Guide to measuring privacy concern: review of survey and observational instruments[☆]

Sören Preibusch

Microsoft Research
Cambridge CB1 2FB
England

Abstract

The debate about online privacy gives testimony of Web users' concerns. Privacy concerns make consumers adopt data protection features, guide their appreciation for existing features, and can steer their consumption choices amongst competing businesses. However, approaches to measure privacy concern are fragmented and often ad-hoc, at the detriment of reliable results.
The need for measurement instruments for privacy concern is twofold. First, attitudes and opinions about data protection cannot be established and compared without reliable mechanisms. Second, behavioural studies, notably in technology acceptance and the behavioural economics of privacy require measures for concern as a moderating factor.
In its first part, this paper provides a comprehensive review of existing survey instruments for measuring privacy concerns. The second part focuses on revealed preferences that can be used for opportunistically measuring privacy concerns in the wild or for scale validation. Recommendations for scale selection and reuse are provided.

Keywords: privacy concern, willingness to disclose, information privacy, measurement, scale development, scale reuse, experiments and questionnaires, observational methods, survey research

[☆]Section 3.3 of this article was written while the author was at the University of Cambridge, Computer Laboratory

Email address: spr@microsoft.com (Sören Preibusch)
URL: http://preibusch.de/ (Sören Preibusch)

1. Introduction

The flow of personal information sustains our day-to-day use of the Web. It offers personalised services free of charge and at unprecedented levels of convenience, including search, shopping, and socialising. In electronic retailing, behavioural recommendations drive a substantial proportion of sales (Hess and Schreiner, 2012).

The advent and global-scale uptake of the participatory Web has led to further proliferation and commodification of personal information. Through location-based services, personal data flows permeate our neighbourhoods. Beyond the Web, utility providers or mobile phone operators extract and market customer profiles with the aim of monetising 'big data' (Telefónica S.A., 2012).

In the European Union, three in four consumers agree that disclosing personal information is an increasing part of modern life and necessary to obtain products or services. However, a similar proportion is also concerned they have been asked for unnecessary information in the past and that data they provided to companies may be repurposed (TNS Opinion & Social, 2011).

Concerns about privacy have arisen as a research topic in multiple disciplines, including computer science, media studies, economics and law. In addition, research into the consumer-facing Internet in general has to consider privacy issues at large. A prerequisite for conducting meaningful research into and with privacy attitudes are ways to quantify the latter. The hallmarks of empirical research are repeatability, reproducibility and validity (Maxion, 2011). The first two hinge on the reliability of the measurement instrument, and are a prerequisite for validity.

This article reviews established instruments to measure consumers' privacy concerns at the individual level. Its aim is to guide researchers in choosing reliable survey and observational instruments to gauge a participant's level of privacy concern.

Section 2 briefly establishes the working definition of privacy as used in this article, with a perspective on the implicit conceptualisations used in the various instruments. Those are reviewed grouped by methodology, starting with survey-based instruments (Section 3), and then examining observational procedures (Section 4). Recommendations on how and which scale to reuse are provided in Section 5, along with perspectives on scale validation and development, before concluding.

2. Focus on information privacy

The term 'privacy' is used by academics across disciplines and overloaded in each of those. Thorough discussions of how to understand privacy have been carried out in their own right (e.g., recently Gürses, 2010, Sections 2–3). Within the scope of this article, the working definition echoes the concept of privacy underlying each of the scales reviewed herein.

Tavani (2007) categorises the different approaches by distinguishing between descriptive and normative theories of privacy, and demonstrates how each of these theories has been criticised for being too restrictive or even naïve. Normative theories would often be rights-based, for example as a spatial zone that must not be intruded upon without permission (Tavani, 2007). Descriptive theories understand privacy as a depletable resource, which can diminishes until it is lost (Tavani, 2007). Obviously, both aspects are related but hard to unify. In the debate, they sometimes conflate in the term 'privacy'

The definitions of privacy as non-intrusion ("being let alone") and seclusion ("being alone") build on a spatial understanding of privacy (Tavani, 2007), which was prominently defended by Altman (1975), for instance. With the advent of the Internet, the focus has shifted from spatial towards *information privacy*, although it can be argued that both interpretations have similarities (Margulis, 2003). Amongst the commonalities is the emphasis on controlling or regulating access to the self, and neither considers invasions or violations of privacy in depth. Both theories can be applied at the individual and group levels. They consider privacy a cultural universal despite culture-dependent expression, and acknowledge the potential misuse of privacy (Margulis, 2003). Information privacy would come from the limitation of access to personal information, or arise in the control that the data subject has over information about herself (Tavani, 2007).

Recent approaches by computer scientists to reframe the privacy debate have introduced the distinction between "privacy as hiding" (confidentiality), "privacy as control" (informational self-determination), and "privacy as practice" (identity construction) (Gürses, 2010, Section 2.2), (Berendt, 2012). The first two categories map to the conceptualisation of privacy as limitation and control, respectively, as summarised by Tavani (2007). Privacy as practice refers to the individual's effective ability to define her identity by strategically revealing or concealing data: "Privacy as practice demands the possibility to intervene in the flows of existing data and the [social] re-

negotiation of boundaries with respect to collected data" (Berendt, 2012).

In a similar vein, I have argued for the benefits arising from privacy negotiations at the individual level (Preibusch, 2006). In privacy negotiations, consumers and service providers establish, maintain, and refine privacy policies as individualised agreements through the ongoing choice amongst service alternatives (Preibusch, 2009). These agreements set out which and how much personal data flows and how it may be used or shared further. They overcome the inflexibility of take-it-or-leave privacy notices, which are current corporate practice. In incentivised privacy negotiations, the transaction partners may additionally bundle the personal information collection and processing schemes with monetary or non-monetary rewards (Preibusch, 2009).

When reviewing instruments to measure privacy concerns, this article focuses on information privacy, as opposed to physical privacy, for instance. Information privacy is the most natural to computer-mediated transactions, and it has been the focus of most scales discussed here, whether or not aimed at online scenarios (Buchanan et al., 2007). It encompasses an individual's ability to personally control the collection, use, and proliferation of information about herself (Bundesverfassungsgericht, 1983; Stone et al., 1983). When transacting, consumers selectively disclose personal details. This working definition echoes privacy as informational self-determination (Westin, 1967), and is consistent with the concept of privacy negotiations (Preibusch, 2006).

3. Survey instruments for measuring privacy concern

3.1. Cautious use of surveys

High-profile cases of data misuse, breaches and leaks have raised interest in data protection. Consequently, privacy has become a topic for mass media, where opinion polls are regularly quoted as supporting evidence. "94% of consumers consider online privacy important" is an example of the claims that recently made it into the press (TRUSTe, 2012). This headline was based on a single question within a self-administered online survey. Along with the figure of 40% of respondents who indicate to read a Website's privacy statement, it is likely to be an exaggerated figure that does not translate into actual privacy-enhancing behaviour.

The mismatch between self-professed privacy attitudes and awareness on the one hand and privacy-undermining behaviour on the other hand has been

called the *privacy paradox*. The term was first applied to describe the interplay between privacy and personalisation: consumers want to enjoy the benefits from profiling, but they do not want to be profiled (Kobsa, 2007). More recently, disclosure on online social networking sites has also been described as a privacy paradox (Barnes, 2006). When surveyed about data protection issues, consumers repeatedly report high concerns about their information privacy (The Gallup Organization, 2008). Nonetheless, the online population increasingly engages in online activities deemed privacy-threatening, namely online social networking (Acquisti and Gross, 2006). Similarly, the use of location-based services or enrolment in retailers' loyalty schemes is high.

The privacy paradox is an existential challenge for endeavours to measure privacy concern: why would one be interested in attitudes that do not translate into behaviour? My answer to this is twofold. First, disagreement between the two can be explained as a consumer's rational choice. Second, we have yet to understand how attitudes and behaviour actually diverge.

It remains unclear whether the privacy paradox is an inaccurate interpretation of observable phenomena. As a first example, I consider the case of online social networking. On social networking sites, users share their details vertically with the site operator, and thereby also horizontally with other users. In both cases, users can appropriate returns from disclosing personal data, such as better prospects of finding a job or a romantic relationship. A second example is personalisation, where data disclosure happens mainly vertically. Again, consumers appropriate returns in the form of better product recommendations (Personalization Consortium, 2000, 2005). In both cases, users' benefits may well outweigh their privacy concerns. It can be one's best choice to disclose personal details while still being concerned about privacy. The paradox disappears when interpreting both concern and disclosure as gradual phenomena. The model of a "privacy calculus" (Dinev and Hart, 2006a), for instance, acknowledges the decision to disclose personal information as a fully rational choice in the presence of privacy concerns. Although privacy-related decisions are not necessarily rational, I argue that reports of high privacy concerns can reasonably co-exist with widespread privacy-invasive behaviour.

Our understanding of the privacy paradox is also limited by the paucity of instances, where disagreement between attitudes and behaviour has actually been observed. It is often assumed, but not demonstrated, that concern and disclosure happen within the same population. Sampling biases can explain a seeming paradox: within a population of generally privacy-concerned indi-

viduals, a sub-group with lesser concerns sign up for social networking sites where they maintain open profiles.

Only observational studies provide the opportunity to record stated privacy attitudes and actual privacy-related behaviour within subjects. As an example of information-only transactions, participants provided more information than they had previously stated they would be willing to provide (Norberg et al., 2007). In a shopping experiment, participants who reported high privacy concerns exhibited behaviour that diminished their information privacy (Spiekermann et al., 2001). Still, higher concerns were not observed in conjunction with higher willingness to disclose. A strict paradox could not be observed.

Furthermore, other experiments do not necessarily support the notion of a disagreement between attitudes and behaviour. Individuals with stronger privacy concerns were found to place higher values on privacy in information-only transactions (Grossklags and Acquisti, 2007). Web users who reported higher willingness to disclose personal details were also found to type in their data more freely into Web forms (Malheiros et al., 2013).

It has also been argued that disclosure seemingly diverging from attitudes may be explained by strong beliefs into the confidentiality of disclosed data. Divergence would originate in experimenter trust, framing effects, or deceit by the experimenter (Rivenbark, 2010). It seems that the divergence of users' behaviour from their self-professed privacy attitudes would be an artefact, originating in measuring with an unsound methodology. In refining the methodology, one has to consider a specificity issue. Concern is often measured at a global level, while behaviour is measured at a much lower down level of analysis.

In summary, we acknowledge that privacy attitudes and behaviour do not always agree. The methodological conclusion is to measure both in their own right and with their specific procedures. Preference should be given to experimental procedures when studying privacy behaviour; surveys offer themselves to assess attitudes. Both approaches must be subjected to the same scrutiny of reliability and validity.

To refine or refute the notion of a privacy paradox, there is value in contrasting attitudes and behaviour in a single observational study where surveys complement experimental procedures. Before an experiment, they serve exploratory purposes or help screening a population for suitable participants, for instance if a sample with rather high or rather low privacy concerns is needed. After the experiment, exit-questionnaires—sometimes

called follow-up, especially for field experiments—can establish the demographics of the sample and collect psychometrics to control for confounds. Questions regarding privacy opinions and stated behaviour are regularly included; the instruments are administered computerised or on paper. These survey elements allow comparing participants' actual behaviour in the experiment with their stated privacy concerns. Such studies are indispensable in developing survey instruments for concern that exhibit good predictive power for behaviour. They also promise new instruments for measuring attitudes as a precursor for behaviour.

In reviewing existing instruments for measuring privacy concern, pure survey-based method (Section 3.2) are considered along with observational studies that consider privacy concern a precursor (Section 3.8), and experiments where privacy concerns moderate users' appreciation of privacy (Section 4).

3.2. Scales to measure privacy concern: overview

Any attempt to relate privacy choices to privacy attitudes requires a reliable instrument to measure privacy attitudes and opinions. There are five different approaches to measuring privacy concern through one or multiple question items:

- ask the respondents directly, how much they agree to be concerned about privacy.
- describe one to several scenarios to respondents and ask them directly how much they would be concerned about privacy in each setting.
- assume privacy concern is a latent variable: ask respondents how much they would be concerned about certain practices (or to which extent they agree to be concerned). Privacy concern is not mentioned directly.
- assume privacy concern is a latent variable: ask respondents how much they engage or have been engaged in behaviour deemed privacy-enhancing. Neither privacy concerns, nor privacy are mentioned directly.
- assume privacy concern is a moderating factor. Respondents answer questions regarding behaviour or attitudes; these questions do not evoke privacy but it is assumed that response vary with respondents' privacy concerns.

Unfortunately, privacy attitudes are often asked for in an ad-hoc manner in questionnaires, instead of reusing measurement instruments. Endeavours to create validity-tested privacy scales remain limited, although the recent literature has proposed scales aimed at information privacy and Web interactions. The following is therefore a comprehensive overview scales which were rigorously developed, considering more influential and popular works first.

- the "concern for information privacy" (CFIP) instrument by Smith et al. (1996): privacy concern emerges as a latent variable from other concerns
- an investigation of the dimensions of privacy concern by Sheehan and Hoy (2000): privacy concern emerges as a latent variable from concerns about certain privacy-invasive practices
- the scale of "Internet users' information privacy concerns" (IUIPC) by Malhotra et al. (2004): same methodology as Smith et al.
- an instrument for measuring online privacy concern by Buchanan et al. (2007): concerns about data misuse and misrepresentation, and online fraud
- another instrument for measuring privacy concern about online practices by Earp et al. (2005): same methodology as Sheehan and Hoy
- two scales for privacy concern about (a) someone finding out information about oneself (PCIF) and (b) abusing it (PCIA), by Dinev and Hart (2004): same methodology as Sheehan and Hoy
- an indirect measurement of privacy attitudes by Braunstein et al. (2011): privacy concern as a moderating variable

Although some scales share the conceptualisation of privacy concern, their question items are typically disjoint. Direct comparisons are therefore difficult. In the following section, each instrument is briefly portrayed, highlighting the number, phrasing and scaling of question items, the assumed or confirmed factor structure, and the coding key (if any).

3.3. Details on each reliable scale to measure privacy concern

The first and most influential approach to measure privacy concern has been developed by Smith et al. (1996). Their "information privacy instrument", subsequently called CFIP (concern for information privacy) in the literature, was structured into four sub-scales of three to four items each. These sub-scales were labelled "collection", "errors", "unauthorised secondary use" and "improper access" (Smith et al., 1996). In total, fifteen statements were presented to respondents, such as "It usually bothers me when companies ask me for personal information" (Smith et al., 1996). Respondents indicated their agreement with each of those statements on a seven-point Likert scale anchored in "strongly disagree" and "strongly agree". All items were worded positively. A weighted average is calculated from the response to yield a numeric measure of concern. Averaging over the scores of Likert scale is debatable, because it assumes the scale levels are equidistant. Nonetheless Smith et al. are the only authors to provide any guide on how to compute a numeric score for privacy concern from the responses to the different question items. The scenarios are kept abstract, mentioning "companies" and "computer databases", but no online phenomena, for the scale predates the Web (Smith et al., 1996). Confirmatory factor analysis by follow-up research with a new sample of respondents suggests that all four dimensions of this scale are reliable and distinct (Stewart and Segars, 2002).

Whereas Smith et al. derived the assumed dimensionality of privacy concern from a literature review, Sheehan and Hoy (2000) aimed at exploring these dimensions and relating them to the principles of fair information practices (Federal Trade Commission, 2007). In their scale, respondents were confronted with a series of fourteen potentially privacy-invasive scenarios and asked to indicate the resulting level of privacy concern on a seven-point scale anchored in "not at all concerned" and "extremely concerned" (Sheehan and Hoy, 2000). The structure of the scale is therefore very similar to the earlier approach. However, the scenarios directly involve the respondent's reality and evoke online contexts by revolving around email and Websites (e.g., "You receive e-mail from a company whose Web page you visited.") (Sheehan and Hoy, 2000). Exploratory factor analysis on their survey results indicate that consumers' privacy concerns are influenced by three factors, in decreasing order of generating concern: (1) "control over collection and usage of information", (2) "short-term, transactional relationship", and (3) "established, long-term relationship" (Sheehan and Hoy, 2000). The second factor includes the compensation that the user receives in a specific, context-bound exchange

relationship of data for benefits. The third factor captures an ongoing relationship between a company and its customer, during which communication has already happened.

Interestingly, Sheehan and Hoy do not reference the earlier work by Smith et al. This disregard is symptomatic for the development of scales to measure privacy concern: also the following works implement radically new instruments rather than incrementally improving preceding works. A notable exception is the work by Malhotra et al. (2004) that includes and extends the previously found dimensions. The authors blend the items developed by Smith et al. with a few new items, for instance regarding awareness of privacy practices. In addition, all existing items were rephrased and turned into a Web-context by systematically replacing "companies" with "online companies" (Malhotra et al., 2004). The scale structure is kept. The resulting IUIPC (Internet Users' Information Privacy Concerns) scale revolves around control, collection and awareness of privacy practices.

The instrument by Buchanan et al. (2007) is structurally different and aimed specifically at online deployment. On a five-point scale ranging from "not at all" to "very much", Buchanan et al. ask respondents how much they are concerned about different aspects of privacy; all but the first of the sixteen items are phrased as "Are you concerned. . . ". Information privacy is interpreted broadly and includes topics such as unauthorised access to and various scenarios of misusing data, shoulder surfing, and false representations of one's name. Still, all items clearly evoke online threats ("online", "emails", "Internet") or electronic data storage, and responses were most interpretable when considered as a single factor. These attitudinal items are complemented by two separate six-item scales regarding privacy behaviours in the areas of general caution and IT protection. Respondents indicated often they engage in activities considered privacy-enhancing, such as shredding/burning personal documents or using a pop-up window blocker (Buchanan et al., 2007). The focus on the respondent ("you") is similar to the scenarios used by Sheehan and Hoy, but participants now report the frequency of some past behaviour. Privacy concern according to Buchanan et al. was found to correlate significantly positively with general caution and also with privacy concern as measured according to Malhotra et al..

A much longer, 36-item scale was developed by Earp et al. (2005) to measure respondents' concern about certain, potentially privacy-invasive practices by Websites. A five-point scale anchored in "strongly disagree" and "strongly agree" was used and items similar to the IUIPC: "I mind when a

Web site ..." (e.g., "discloses my buying patterns to third parties"), or "I am concerned about ..." (e.g., "unauthorized employees getting access to my information") (Earp et al., 2005). The scale exhibited good reliability scores and the authors confirmed six factors as dimensions of concern: personalisation, notice/awareness, transfer, collection, information storage, and access/participation (Earp et al., 2005). However, the scale was developed only on a single sample of respondents plus a pilot study, and not validated against other measures of privacy attitudes and behaviour. The authors reused the same scale in 2009, but no reliability metrics were reported.

Another endeavour to develop and to validate an instrument to measure the privacy concerns was undertaken by Dinev and Hart (2004). From the outset, the authors consider privacy concerns related to Web interactions and study the influence of two antecedents, perceived vulnerability and perceived ability to control information (Dinev and Hart, 2004). The thirteen items in the privacy concern scale are inspired by the earlier items from Smith et al. and Culnan and Armstrong (1999). They cover the dimensions of data misuse (PCIA for '*a*buse', e.g., "I am concerned about submitting information on the Internet, because of what others might do with it") and the ability for third parties to learn information about the respondent (PCIF for '*f*ind out', e.g., "When I am online, I have the feeling that all my clicks and actions are being tracked and monitored"). Respondents report their level of agreement with the statements on a five-point Likert scale. Structurally, the scale by Dinev and Hart therefore resembles the IUIPC and the work by Earp et al.. Interestingly, seven of the nine items in the 'finding' (PCIF) sub-scale are constructed on the model "I am concerned that a person can find the following information about:" with a list of data items almost exclusively focussed on offline identifiers, such as current and previous addresses, names, relatives, telephone numbers, and financial or driving records (Dinev and Hart, 2004). This data-centric approach strongly differs from the other scales. Later work by the same authors suggests that the two dimensions PCIA and PCIF are indeed different, but their influence on consumers' self-reported level of information exchange with online services cannot be separated (Dinev and Hart, 2006b). It seems this item battery has not been reused by other authors.

The most recent approach to measure privacy attitudes has been proposed by Braunstein et al. (2011). Their work cannot be seen in line with the previous scales. Instead, it is the first to propose an indirect survey instrument to measure privacy concern, after recognising that aforementioned scales and in particular the use of non-validated questions have led to inflated reports

of privacy concern (Braunstein et al., 2011). The authors start with the observation that privacy-related attitudes and actions are subject to framing: when privacy is made salient, participants report higher concerns. This is undesirable because it limits the reliability of the measurement instrument. As a first innovation, Braunstein et al. trial a new way to measure respondents' privacy concern about exposure of personal digital content, including online calendar, online bank records or Web history (Braunstein et al., 2011). A second innovation is the use of ranking rather than rating the different data items, for respondents to express how keen they would be to have the data recovered after technical failure and subsequent data loss. Unfortunately, rating scales are not used throughout: a fully labelled six-point scale ranging from "very likely" to "never" is used for respondents to report how likely they would be to recover the data item it if accidentally left behind in a restaurant (Braunstein et al., 2011). In being data-centric, their approach is similar to the scale developed by Dinev and Hart, despite the contrast in the data items considered. However, no effort is made to deduce a measurement instrument for general privacy concern. Another drawback of this work are the contrived statistical analyses and the lack of exploration in the structure of privacy concerns, for instance through factor analysis.

In summary, the scale by Smith et al. has been most influential in the literature—by applications and in the development of later scales—followed by its expanded and revamped version by Malhotra et al. and the independent works of Sheehan and Hoy. Amongst the prominent scales, the items by Braunstein et al. and Earp et al. are currently least used, keeping in mind that those were developed more recently. New approaches, such as indirect scales that break out of the commonality of Likert scale item batteries, have been proposed recently, but have not yet reached maturity.

Overall, the little, often non-incremental research devoted to scale development for measuring privacy attitudes neither gives a coherent picture as to what the dimensionality of privacy concerns, or good conceptualisations would be. The change in dimensions from study to study seems influenced by the initial scenarios presented to the respondent population—which may cast a shadow on their validity. All the same, treating privacy concern as a uni-dimensional construct (Section 3.6) seems even less appropriate, and is one of the scale authors' recurring conclusions.

3.4. Reuse of scales to measure privacy concern

Unfortunately, even publicly funded studies rarely make use of the few available scales to measure privacy concerns. A notable exception is the 'Visualisation and Other Methods of Expression' (VOME) privacy survey (Coles-Kemp et al., 2010), which reused the IUIPC scale (Malhotra et al., 2004).

The paucity of reuse is a missed chance to opportunistically re-evaluate the scales' validity. It also makes comparisons across studies more difficult. Instead, even large-scale surveys investigate privacy attitudes in an ad-hoc manner. Most prominently, the Eurobarometer surveys 2008 and 2011 on data protection measure privacy attitudes by simplistic questions such as "Are you concerned or not that your personal information is being protected by these organisations?" (The Gallup Organization, 2008). Most questions solicit yes/no answers to a single item; reliability measures are not reported.

Another example of bad practice is a study from 2001, at a time when validated scales were already available. In an endeavour to analyse Internet users' "online privacy concerns", 1482 respondents answered the question: "In general, how concerned are you about security on the Internet? (e.g., people reading your e-mail, finding out what Web sites you visit, etc.) Keep in mind that 'security' can mean privacy, confidentiality, and/or proof of identity for you or for someone else." (O'Neil, 2001). This was the single question used in the survey to investigate privacy concern. In its verbosity, the question also confounds privacy and security issues. The use of poor measurement instruments that lack reliability and validity leads to pseudo-discoveries (Feynman, 1974). It can also be deemed unethical as it wastes the scientific resource of participants.

3.5. Scale stubs

Although not aiming at developing a new scale, other authors applied the scientific method of scale development with carefully crafted item batteries and reliability tests on the resulting instrument. These works have innovated new items not seen in the previously presented scales, which could be useful for future work.

The PRIME survey on "Privacy and Identity Management for Europe" blended its own questions on data protection attitudes and behaviour with broadly adapted questions from the literature, for instance studies by the British Information Commissioner's Office (Oomen and Leenes, 2008). This study stands out by calibrating privacy concerns against concerns about more general issues such as "quality of health services" or "environmental issues

(e.g. pollution)". This approach has also been taken by Preibusch et al. (2013) but is missing from the scales presented in Section 3.3.

The PRIME instrument consists of three parts: first, it gauges concerns about seven potential consequences of abuse/misuse of personal information on a fully labelled five-point Likert scale; these consequences go beyond financial loss and include aspects such as "Unjust treatment" and "Threat to your dignity" (Oomen and Leenes, 2008). Second, thirteen privacy invasions are enumerated and respondents are asked to indicate their concern. Invasions evolve around actions of other people, by companies, and by the government. Different types of invasions (e.g., prying into personal communications) are not varied systematically by actor, however. Third, respondents are asked to indicate their willingness to provide items of personal information on a fully labelled five-point scale ("very uncomfortable" to "very comfortable"). The 24 data items include name, contact and financial details, special data such as ethnicity or religion, and health details and biometrics (e.g., iris scan). This data-centric approach is similar to Dinev and Hart scale and to Preibusch et al. (2013).

Overall, the item batteries in the PRIME survey 2008 could be used as draft psychometric instrument for privacy concern, although they are not interpreted in that way. Further questions in the study revolve around attitudes towards privacy statements and control over one's personal data. In questions about responsibility of the government, the legislator and companies (e.g., "Organisations should be clearer about what happens with my personal data"), some of those are similar to the scale by Smith et al.

Culnan and Armstrong (1999) aggregated a measure of privacy concern from three dichotomous items (yes/no). They asked respondents whether they had engaged in examples of overt steps to restrict the disclosure of personal information towards an organisation. These actions do not relate to an online context, but to limiting the potential for unsolicited contact (e.g., "Does your household have an unlisted or unpublished telephone number?"). Such action, restricting disclosure or limiting the use of data for targeted marketing, would reflect a concern for privacy Culnan and Armstrong (1999). Similar to the privacy behaviour scale by Buchanan et al., all items are phrased to ask for actual past behaviour rather than intended future behaviour. In contrast, Culnan and Armstrong do not provide tiered but dichotomous answer categories, which may make responding easier and also more appropriate.

Chellappa and Sin (2005) developed a new four-item, seven-point Lik-

ert scale anchored in "strongly disagree" and "strongly agree" to measure privacy concern; they motivate their scale by specific shortcomings of the scale by Smith et al.. Respondents express concerns about sharing data of four kinds: preference information, anonymous information regarding one's IT equipment (e.g., operating system), personally un-identifiable information (e.g., postal code or age range), and finally personally identifiable information (e.g., shipping address). In this respect, the instruments can be seen in line with other data-centric approaches. However, the data items are not enumerated individually and the questions frame each data category—making the questions quite long (e.g., 46 words for the last data category). Chellappa and Sin used this instrument in conjunction with a six-item battery to measure consumers' value for online personalisation; in contrast to Earp et al., these items highlight positive aspects of personalisation.

3.6. Single question instruments

The literature is abound of single-question tactics to measure privacy concern. In contrast to the scale stubs presented in the preceding Section 3.5, the questions given in this section were not developed methodologically. Often used in surveys commissioned by corporate entities, they lack indicators on scale reliability and internal consistency (e.g., Cronbach's alpha).

Reuse of the question items presented in this section is generally not advisable. They should only be reused if shortness is crucial or if comparability with original study is paramount. Consequently, I focus on published questions for which comparability is most likely to be desirable:

- the Eurobarometer 2008, question Q1
- the Eurobarometer 2011, in particular questions Q13, Q26
- "The Data Dialogue", commissioned by Demos (Bartlett, 2012)
- privacy attitudes enquired for "Next Generation Users" (Dutton and Blank, 2011)
- a poll by TRUSTe (2012)

The Eurobarometer is a series of recurring and one-off special surveys into public opinion in the European Union. Data protection has been a topic repeatedly, most recently in 2008 and 2011. Both waves provide a valuable

resource for privacy research: first, the survey is carried out EU-wide, on a representative sample in each participating country. This provides valuable baseline indicators against which one can compare their own sample. Second, and consequently, the survey is translated in the languages of all participating countries, making it unnecessary to costly develop own translations. Third, the entire questionnaire is made available. On the downside, there is often a single question for each aspect of privacy attitudes. In The Gallup Organization (2008), first question every participant is asked is: "Different private and public organisations keep personal information about people. Are you concerned or not that your personal information is being protected by these organisations?". Depending on the country, this question has exhibited low discriminatory power. In Germany, for instance, 86% of respondents indicated they were very of fairly concerned (The Gallup Organization, 2008).

In TNS Opinion & Social (2011), there was no directly equivalent question regarding privacy concerns. The much longer survey focussed on privacy and data sharing behaviour on social networking sites, as well as on identity management on the Web. Further questions probed data handling by the government and by companies. Most closely related to privacy concerns, participants were asked in question 13: "Nowadays, cameras, cards and websites record your behaviour, for a range of reasons. Are you very concerned, fairly concerned, not very concerned or not at all concerned about your behaviour being recorded...?", enumerating six 'spheres': on the Internet, in public, on private, via mobile Internet, via payment cards, and via loyalty cards (TNS Opinion & Social, 2011). And in question 26: "Companies holding information about you may sometimes use it for a different purpose than the one it was collected for, without informing you (e.g. for direct marketing, targeted online advertising). How concerned are you about this use of your information?"

Representative samples were also recruited by other large-scale surveys. Most recently, in Great Britain, "new pattern of Internet use" were investigated by surveying a nationally representative sample (Dutton and Blank, 2011). Further, Demos (2012) commissioned "The Data Dialogue", a survey of more than 5000 British Web users, which would also generalise to the general population. In the United States, TRUSTe 2012 asked an existing online panel about basic privacy attitudes.

Amongst those three, the Data Dialogue by Bartlett (2012) is the most advanced survey. It included data-centric questions ("To what extent do you regard each of the following pieces of information about you as personal or

impersonal?", spanning preferences and interests, contact details, and sensitive data) as well as the ability for respondents to express their amount of concern about twelve data usage practices (e.g., companies or government losing or selling data, unsolicited telephone calls or email, cross-border data flows). On the one hand, this question is valuable in paralleling data usage by corporate and governmental entities. On the other hand, all items describe a priori undesirable practices, such as companies using data without permission or the government losing one's personal information. The absence of desirable data usage makes the instrument prone to overstated concerns. In another question in the same survey, participants expressed the extent to which they were "comfortable with [their] data being used" in various privacy-invasive manners (e.g., supermarket loyalty scheme, location-based applications and offers, or banner advertisements) (Bartlett, 2012).

An investigation in emerging usage patterns amongst British Web users gauged privacy attitudes through a three-item question. Respondents expressed their agreement with: "People should be concerned about protection of credit card details", "People should be able to express their opinion anonymously on the Internet", and "The use of computers and the Internet threatens privacy" (Dutton and Blank, 2011, question QB1). The first two items are exceptional in soliciting respondents' expectations about normatively appropriate privacy attitudes rather than their own privacy attitudes. These two do not necessarily coincide; this item battery may not validly measure privacy concern but rather perceptions about desirable levels of privacy concern.

TRUSTe (2012) conceptualised privacy concern as the importance one places on online privacy, similarly to the 2008 Eurobarometer. A question later in the survey asked whether respondents had ever "stopped doing business online with any companies or stopped using their websites because of privacy concerns" (yes/no) (TRUSTe, 2012).

The TRUSTe survey was administered to the Harris Interactive online consumer panel. Harris also supported the privacy indices proposed by Westin (1991), who measured privacy concern by two or three question items, some of which were reverse-coded. Based on their answers, respondents were then assigned to one of three privacy types. Despite numerous shortcomings of Westin's segmentation of users by privacy concern, the underlying questions continue to be used widely (Malheiros et al., 2013). In the light of volatile phrasing across the several survey waves and given their patchy documentation, reusing Westin's question should best be avoided, or at least

combined with an alternative instrument.

Finally, early research into Web users' privacy concerns was carried out by Ackerman et al. (1999). They considered concerns about persistent identifiers and identifiable information, unsolicited communication and Web browsers automatically submitting personal data. However, the authors do not share the original wording of their questions and the scenarios they used. Without guesswork into their methodology, reuse is therefore not possible.

3.7. Disclosure and preferences beyond information privacy

Well before the study of information privacy and the measurement of concern about it, scales were developed to measure preferences for privacy as a broader concept. These scales conceptualise privacy according to original definition by Westin (1967), and revolve, for instance, around solitude, intimacy and anonymity. Marshall (1974) constructed and validated a 56-item Privacy Preference Scale (PPS), differentiated by sex and age, with sub-scales around six factors: intimacy, not-neighbouring, seclusion, solitude, anonymity and low self-disclosure (i.e., reserve). The work by Marshall sparked critical responses and other endeavours to develop privacy scales. A concise overview is given by Margulis (2003, p. 414).

Although these scales pre-date the Web, their extensive study could make them useful for investigating privacy concerns today. Because the scales were originally conceived as a stand-alone instrument, their length would be prohibitive for including them in an exit-questionnaire, for instance. As far as I am aware, the literature on privacy on the Web has not made use of the Marshall scale and its successors.

The last factor in the Marshall scale, self-disclosure as the flip side of privacy, was partly motivated by earlier works by Jourard. Disclosure of personal information is traditionally measured with the scale by Jourard and Lasakow (1958), that investigates willingness to share opinions, intimate details and other potentially embarrassing details. An abridged, 21-item version was developed later (Jourard, 1971), and is widely used. There are also two ten-item open-source scales to measure self-disclosure with good reliability (IPIP / Oregon Research Institute, 2012, AB5C and RD3). In contrast to observing disclosure behaviour (Section 3.8), these scales measure disclosure as a latent variable.

3.8. Observed disclosure as a measure of privacy concern

As a complementary approach, information privacy concern is measured in its role as an antecedent for willingness to disclose items of personal data (Mothersbaugh et al., 2012). This procedure builds on earlier findings that users with high levels of concern about information privacy are less willing to divulge personal details (Son and Kim, 2008). They adopt two types of privacy-enhancing behaviour: refusing to provide data or falsifying their details.

There is a standard experimental procedure in the literature that uses compliance with personal data requests as a proxy for privacy concern: first, participants are subjected to a Web form that asks for various personal details. This Web form is part of a primary task that participants have to complete during the experiment; its design is as close to a commercial Web form as possible. Consequently, it includes standard fields such as name, date of birth or age, gender, email and street address. Second, a university-branded follow-up questionnaire investigates whether participants used any avoidance strategies, such as lying or withholding their data. There is a clear break between the two phases. Assurances of confidentiality and the change in the interacting party (company versus researcher) make it easier for participants to admit lying about their data.

Horne et al. (2007) used an eleven-item Web form made up from the standard items plus weekly spending and consumption of alcohol, fast food and tobacco (all of which ranged in the lower half by percentage of respondents who falsified that information). Based on their disclosure strategies, three clusters of users were identified: half of the participants tended to provide data truthfully; the remaining are split between omitting and falsifying their details Horne et al. (2007). The authors also measured privacy concern with two items; no details were provided on the items used. There was no differences in concern across the three clusters.

Metzger (2007) used a much longer form with 23 items that also asked for preferences and profile data (e.g., preferred Website, music, political party, hobbies) and socio-economic status (e.g., income, household size, education level) on top of the standard details. All items but name and address were optional. Disclosure rates and falsification rates were interpreted as indicators of privacy concern. Again, there was no evidence that disclosure behaviour correlated with privacy concern as measured by a conventional yet unspecified survey instrument.

Malheiros et al. (2013) measured the amount and truthfulness of personal data disclosure on an all-optional Web form asking for name and demographic details, but also for financial details (e.g., income, debt situation, weekly spending, credit card count) and for family details (e.g., marital status, number of children, number of relatives who died during one's childhood, duration of the longest relationship). The follow-up questionnaire asked for truthfulness in the disclosure and included a separate instrument where respondents rated 36 only partially overlapping personal data items by their willingness to disclose them. The average willingness to disclose was significantly negatively associated with the actual number of data items disclosed (Malheiros et al., 2013). No significant association was found between users' disclosure behaviour and their privacy score after Westin (Section 3.6).

In summary, online populations can be segmented by their observed disclosing behaviour. Even when the overlap in data items is little, actual disclosing behaviour correlates well with the aggregate stated willingness to disclose a range of data items where traditional survey instruments for privacy concern fail to explain user behaviour (Malheiros et al., 2013). This indicates that data-centric stated willingness to disclose could be a valid measurement instrument for information privacy in its own right. So far, authors of such procedures try to include items with varying levels of sensitivity, have not done scale development to elicit which data requests are most discriminatory.

The good predictive power of stated willingness to disclose may be attributed to it mirroring the actual disclosing scenario: the Web form remains the most prevalent way of asking for personal details online (Preibusch et al., 2012). It implements a privacy invasion where privacy concern should moderate disclosure behaviour.

As an observational method, Web forms can be applied to field and lab studies alike, as part of an experiment or in a survey. Mechanisms building on Web forms can even be integrated into the sign-up phase of a study. Integration is inexpensive, easy, and compatible with participants working on their primary task. Respondents may not even become aware a given Web form fulfils research purposes—which is good for external validity but requires stringent ethics oversight. Provided participants know that completing certain fields in a Web form is voluntary, their completion behaviour gives an account of trade-offs they make regarding privacy, effort (time, typing, potential follow-up questions), and actual or perceived benefits from answering (Preibusch et al., 2012). Web forms allow high-resolution, oppor-

tunistic observation of privacy concern indicators; further observational and opportunistic methods are discussed in the following Sections 4.2 and 4.1 respectively.

4. Observational procedures and revealed privacy concerns

4.1. Observational procedures

Beside users' attitudes reported on survey instruments, their observed actions can be used to infer their level of privacy concern. This section highlights some experimental mechanisms in which consumers are subjected to choice scenarios that provide an indication about their privacy preferences and concerns. The overarching idea is to measure how much a user must be compensated to accept an invasion of privacy, or how much a user would be willing to spend to improve her privacy. These two metrics correspond to willingness to accept and willingness to pay. Although it has been argued that both price levels would diverge, they vary concordantly. A higher monetary appreciation of privacy is positively associated with higher privacy concerns.

The design of methodologically sound experiments into privacy-related behaviour is hard. Only incentive-compatible experiments that make users expose their true preferences can be used to learn their privacy concerns. Consequently, studies with hypothetical privacy choices must be discarded. They suffer from low reliability issues similar to single question survey instruments. The remaining procedures fall into two camps, depending on the exchange relation: first, experiments in which a consumer reveals personal information in exchange for money; second, exchanges of personal information, money, and goods or services.

Regardless of the exchange relationship, that is, whether or not a product is exchanged in addition to money and data, researchers can gauge users' valuation of privacy in two ways: making participants choose between a menu of fixed pecuniary amounts for a given invasion of privacy; making participants name their price for the privacy invasion. Both approaches can be implemented succinctly and explained easily to participants. They are therefore well-suited for complementary use in the context of a larger study. Still, the latter mechanism provides richer data. It can be implemented as an auction, in which participants have an incentive to truthfully report their valuations (Carrascal et al., 2011; Cvrcek et al., 2006). As users choose their own price points, there is a continuum of cardinal responses instead of frequency counts on an ordinal scale.

Amongst the auction mechanisms, the recent work by Carrascal et al. into valuing the privacy of browsing behaviour is most interesting. Participants installed a browser plug-in, which invited them at intervals to place a bid for selling personal information relating to the Website they currently viewed (Carrascal et al., 2011). In addition, bids were also solicited for various items of personal information detached from a browsing context. This procedure can be added easily to other studies.

Auction mechanisms reduce the transaction on a money for information exchange. Such transactions rarely happen on the Web, but instead the data exchange complements the consumption of goods and services. Experimental results regarding such composite transactions have been found to generalise well from the laboratory into the field (Jentzsch et al., 2012). However, this stream of research is relatively small (Hess and Schreiner, 2012).

There are three experiments reported in the literature that observed privacy concerns in Web shopping scenarios. Tsai et al. (2007) consider consumers' trade-offs as they choose between competing sellers for the same good. Sellers differ by price and privacy; there are innocent and sensitive products (e.g., batteries and a vibrator, respectively). Beresford et al. (2012) gave participants the choice between to DVD retailers that differed in the sensitivity of the personal information collected: the privacy-invasive shop asked for income and mobile phone number instead of favourite colour. Depending on treatment, it was one euro cheaper. Jentzsch et al. (2012) invited participants to shop for cinema tickets. Tickets could be bought from two retailers and were half a euro cheaper with the shop that asked for mobile phone number in addition to the common details (full name, email address, and date of birth). So far, all three experiments have exclusively used fixed monetary values for an invasion of privacy.

Recently, Preibusch (2013) measured Web users willingness to pay for various privacy-enhancing features in a Web search engine; different treatments explored varying prices for privacy. On average, 15% of participants spent money on privacy protection; the demand for privacy went up significantly when search tasks related to sensitive topics. An exit-questionnaire established participants privacy preferences and self-assessed importance of the privacy features on trial; neither of those attitudinal responses were systematically associated with actual spending on privacy (Preibusch, 2013).

Most importantly, any exchange needs to be executed according to participants' choices: they need to provide the data, be subjected to differential payoffs, and receive the goods or services if applicable. If the exchange is

not effectuated, participants are deceived and the instrument is invalidated. It degenerates to a hypothetical choice. Best practice for scale reuse also applies to the reuse of experimental designs: the parameters of the experiment (payoffs, type of goods, data items) should only be changed to account for cultural differences. This encompasses different currencies, different price levels depending on spending power, and the choice of products with a relevance and sensitivity similar to the original culture. An overview is given by Harkness (2010, chapter VII).

Fulfilment of exchanges can require substantial effort, resources and budget. In the experiment by Carrascal et al. (2011), for instance, participants' median bid value across data categories was 25 euro for context-independent data and 7 euro for context-dependent data, that is when bids were placed while a Web page was viewed. In their experiment, Jentzsch et al. (2012) sold more than 350 cinema tickets.

In summary, using experimental procedures to ascertain the level of privacy concern promises high levels of external validity. This advantage has to be weighed against two major drawbacks: first, experimental procedures require more work and time than survey instruments. This holds for both the researcher implementing the experiment and for participants who take part, resulting in longer sessions. Second, experimental procedures are more expensive than survey-based approaches. Some research questions can be answered using crowd-sourced and online experiments, which alleviates the costs, time spent, and student-biased samples (Malheiros et al., 2013).

4.2. Revealed privacy preferences

Privacy-related behaviour can also be observed as part of naturally occurring online interactions. In contrast to an experiment, a manipulation or intervention may not be necessary. Through their browser settings, for instance, Web users exhibit how much they are concerned about data protection and security. Arguably, browser settings may not be self-chosen but recommended by a privacy-aware peer, such as an IT-literate relative configuring the computer or a system administrator. Still, such peer influence ultimately impacts upon privacy attitudes so that revealed settings and attitudes converge (Lewis et al., 2008).

Browser settings of particular interest for inferring privacy concerns include the following:

- an activated 'do not track' (DNT) header in the HTTP request (Fielding and Singer, 2012), unless this setting comes by default (Lynch,

2012)

- acceptance of third-party cookies
- privacy-enhancing browser add-ons, such as the NoScript Firefox extension (Mowery et al., 2011)
- evidence of a user enabling private browsing (Aggarwal et al., 2010)
- evidence of privacy-enhancing user intervention outside private browsing, such as manually deleting cookies or purging the history of visited sites
- browser configurations to always deny API data requests for location or similar capabilities (e.g., address book contacts)
- settings relating to secure connections (e.g., disabled SSL 2.0)

Browser settings are available for field studies, but not in the laboratory. Unless participants bring their own devices to the experiment session (e.g., Krol et al., 2012) or are invited to re-configure the installed machines, the settings applied by the laboratory administrator will be used for all participants. Crowd-sourced experiments have delivered evidence that the choice of the Web browser (e.g., Internet Explorer or other) can be systematically associated with online disclosing behaviour (Preibusch et al., 2012).

5. Recommendations and critical review

5.1. General recommendations on scale reuse

Unless it is the express objective to develop a new scale, an established scale should be reused whenever possible (Jenkins and Solomonides, 1999). In my own studies, reused scales performed typically well and delivered good discriminatory power. Reuse has a threefold advantage: first, it is good academic practice and advances the state of the art to build on prior work. Second, reuse makes high-quality available to the current research. Established scales have been scrutinised and re-validated by researchers other than the original authors. Third, reuse spares the researcher from developing her own measurement instrument. The time saved by building on previously developed scale can be better spent on the original contribution. As pragmatic considerations, an ethics committee / institutional review board and

academic reviewers are rightfully more inclined to approve reused scales than self-devised instruments. It also helps the reader who can look up the details of the measurement in the original work, where those can be laid out much more prominently.

The known deficiencies of existing, well-developed scales are generally more acceptable than the unknown weaknesses in reliability and validity of an ad-hoc measurement instrument for privacy concern. It is the onus of anyone who does not use a pre-established scale to demonstrate that one's own approach delivers high-quality empirical evidence. For the opportunistic measurement of privacy attitudes, this would often be a prohibitively high burden that goes beyond the constraints of a paper.

In reusing a scale to measure privacy concern, one should:

- choose carefully the scale one wants to reuse. The following Section 5.2 gives guidance on which scale to use;

- refrain from changing the scale unless there are good reasons for it. Items should not be altered (re-ordered, removed or added) to an established scale, and scale levels and their anchoring should also be kept unchanged. The scales reviewed here refrain from using colour or interactivity and such elements should not be added. All the same, scale reuse does not preclude adaptations, for instance in the wording, terminology or item order. Indeed, enabling adaptation has been a driver in creating a repository of reusable scales (Goldberg et al., 2006). But changes may invalidate the pre-established reliability and alterations mandate re-establishing reliability and demonstrating that the changes have improved the scale;

- establish translational equivalence when reusing the scale in another language (Maneesriwongul and Dixon, 2004). Unify two independent forward translations, which is then backward translated into the original language of the scale. A native speaker checks for semantic equivalence. Sometimes, the original scale authors also provide translations;

- combine an established scale with an independent new measurement instrument if it necessary to cover new aspects. Subject to the length restrictions of the overall survey, one may combine scales of different levels of maturity. This can be helpful if an unreliable instrument must be reused to maintain comparability with other studies;

- calibrate reported privacy concerns within the population and against concerns about other, more general issues. Examples of calibration questions can be found in Oomen and Leenes (2008) and Preibusch et al. (2013);

- re-assess and report reliability indicators for each reuse and compare them against the original metrics;

- exercise common best practice in survey research. Pretesting / piloting also applies to reused scales. Ensure good usability for the survey in which the instrument is reused. When reusing scales in unsupervised environments, including self-administered in a laboratory setting, add attention probing and check answers form straightlining and speeding.

5.2. Recommendations for choosing which scale to reuse

In addition to how to reuse a measurement instrument for privacy concerns, I provide the following recommendations on which instruments to build on:

- Actual behaviour is best studied with experimental or observational methods. Survey instruments measure attitudes and opinions—for instance concern.

- Survey instruments can be complemented by observational methods, which must be subjected to similar quality checks. A good observational procedure can complement a survey, provided that (a) one has enough resources and (b) it puts no undue burden on participants. Observation of Web form filling behaviour is an inexpensive measure for users' disclosing behaviour. More expensive, but still manageable, are information-for-money exchanges with user-supplied price tags for their personal data.

- Observed Web form filling and lying behaviour is easily complemented with survey questions into the willingness to provide various personal data items. All of such methods presented here invite themselves for reuse.

- The scale by Braunstein et al. (2011) can be used as a springboard for developing new scales that measure privacy concern as a moderating

factor. Currently, the instruments requires caution since its results are hard to interpret.

- Unless one is limited to a one question or unless comparability with previous studies is crucial, the single question instruments presented in Section 3.6 should be avoided.

- The scale by Smith et al. (1996) is a safe bet. Whether the original version or the modernised version by Malhotra et al. (2004) are used should be decided by the researchers themselves. Their maturity notwithstanding, both versions suffer from the absence of reverse-coded items. This makes the instruments prone to straightlining, in particular when the overall survey is tiresome.

- The scale by Earp et al. (2005) is a valuable resource if one desires broader coverage of privacy aspects than provided by Malhotra et al. (2004). The advantages of the Earp et al. scale are: first, actionable statements, easy for respondents to relate to and to answer; second, the modularity of the scale, which can be split by dimension, if only selected aspects are of interest are required to complement other instruments. The dimensions of 'transfer', 'collection' and 'personalisation' exhibit particularly good reliability scores. However, the scale also lacks reverse-coded items.

5.3. Limitations in scale validation and outlook

The systematic development of ways to measure consumers' privacy concerns has attracted little research compared to the growing literature on data protection and privacy. Those survey instruments which have been developed remain under-used. Instead, in commercial and academic studies alike, one observes a prevalence of ad-hoc procedures to assess users' concern about privacy and its invasion. Regularly, questions without established reliability and validity indicators are used.

Compared with other psychometrics, scale development regarding privacy concern is still in its infancy. There are two avenues for future work: improving the instruments to measure privacy concern, and encouraging their reuse. This article targets both by giving a comprehensive account of currently available, reliable and valid scales for privacy concern.

With the aim of facilitating instrument reuse, I give clear recommendations how and which scales to deploy. At the same time, I highlight scales

which are not yet mature enough for reuse, but which can provide valuable input to future scale development. So far, scale development has often been non-incremental. In curating existing scales, this article also provides a repository of referenced question items to draw from. The overview of survey instruments is complemented by an outline of observational methods and ways in which behaviour can be used for learning users' privacy concerns.

Although researchers now have a handful of good instruments to measure privacy concern, there is still ample space for innovation. I see most potential in, first, indirect measurement approaches that exploit framing to their benefit, and second, in opportunistically observable, revealed preferences and concerns. Interactions on the Web and soon with intelligent spaces are prime examples. At the same time, traditional survey scales need maintenance to include newly arising privacy threats that arise in ubiquitous connectivity and increasingly computer-mediated societies.

Scale validation remains paramount, yet expensive and challenging given the repeatedly observed divergence of actual behaviour and self-professed privacy attitudes.

Acknowledgments

Bettina Berendt made helpful comments on earlier versions of this article.

References

References

Ackerman, M. S., Cranor, L. F., Reagle, J., 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In: Proceedings of the 1st ACM conference on Electronic commerce. EC '99. ACM, New York, NY, USA, pp. 1–8.
URL http://doi.acm.org/10.1145/336992.336995

Acquisti, A., Gross, R., 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In: Danezis, G., Golle, P. (Eds.), Privacy Enhancing Technologies. Vol. 4258 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 36–58.

Aggarwal, G., Bursztein, E., Jackson, C., Boneh, D., 2010. An analysis of private browsing modes in modern browsers. In: Proceedings of the 19th USENIX Security Symposium.

Altman, I., 1975. The environment and social behavior: privacy, personal space, territory, crowding. Brooks/Cole Pub. Co.

Antón, A. I., Earp, J. B., Young, J. D., 2009. How internet users' privacy concerns have evolved since 2002. Computer Science Technical Report TR-2009-16, North Carolina State University.

Barnes, S. B., September 2006. A privacy paradox: Social networking in the United States. First Monday 11 (9).

Bartlett, J., September 2012. The data dialogue.
URL http://www.demos.co.uk/files/The_Data_Dialogue.pdf

Berendt, B., 2012. More than modelling and hiding: towards a comprehensive view of web mining and privacy. Data Mining and Knowledge Discovery 24, 697–737.
URL http://dx.doi.org/10.1007/s10618-012-0254-1

Beresford, A. R., Kübler, D., Preibusch, S., 2012. Unwillingness to pay for privacy: A field experiment. Economics Letters 117 (1), 25–27.

Braunstein, A., Granka, L., Staddon, J., 2011. Indirect content privacy surveys: measuring privacy without asking about it. In: Proceedings of the Seventh Symposium on Usable Privacy and Security. SOUPS '11. ACM, New York, NY, USA, pp. 15:1–15:14.
URL http://doi.acm.org/10.1145/2078827.2078847

Buchanan, T., Paine, C., 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 (2), 157–165.
URL http://dx.doi.org/10.1002/asi.20459

Bundesverfassungsgericht, 1983. Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 (Volkszählung). BVerfGE 65, 1, Bundesverfassungsgericht [Federal Constitutional Court of Germany].
URL http://www.servat.unibe.ch/dfr/bv065001.html

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., de Oliveira, R., 2011. Your browsing behavior for a big mac: Economics of personal information online. CoRR abs/1112.6098.

Chellappa, R. K., Sin, R. G., 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information Technology and Management 6, 181–202.
URL http://dx.doi.org/10.1007/s10799-005-5879-y

Coles-Kemp, L., Lai, Y.-L., Ford, M., 2010. Privacy on the Internet: attitudes and behaviours. Tech. rep., VOME Project.

Culnan, M. J., Armstrong, P. K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science 10 (1), 104–115.
URL http://www.jstor.org/stable/2640390

Cvrcek, D., Kumpost, M., Matyas, V., Danezis, G., 2006. A study on the value of location privacy. In: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society. WPES '06. ACM, New York, NY, USA, pp. 109–118.
URL http://doi.acm.org/10.1145/1179601.1179621

Dinev, T., Hart, P., 2004. Internet privacy concerns and their antecedents – measurement validity and a regression model. Behaviour & Information Technology 23 (6), 413–422.

Dinev, T., Hart, P., 2006a. An extended privacy calculus model for e-commerce transactions. Information Systems Research 17 (1), 61–80.

Dinev, T., Hart, P., 2006b. Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use. e-Service Journal 4 (3), 25–60.
URL http://www.jstor.org/stable/10.2979/ESJ.2006.4.3.25

Dutton, W. H., Blank, G., October 2011. Next generation users: The internet in britain. Oxford internet surveys (oxis), Oxford Internet Institute, University of Oxford.

Earp, J. B., Anton, A. I., Aiman-Smith, L., Stufflebeam, W. H., may 2005. Examining internet privacy policies within the context of user privacy values. IEEE Transactions on Engineering Management 52 (2), 227–237.

Federal Trade Commission, 2007. Fair information practice principles. URL http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Feynman, R. P., June 1974. Cargo cult science. Engineering and Science 37 (7), 10–13.

Fielding, R. T., Singer, D., Oct. 2012. Tracking preference expression (dnt). W3c working draft, World Wide Web Consortium (W3C). URL http://www.w3.org/TR/tracking-dnt/

Goldberg, L. R., Johnson, J. A., Eber, H. W., Hogan, R., Ashton, M. C., Cloninger, C. R., Gough, H. G., 2006. The international personality item pool and the future of public-domain personality measures. Journal of Research in Personality 40 (1), 84–96.

Grossklags, J., Acquisti, A., 2007. When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In: The Sixth Workshop on the Economics of Information Security (WEIS).

Gürses, S., May 2010. Multilateral privacy requirements analysis in online social networks. Ph.D. thesis, HMDB, Department of Computer Science, K.U. Leuven, Belgium.

Harkness, J., November 2010. Cross-cultural survey guidelines. URL http://ccsg.isr.umich.edu/

Hess, T., Schreiner, M., 2012. Ökonomie der Privatsphäre. Datenschutz und Datensicherheit - DuD 36, 105–109. URL http://dx.doi.org/10.1007/s11623-012-0026-5

Horne, D. R., Norberg, P. A., Ekin, A. C., 2007. Exploring consumer lying in information-based exchanges. The Journal of Consumer Marketing 24 (2), 90–99.

IPIP / Oregon Research Institute, 2012. International personality item pool: A scientific collaboratory for the development of advanced measures of personality traits and other individual differences. URL http://ipip.ori.org/

Jenkins, S., Solomonides, T., 1999. Automating questionnaire design and construction. International Journal of Market Research 42 (1), 79–94.

Jentzsch, N., Preibusch, S., Harasser, A., February 2012. Study on monetising privacy. An economic model for pricing personal information. ENISA.

Jourard, S., 1971. Self-disclosure: an experimental analysis of the transparent self. Wiley-Interscience.

Jourard, S. M., Lasakow, P., 1958. Some factors in self-disclosure. The Journal of Abnormal and Social Psychology 56 (1), 91–98.

Kobsa, A., 2007. Privacy-enhanced web personalization. In: Brusilovsky, P., Kobsa, A., Nejdl, W. (Eds.), The Adaptive Web. Vol. 4321 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 628–670.

Krol, K., Moroz, M., Sasse, M. A., Oct. 2012. Don't Work. Can't Work? why it's time to rethink security warnings. In: 7th International Conference on Risk and Security of Internet and Systems (CRiSIS), 2012.
URL http://dx.doi.org/10.1109/CRISIS.2012.6378951

Lewis, K., Kaufman, J., Christakis, N., 2008. The taste for privacy: An analysis of college student privacy settings in an online social network. Journal of Computer-Mediated Communication 14 (1), 79–100.
URL http://dx.doi.org/10.1111/j.1083-6101.2008.01432.x

Lynch, B., May 2012. Advancing consumer trust and privacy: Internet Explorer in Windows 8. TechNet Blogs: Microsoft on the Issues.

Malheiros, M., Preibusch, S., Sasse, M. A., 2013. "fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. In: 6th International Conference on Trust & Trustworthy Computing. Vol. 7904 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 250–266.
URL http://dx.doi.org/10.1007/978-3-642-38908-5_19

Malhotra, N. K., Kim, S. S., Agarwal, J., 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research 15 (4), 336–355.

Maneesriwongul, W., Dixon, J. K., 2004. Instrument translation process: a methods review. Journal of Advanced Nursing 48 (2), 175–186.
URL http://dx.doi.org/10.1111/j.1365-2648.2004.03185.x

Margulis, S. T., 2003. On the status and contribution of Westin's and Altman's theories of privacy. Journal of Social Issues 59 (2), 411–429.

Marshall, N. J., 1974. Dimensions of privacy preferences. Multivariate Behavioral Research 9 (3), 255–271.

Maxion, R., 2011. Making experiments dependable. In: Jones, C., Lloyd, J. (Eds.), Dependable and Historic Computing. Vol. 6875 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 344–357.

Metzger, M. J., 2007. Communication privacy management in electronic commerce. Journal of Computer-Mediated Communication 12 (2), 335–361.
URL http://dx.doi.org/10.1111/j.1083-6101.2007.00328.x

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., Wang, S., 2012. Disclosure antecedents in an online service context: The role of sensitivity of information. Journal of Service Research 15 (1), 76–98.
URL http://jsr.sagepub.com/content/15/1/76.abstract

Mowery, K., Bogenreif, D., Yilek, S., Shacham, H., May 2011. Fingerprinting information in JavaScript implementations. In: Proceedings of W2SP 2011. IEEE Computer Society.

Norberg, P. A., Horne, D. R., Horne, D. A., 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs 41 (1), 100–126.

O'Neil, D., 2001. Analysis of internet users' level of online privacy concerns. Social Science Computer Review 19 (1), 17–31.

Oomen, I., Leenes, R., 2008. The PRIME survey – A study regarding privacy attitudes and behaviour of students in the Netherlands, Flanders and the UK. Tech. rep., PRIME (Privacy and Identity Management for Europe).

Personalization Consortium, 2000, 2005. Personalization & Privacy Survey. Via Internet Archive.
URL http://replay.waybackmachine.org/20050513193924/http://personalization.org/SurveyResults.pdf

Preibusch, S., 2006. Implementing privacy negotiations in e-commerce. In: Zhou, X., Li, J., Shen, H., Kitsuregawa, M., Zhang, Y. (Eds.), Frontiers of WWW Research and Development - APWeb 2006. Vol. 3841 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 604–615.

Preibusch, S., 2009. Key facts on privacy negotiations.
URL http://privacy-negotiations.de/

Preibusch, S., 2013. The value of privacy in web search. In: The Twelfth Workshop on the Economics of Information Security (WEIS).

Preibusch, S., Krol, K., Beresford, A. R., 2012. The privacy economics of voluntary over-disclosure in web forms. In: The Eleventh Workshop on the Economics of Information Security (WEIS).

Preibusch, S., Kübler, D., Beresford, A. R., 2013. Price versus privacy: an experiment into the competitive advantage of collecting less personal information. Electronic Commerce Research, forthcoming.
URL http://dx.doi.org/10.1007/s10660-013-9130-3

Rivenbark, D. R., November 2010. Experimentally elicited beliefs explain privacy behavior. Tech. rep., University of Central Florida – College of Business Administration.
URL http://web.bus.ucf.edu/documents/economics/workingpapers/2010-09.pdf

Sheehan, K. B., Hoy, M. G., 2000. Dimensions of privacy concern among online consumers. Journal of Public Policy & Marketing 19 (1), 62–73.
URL http://www.jstor.org/stable/30000488

Smith, H. J., Milberg, S. J., Burke, S. J., 1996. Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly 20 (2), 167–196.
URL http://www.jstor.org/stable/249477

Son, J.-Y., Kim, S. S., 2008. Internet users' information privacy-protective responses: a taxonomy and a nomological model. MIS Quarterly 32 (3), 503–529.

Spiekermann, S., Grossklags, J., Berendt, B., 2001. E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM Conference on Electronic Commerce. EC '01. ACM, New York, NY, USA, pp. 38–47.

Stewart, K. A., Segars, A. H., 2002. An empirical examination of the concern for information privacy instrument. Information Systems Research 13 (1), 36–49.

Stone, E. F., Gueutal, H. G., Gardner, D. G., McClure, S., 1983. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. Journal of Applied Psychology 68 (3), 459 – 468.

Tavani, H. T., 2007. Philosophical theories of privacy: Implications for an adequate online privacy policy. Metaphilosophy 38 (1), 1–22.
URL http://dx.doi.org/10.1111/j.1467-9973.2006.00474.x

Telefónica S.A., Oct. 2012. Telefónica launches Telefónica Dynamic Insights – a new global big data business unit.
URL http://dynamicinsights.telefonica.com/view-news/?i=94

The Gallup Organization, February 2008. Data Protection in the European Union. Citizens' perceptions. analytical report. Tech. Rep. 225, Flash Eurobarometer.

TNS Opinion & Social, June 2011. Attitudes on Data Protection and Electronic Identity in the European Union. Tech. Rep. 359, Special Eurobarometer.

TRUSTe, July 2012. U.S. consumer privacy attitudes and business implications. Tech. rep.
URL http://download.truste.com/dload.php/?f=FG35QMFR-188

Tsai, J., Egelman, S., Cranor, L., Acquisti, A., 2007. The effect of online privacy information on purchasing behavior: An experimental study. In: The Sixth Workshop on the Economics of Information Security (WEIS).

Westin, A. F., 1967. Privacy and freedom. Atheneum.

Westin, A. F., 1991. Harris-Equifax consumer privacy survey 1991. Tech. rep., Harris, Louis and Associates / Equifax Inc.