, Internet experience and location. Statistical tests are conducted to determine whether any differences observed are statistically significant. Finally, respondents’ detailed privacy actions are described.

3.4.1. Do respondents take any action(s) to protect their privacy while they are using the Internet? ($n = 450$)

The majority of respondents (73%) stated that they take actions to protect their privacy when online. This pattern was true for both males and females. A larger percentage of males (75%) reported taking action than females did (68%). This difference between males and females was not shown to be statistically significant.

Respondents were again split into four groups on the basis of their reported age. For all categories of age a higher percentage of respondents took action than those who did not. The relationship between privacy action and the age of respondent was not found to be statistically significant.

The mean hours per week and the mean number of years respondents spend on the Internet was calculated and is shown in relation in Table 3.

From Table 3, it can be seen that respondents who do take action to protect their privacy online spend, on average, a higher number of hours per week online and have also been using the Internet for a greater number of years.

Finally, no differences were observed between the percentage of respondents who reported taking action to protect their privacy and their location.

3.4.2. Statistical analyses

Discriminant analysis was again used to enable us to determine whether the information we had about the participants (their age, the number of hours per week they spend on the Internet and the number of years they have been using the Internet) could allow us to discriminate between whether they took action to protect their privacy when they used the Internet. A discriminant analysis was performed with *Privacy Actions* (yes or no) as the dependent variable and *Age*, *Number of hours spent per week using the Internet* and *Number of years spent using the*

Table 3

Mean hours per week and mean number of years spent online for respondents who reported they do take action to protect their privacy online

Take privacy action?	Mean (<i>SD</i>) hours per week	Mean (<i>SD</i>) years
No	27.1 (28.1) ($n = 110$)	5.4 (3.0) ($n = 102$)
Yes	37.4 (33.5) ($n = 309$)	6.5 (4.1) ($n = 305$)

Internet as the predictor variables.² Overall, the discriminant function successfully predicted outcome for 55.6% of cases, with accurate predictions being made for 56.8% of users who do not take actions to protect their privacy and 55.3% of users who do.

The results of the discriminant analysis suggest that the more hours users spend on the Internet a week, and the more years users have been using the Internet, the more likely they are to take actions to protect their privacy.

3.4.3. What actions did respondents report taking to protect their privacy when using the Internet?

Of the respondents who do take actions to protect their privacy online, 66% ($n = 217$) detailed the actions they take. The actions listed were categorized as described previously. All of these respondents reported using some kind of “software” or “programme”. The most common actions listed by respondents are shown in Table 4.

From Table 4 it can be seen that the top two actions listed were the use of a “firewall” and of some kind of “antivirus” software, some respondents detailed the specific software they use. A number of respondents also reported using Antispam software.

Some respondents stated that they are careful about the amount and type of information they give away when online. For example, they do not reveal their real name, they change it or they use a nickname, and they limit the amount of information they provide: “Not to show e-mail address, phone number and details about me for everyone”.

The respondents who stated that they did not take any action to protect their privacy online were asked to outline why they did not. About 51% ($n = 61$) of respondents detailed their reasons for not taking actions. The most common reasons provided are shown in Table 5.

²A total of 363 cases were analysed. Univariate ANOVAs revealed that the privacy action and privacy non-action differed significantly on the predictor variable of Number of years using the Internet [$F_{(1,361)} = 4.098$, $p < .05$]. Number of hours spent per week using the Internet was marginally significant [$F = 3.583_{(1,361)}$, $p = .059$]. A single discriminant function was calculated. The value of this function only approached significance for privacy action and privacy non-action [$\chi^2 = 6.891$, $df = 3$, $p = .075$]. The correlations between the predictor variables and the discriminant function suggested that Number of hours spent per week using the Internet and Number of years using the Internet were the best predictor of privacy action. Number of hours spent per week using the Internet and number of years using the Internet were positively correlated with the discriminant function value.

Table 4
Respondents' main actions taken to protect privacy online

Action	% of respondents	<i>n</i>
Firewall	42.9	93
Antivirus	37.8	82
Careful about information give away/use nickname etc	9.7	21
Antispam	4.6	10
Work responsible	0.9	2

From Table 5 it can be seen that the most common reason for not taking action to protect privacy online when using the Internet was indifference. For example, respondents stating “I don’t care about it [privacy]”. A large proportion of respondents reported that they did not know how to take action to protect their privacy. Many felt there was no need to, that they were “safe enough”. For a couple of respondents this response was followed up with further information, for example, “it is all done for me by my company”. However, in the majority of cases it was not possible to determine whether respondents felt their was no need to take action because they simply did not feel a need to or because they thought that they were already secure as their work takes action to protect their privacy.

Some respondents appeared to have resigned themselves to the thought that there was nothing that they could do to completely protect their privacy. For example, “well, I don’t publish any very detailed information about me, like address, social security number, but I also realise that any sufficiently determined individual or group can find out pretty much anything they want”.

3.5. Privacy concern and privacy action

Fig. 4 shows the relationship between respondents' privacy concerns and privacy actions.

From Fig. 4 it can be seen that there are four ‘privacy concern-action’ types of respondent. The majority of participants who have privacy concerns take action to protect their privacy when they are online. However, there are a number of respondents who are concerned about privacy but do not take any actions. The most common reason for not taking action provided by this group of participants was that they did not know how to. There was no clear reasoning for the respondents who stated that they were not concerned about privacy but still took action to protect their privacy online.

4. Discussion

4.1. Discussion of results

In the present study, 56% of respondents stated that they were concerned about privacy online. This figure is lower than those reported by studies using a Likert scale response option. For example, the Harris et al. (1998) study reported

Table 5
Respondents reasons for not taking action to protect their privacy online

No action	% of respondents	<i>n</i>
Indifference	31.2	19
Do not know how to	19.7	12
No need	16.4	10
Have nothing to hide	9.8	6
No good/not effective	3.3	2

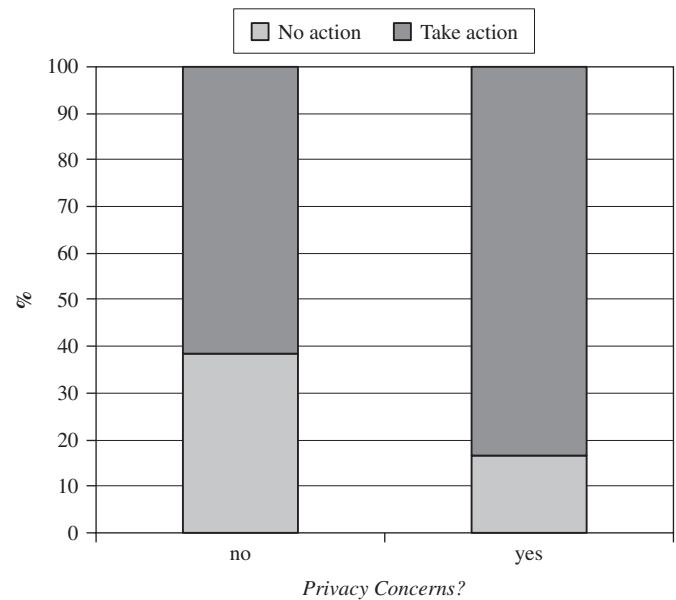


Fig. 4. Relationship between privacy concerns and privacy actions.

87% of respondents, and Jupiter (2002) reported 70% of respondents were concerned about privacy online. The use of an open question format as a follow up to a closed question about privacy concerns in the present study allowed some insight into the reasoning behind participants' responses. Responses to the open question demonstrated that there were very different reasons for users' levels of privacy concern. For example, some users were not concerned due to the fact that they already take action to protect their privacy when online. This may perhaps be a response to the numerous articles in the media about threats to privacy online (e.g. 'Beware the dark side of the net', BBC News, 10th December, 2004). A recent survey by Pew Internet and American Life project (2005) found that nine out of ten US Internet users had changed their behaviour online due to the fear of installing spyware and viruses. In contrast, some users were not concerned simply because they were not aware of any threats to their privacy when they are online. Such responses indicate that there are very different levels of awareness and knowledge of violations or possible violations to online privacy.

In addition, the previous online privacy surveys described (e.g. Harris et al., 1998; Jupiter, 2002) did not mention any participants asking for clarification of the

term ‘privacy’ when they were providing their responses. In other words, all participants responded to questions which included the term privacy without asking for further explanation of its definition. This finding has also been reported by researchers exploring online privacy through semi-structured interviewing and participation-observation methods (Viseu et al., 2004). In the present study, participants also readily responded to the term privacy. This can be demonstrated by the low number of participants requesting more “INFO” when responding to the privacy items.

The privacy concerns reported by respondents covered a wider range of areas than previous privacy surveys usually consider. The detailed responses in the present study indicate that Internet users are not only concerned about informational privacy, even though this is the only privacy dimension they are usually surveyed on (e.g. Harris et al., 1998; Malhotra et al., 2004). The concerns reported in the present study covered all of the different privacy dimensions defined by Burgoon et al. (1989) and DeCew (1997). For example, respondents used terms such as ‘viruses’ and ‘spam’ when asked about privacy concern. However, these terms have not usually been thought of as privacy issues by previous researchers as they do not relate to informational privacy: although Harper and Singleton (2001) acknowledge in their review of surveys that spam is an issue that some may include with privacy, they report that “spam is not in essence a privacy issue, but rather one of inconvenience and annoyance” (p. 6). However, DeCew’s accessibility dimension includes cases where physical access is at stake, for example through intrusions such as spam and viruses. Surveys which require responses to a closed item about privacy concerns should be aware that respondents may be considering the term ‘privacy’ as a wider concept than just informational privacy.

Results also indicated that privacy concerns varied with age, with older respondents being more likely to be concerned about privacy online. The present study does not distinguish between differing uses of the ICQ client. Perhaps older respondents were using ICQ in a more professional manner and were more aware of privacy threats than younger respondents, who could have been using ICQ predominantly to chat to friends. Whatever the explanation it may be important to keep the differences in mind when designing online services where personal data are collected.

In the present study, 73% of respondents stated that they take actions to protect their privacy when they are using the Internet. There are several technologies available to users to protect online privacy, for example firewalls, meta tags to prevent or guide robots, spiders and crawlers on their way through Web sites (Birnbau and Reips, 2005), hiding of IP addresses and anonymizing services (e.g. anonymizer.com). There are also numerous Websites providing advice about how to protect privacy (e.g. the Electronic Privacy Information Centre, 2005). Despite this there was a proportion of respondents who did not take

any action to protect their privacy. Again, the use of an open ended question as a follow up to the closed question about privacy actions in the present study allowed some insight into the reasoning behind participants’ responses. For example, in some cases users did not take action because their company was responsible for this. However, there were a number of users who did not take action as they simply did not know how to protect their privacy online, even though they were concerned.

Results showed that Internet experience was the best predictor of whether a respondent takes actions to protect their privacy online. The more hours a respondent spends on the Internet, and the more years they have been using the Internet, the more likely they are to take actions to protect their privacy. It follows that the more online experience a person has, the more they will know about possible privacy threats, and the more they will know about how to take actions to protect themselves.

When asked about actions, participants again used terms which covered the different dimensions of privacy. For example, terms such as ‘firewall’ and ‘antivirus’ were used. These terms are not commonly thought of as privacy actions. The surveys and literature which have observed users actions to protect their privacy online usually focus on privacy policies and trust marks (e.g. Jenson et al., 2005).

Finally, it was also evident that individuals approach privacy from the context of their own actual practices, associating it with their individual experiences and concerns. For example, “I have had no untoward experience” and “I never experienced a situation in which my privacy on the Internet has been disturbed”. This further supports the finding that Internet experience was the best predictor of whether a user takes action to protect their privacy online.

4.2. Discussion of methodology

The majority of published online privacy surveys have been conducted with Internet users in the United States as respondents. The present study surveys respondents from a wider geographical area. However, as only ICQ users were interviewed our sample is not representative of the Internet population.

An interview request was sent to 79 707 ICQ users and the response rate was below 2%. Such a low response rate may be due to spam filters used in newer versions of ICQ, because many ICQ accounts are silent, and because of the way potential respondents were contacted. Participation was not actively sought for by the respondents, rather they were contacted by DIP. Naturally, many of those contacted did not have time when they were contacted, and some may have not responded in reactance. There were some complaints from users and as such they did not complete the survey. Other users commented that they would not have privacy concerns as high as other users as they were responding to the survey. Perhaps some users did

not respond as they were very concerned about their privacy. For example, one respondent stated “[I have] not as much concern as many others seem to have (otherwise I would ignore this interview)”. Furthermore, respondents were given the option of responding ‘No’ to the request from DIP to participate, if they did so they were then asked if they would like to be contacted again and thanked for their time.

It is worth noting the demographics of the respondents. The largest number of users were located in Russia, followed by Germany. The survey did not include a measure of respondents’ level of fluency in English and therefore it cannot be assumed that all users understood the term privacy. This may partially explain the wide range of responses provided. Ideally, the open ended questions could have been followed up with more specific questions to ensure respondents explained their concerns fully. Further follow up items could also have related to specific online activities. However, it was necessary to limit the number of questions in order to ensure that the motivation level of respondents was kept high and to avoid reduced data quality (Reips, 2000, 2002). Although statistically significant, the discriminant analysis function only successfully predicted outcomes for 57.4% of participants in relation to their privacy concern, and 55.6% of participants in relation to their privacy actions. Undoubtedly there are a number of other factors at work which certainly warrant further investigation.

Future research will employ DIP to run a number of smaller studies which will focus on participants’ privacy behaviours and specific aspects of privacy. In addition, DIP may be used to investigate whether users who are less concerned about their online privacy (as they take actions to protect it) have a realistic view of their level of protection, given the ever changing nature of privacy threats. Research is also currently underway with a different population of Internet users (including an established panel of distance education students and users recruited through online research sites). This research has focused on the interaction between people’s willingness to disclose online and their privacy concerns and behaviours (Paine et al., 2006); how people’s privacy concerns translate to privacy-enhancing behaviours while online (Joinson and Paine, *in press*) and has resulted in the development of Internet-administered scales which measure all dimensions of privacy concern and behaviours (Buchanan et al., 2007).

To summarise, by using an open question format in the present survey we gained a fine grained understanding of Internet users’ perceptions of ‘privacy concerns’ and ‘privacy actions’. The wide variation in responses to all of the items confirms what is frequently asserted in the privacy literature: The significant reach of the privacy debate. It is clear from the responses to the present survey that privacy is considered a multidimensional concept. When asked for an open response, users mentioned concerns and actions from all dimensions of privacy, not just informational privacy. In conclusion, the results of the

present study provide information which is useful to provide a better understanding of Internet users’ perceptions of privacy. These findings will inform the development of future privacy studies by the authors.

Acknowledgements

The work reported in this article was supported by funding from the UK Economic and Social Research Council E-Society Programme (RES-341-25-0011).

The authors would also like to thank the anonymous reviewers for their helpful and insightful comments.

References

- Altman, I., 1975. *The Environment and Social Behaviour*. Brooks/Cole, Monterey, CA.
- Austin, L., 2003. Privacy and the question of technology. *Law and Philosophy* 22, 119–166.
- ‘Beware the dark side of the net’, BBC News, 10 December 2004. Available online at: <http://news.bbc.co.uk/1/hi/technology/4085421.stm>, accessed on 20 June 2005.
- Birnbaum, M.H., Reips, U.-D., 2005. Behavioural research and data collection via the Internet. In: Proctor, R.W., Vu, K.-P.L. (Eds.), *The Handbook of Human Factors in Web Design*. Erlbaum, Mahwah, NJ, pp. 471–492.
- Buchanan, T., Paine, C.B., Joinson, A.N., 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.
- 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 relationship. *Journal of Social and Personal Relationships* 6, 131–158.
- Cranor, L.F., 1999. Internet privacy. *Communications of the ACM* 42, 29–31.
- DeCew, J., 1997. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, Ithaca.
- Electronic Privacy Information Centre, EPIC. Available online at: <http://www.epic.org/privacy/tools.html>. Accessed on 20 June 2005.
- Harper, J., Singleton, S., 2001. With a grain of salt: what consumer privacy surveys don’t tell us. Available online at: http://www.cei.org/PDFs/with_a_grain_of_salt.pdf, accessed on 16 May 2005.
- Harris, 2004. National Survey on Consumer Privacy Attitudes. Available online at: <http://www.epic.org/privacy/survey/>, accessed on 22 August 2006.
- Harris and Associates Inc., Westin, A., 1998. *Ecommerce and privacy: what net users want*. Privacy and American Business and Pricewaterhouse Coopers. LLP. Available online at: <http://www.pandan.org/ecommercesurvey.html>. Accessed on 20 June 2005.
- Harris Interactive, 2002. First major post-9-11 privacy survey finds consumers demanding companies do more to protect privacy; public wants company privacy policies to be independently verified. Available online at <http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429>, accessed on 20 June 2005.
- Jensen, C., Potts, C., Jensen, C., 2005. Privacy practices of Internet users: self-reports versus observed behaviour. *International Journal of Human-Computer Studies* 63, 203–227.
- Joinson, A.N., Paine, C.B., *in press*. Self-disclosure, privacy and the Internet. In: Joinson, A.N., McKenna, K., Postmes, T., Reips, U.-D. (Eds.), *Oxford Handbook of Internet Psychology*. Oxford University Press, Oxford.
- Jupiter Research, 2002. Security and privacy data. Presentation to the Federal Trade Commission Consumer Information Security Work-

- shop. Available online at <<http://www.ftc.gov/bcp/workshops/security/02052011eathern.pdf>>, accessed on 20 June 2005.
- Klein, S., 2004. The privacy debate: this time it's personal. *The Guardian* newspaper, April 26.
- Malhotra, N.K., Kim, S., Agarwal, J., 2004. Internet users' information privacy concerns, IUIPC: the construct, the scale and a causal model. *Information Systems Research* 15, 336–355.
- Paine, C.B., Joinson, A.N., Buchanan, T., Reips, U.-D., 2006. Privacy and Self-Disclosure Online. Work in Progress Paper presented at the Conference on Human Factors in Computing Systems, CHI, Montréal, Canada, April.
- Parent, W., 1983. Privacy, morality and the law. *Philosophy and Public Affairs* 12, 269–288.
- PC world survey, 2003. Available online at: <<http://www.pcworld.com/article/id,112468-page,1/article.html>>, accessed on August 22, 2006.
- Pew Internet and American Life project, 2005. Available online at: <http://www.pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf>, accessed on August 22, 2006.
- Privacy Knowledge Base, 2005. Available online at <<http://privacyknowledgebase.com>>, accessed on 20 June 2005.
- Reips, U.-D., 2000. The web experiment method: advantages, disadvantages, and solutions. In: Birnbaum, M.H. (Ed.), *Psychological Experiments on the Internet*. Academic Press, San Diego, CA, pp. 89–118.
- Reips, U.-D., 2002. Standards for Internet-based experimenting. *Experimental Psychology* 49, 243–256.
- Reips, U.-D., 2006. Computer-vermittelte Kommunikation [Computer-mediated communication]. In: Bierhoff, H.W., Frey, D. (Eds.), *Handbuch der Sozialpsychologie und Kommunikationspsychologie*. Hogrefe, Göttingen, pp. 555–564.
- Schoeman, F., 1984. Privacy and intimate information. In: Schoeman, F. (Ed.), *Philosophical Dimensions of Privacy*. Cambridge University Press, Cambridge, pp. 403–417.
- Smith, J.H., Milberg, S.J., Burke, S.J., 1996. Information privacy: measuring individuals concerns about organizational practices. *MIS Quarterly*, June, pp. 167–196.
- Solove, D.J., 2004. *The Digital Person. Technology and Privacy in the Information Age*. NYU Press, New York.
- Statistics Canada, 2006. Available online at: <http://ca.today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2006-08-16T062630Z_01_N16412854_RTRIDST_0_TECH-MEDIA-CANADA-COL.XML>, accessed on August 22.
- Stieger, S., Göritz, A., 2006. Using instant messaging for Internet-based interviews. *CyberPsychology & Behavior* 9, 552–559.
- Stieger, S., Reips, U.-D., 2005. Dynamic Interviewing Program, DIP: Online interviews via ICQ. Poster presented at General Online Research (GOR) conference, Zurich, March 22–23.
- Stieger, S., Reips, U.-D., 2007. Dynamic Interviewing Program (DIP): automatic online interviews via the instant messenger ICQ. Submitted for publication.
- Vise, D., 2005. Fears over Big Brother stalked Gmail. *The Sunday Times* news paper. Available online at: <<http://business.timesonline.co.uk/article/0,,9075-1879562,00.html>>, accessed on 8 December 2005.
- Viseu, A., Clement, A., Aspinall, J., 2004. Situating privacy online. Complex perceptions and everyday practices. *Information, Communication and Society* 7, 92–114.
- Warren, S., Brandeis, L.D., 1890. The right to privacy. *Harvard Law Review*, 5. Available online at <http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html>, accessed on 20 June 2005.
- Westin, A., 1967. *Privacy and Freedom*. Atheneum, New York.