COUNTERACTING THE NEGATIVE EFFECT OF FORM AUTO-COMPLETION ON THE PRIVACY CALCULUS

Completed Research Paper

Bart P. Knijnenburg[1]
University of California, Irvine
Donald Bren School of Information and Computer Sciences
5051 Donald Bren Hall
Irvine, CA 92697-3440
bart.k@uci.edu

Alfred Kobsa
University of California, Irvine
Donald Bren School of Information and Computer Sciences
5092 Donald Bren Hall
Irvine, CA 92697-3440
kobsa@uci.edu

Hongxia Jin
Samsung Research America – Silicon Valley
Advanced Technology Lab
75 West Plumeria Dr
San Jose, CA 95134
hongxia.jin@sisa.samsung.com

Abstract

When filling out web forms, people typically do not want to submit every piece of requested information to every website. Instead, they selectively disclose information after weighing the potential benefits and risks of disclosure: a process called "privacy calculus". Giving users control over what to enter is a prerequisite for this selective disclosure behavior. Exercising this control by manually filling out a form is a burden though. Modern browsers therefore offer an auto-completion feature that automatically fills out forms with previously stored values. This feature is convenient, but it makes it so easy to submit a fully completed form that users seem to skip the privacy calculus altogether. In an experiment we compare this traditional auto-completion tool with two alternative tools that give users more control than the traditional tool. While users of the traditional tool indeed forego their selective disclosure behavior, the alternative tools effectively reinstate the privacy calculus.

Keywords: Privacy calculus, information disclosure, decision making, default effect, form auto-completion tools, user experiment, human-computer interaction, structural equation modeling (SEM).

[1] The experiment presented in this paper was conducted by the first author as part of an internship at Samsung Research America – Silicon Valley.

Introduction

Many researchers argue that people employ a *privacy calculus* when deciding whether or not to disclose information about themselves (Culnan 1993; Laufer and Wolfe 1977). When personal information is solicited from them, they assess the benefits that potentially arise from its disclosure in the given context. At the same time, people assess the potential risks of disclosing this information, and decide whether or not to disclose it based on a trade-off between benefits and risks. Giving people control over their disclosure decisions would thus empower them to carefully choose the level of privacy they desire (Lederer et al. 2004; Sadeh et al. 2009).

In contrast, other researchers show that people's privacy decisions are not always so rational (Acquisti and Grossklags 2005, 2008), and that computer users often avoid the hassle of exploiting the control given to them (Compañó and Lusoli 2010). Moreover, an abundance of control can cause significant inconvenience: filling out web forms for instance is seen as a typical nuisance (Bicakci et al. 2011; Trewin 2006). All modern browsers therefore offer some sort of auto-completion feature for web forms, and web designers are encouraged to make forms that use this feature (Garrido et al. 2011; Wroblewski 2008).

Despite their benefits, Preibusch et al. (2012) warn that auto-completion tools may cause users to complete more form fields than they intended. Most auto-completion tools fill out all fields, even those that are not required. We postulate that this counteracts the privacy calculus: it becomes so easy to submit a fully completed form that users skip weighing the benefits and risks of disclosing a certain piece of information in a specific situation.

In this paper we compare three auto-completion tools:

1. A typical auto-completion tool that automatically fills all fields (Auto);
2. A tool that fills out the entire form like the traditional tool but features "remove" buttons next to each field so that users can easily remove individual entries (Remove);
3. A tool that leaves the form empty by default, but has "add" buttons to easily fill individual fields (Add).

The main difference between these latter two tools is whether fields are filled or empty by default. We argue that this "default effect" (Johnson et al. 2002; Lai and Hui 2006; Thaler and Sunstein 2008) may cause users to disclose more to the "Remove" version than to the "Add" version. However, we hypothesize that the increased ease of control over disclosure in both of these alternative tools will nonetheless lead to a lower disclosure than the traditional tool, which does not offer convenient buttons to remove form field entries (and is thus an even stronger default). More specifically, we hypothesize that this ease of control will encourage users to reinstate their privacy calculus and to once again consider the perceived benefits and riskiness of the information. Finally, we hypothesize that the alternative tools will be more satisfying than the traditional auto-completion tool.

This work has several unique contributions. First of all, we empirically validate the idea that users' privacy calculus will lead them to disclose different types of information to different types of websites ("purpose specific disclosure tendency"). This is similar to Hsu (2006), but in a situated behavioral experiment rather than a case-wise behavioral intentions survey. Secondly, although many researchers agree that defaults can have an extensive effect on human decision behavior, we additionally demonstrate that strong defaults such as those in the traditional auto-completion tool can make people ignore their typical decision rationale (i.e., the privacy calculus). Finally, we show how our alternative tools counter this effect and reinstate the privacy calculus.

Related work and hypothesis development

Privacy calculus and purpose specificity

Laufer and Wolfe (1977; Laufer et al. 1973) coined the term "calculus of behavior" to refer to users' conscious process behind their information disclosure decisions. Several researchers have since used the term "privacy calculus" to investigate antecedents of information disclosure (Culnan and Armstrong 1999; Culnan and Bies 2003; Dinev and Hart 2006; Hann et al. 2007; Keith et al. 2011; Li et al. 2010; Milne and

Gordon 1993; Petronio 2002; Wilson and Valacich 2012; Xu et al. 2011, 2009), and it has become a well-established concept in privacy research (Li 2012; Pavlou 2011; Smith et al. 2011).

Li (2012) argues that the privacy calculus can be seen as a privacy-specific instance of decision-making theories like the utility maximization or expectancy-value theory (Awad and Krishnan 2006; Rust et al. 2002; Stone and Stone 1990). The expectancy-value theory states that people gather information about various aspects of each choice option, and assign a value to each of these aspects (Fishbein and Ajzen 1975). Utility maximization, in turn, states that people will trade off the different aspects and then choose the option that maximizes their utility[2] (Bettman et al. 1998; Simon 1959).

What are the aspects that people trade off in privacy decisions? Two aspects are mentioned repeatedly in existing work: perceived risk and perceived relevance.

Featherman and Pavlou define privacy risk as the "potential loss of control over personal information, such as when information about you is used without your knowledge or permission" (Featherman and Pavlou 2003 p. 1036). This loss of control can lead to unintended uses and distribution of the information (Olivero and Lunt 2004; Sheehan and Hoy 2000; Van Slyke et al. 2006). The *perception* of risk is the fear that these unintended consequences will happen (Jacoby and Kaplan 1972; Li 2012). In this sense, perceived risk can be seen as *contextualized* privacy concerns: concerns about the possible consequences of disclosing a *specific* piece of information to a *specific* recipient (Culnan and Bies 2003; Malhotra et al. 2004; Phelps et al. 2000; Smith et al. 1996). Youn (2009) further unpacked perceived privacy risks along Cunningham's (1967) five dimensions of risk: psychological, social, financial, time, and physical risk. From these dimensions it is easy to see that risks may differ from item to item and from recipient to recipient.

Risk perceptions lead us to restrict access to our personal information (Li and Santhanam 2008; Petronio 2002). In fact, surveys have found that between 58.2% (Metzger 2007) and 72% (Hoffman et al. 1999) of all respondents cite risk as a reason not to disclose their personal information. Comparing effect sizes between studies, Dinev & Hart (2006) note that privacy risk may even be more likely to dissuade people from making an e-commerce transaction than the economic risk of the transaction (see also Bhatnagar et al. 2000). White therefore argues that "Marketers' efforts may be wisely directed at attempts to mitigate any perceived "downside risks" associated with disclosure." (White 2004 p. 43).

Several studies found a direct effect of perceived risk on disclosure intentions (Li et al. 2010, 2011; Norberg et al. 2007), while others believe this effect to be (partially) mediated by privacy concerns (Youn 2009) or trust (Dinev and Hart 2006; Dinev et al. 2006). Still others reverse the relationship between risk and concerns/trust, and find that risk is a mediator between concerns or trust and disclosure intentions (Malhotra et al. 2004; Van Slyke et al. 2006; Xu et al. 2005; Zhou 2012). The relationship between perceived risk, concerns, and trust is thus not entirely clear, but the relationship between perceived risk and disclosure—mediated or not—is strong and consistent. Perceived privacy risk may even have longer-term effects beyond disclosure; it may influence users' intention to transact in a web shop (Kim et al. 2008; Pavlou 2003), or their intention to adopt an online service (Featherman and Pavlou 2003).

Whereas perceived risk describes the negative side of the privacy calculus, the positive side appears to be governed by the *perceived relevance* of the request. Just like perceived risk can be seen as contextualized privacy concerns, perceived relevance can be seen as *contextualized* benefit: the perceived benefit of disclosing a *specific* piece of information to a *specific* recipient (Li et al. 2011). Stone (1981) was the first to consider the effect of the perceived relevance of information requests on privacy-related behaviors, and this effect has since been demonstrated empirically (Li et al. 2011). Li et al. (2010) furthermore find that monetary incentives only increase disclosure for requests that are seemingly relevant. Similarly, Phelps et al. (2000) note that people's purchase intentions go down when a service requests information that does not serve the purpose of the request. They therefore argue that "marketers need to resist asking for such information in situations in which the relevance is not readily apparent" (Phelps et al. 2000 p. 38). In the

[2] In the classic utility maximization theory, also called "weighted adding" (Keeney and Raiffa 1976), people are said to assign weights to each of the aspects. The utility of an option is then the value of an aspect times the weight of that aspect, summed over all aspects.

area of privacy norms, the OECD guidelines on the Protection of Privacy recommend that "personal data should be relevant to the purposes for which they are to be used" (OECD 1980).

Based on the above, we argue that the privacy calculus can be operationalized as a combination of perceived relevance and perceived risk. It is remarkable that despite the large body of work on privacy calculus, perceived risk and perceived relevance, these concepts have primarily been studied at the macro-level: Most studies measure how the *overall* perceived risk and relevance influence the *overall* disclosure. We believe that measuring these aspects *per item* will lead to a much more robust and more accurate model of privacy calculus (cf. Knijnenburg et al. 2013a). We therefore hypothesize that users' disclosure of a certain item on a web form will depend on their perceptions of the risk of disclosing that item in the current context, as well as the perceived relevance of that item in the current context:

H1 The perceived risk of disclosing an item (in context) decreases the disclosure of that item.

H2 The perceived relevance of an item (in context) increases disclosure of that item.

If we conjecture that perceived risk and relevance indeed influence the disclosure of personal information, then what determines these perceptions of risk and relevance? In other words, why do users perceive a certain item to be more risky to disclose or less relevant than some other item? For this, we turn to Olson et al. (2005), who show that users of social media tend to selectively share certain types of information with certain types of people only, depending on the *purpose* of the information. This result that has been confirmed for modern social networking sites, cf. (Johnson et al. 2012; Kairam et al. 2012; Watson et al. 2012). Similarly, Consolvo et al. (2005) argue that users of location-sharing services tend to disclose what they think would be useful for the requester.

Scholars have argued for long that the context of the information exchange is important for understanding consumers' willingness to disclose their personal information (Bansal et al. 2008; Borcea-Pfitzmann et al. 2011; Hine and Eve 1998; Xu et al. 2008). This idea of "*purpose specificity*" also has gained much traction in privacy legislation (EU 1995; FTC 2000; White House 2012). Nevertheless it has to date not been studied in a consumer privacy context. It is true that Hsu (2006) demonstrates that users disclose different types of information in different extent to different types of websites, but she does not explain this effect as being the result of the purpose of the information. Still, based on the evidence from the social privacy field, it seems reasonable to assume that this concept of "purpose specificity" extends to online information disclosure as well.

Note that the idea of purpose specificity may be related to Nissenbaum's concept of *contextual integrity* (Nissenbaum 2004, 2010). In her book, Nissenbaum argues that "contextual integrity is defined in terms of informational norms" (Nissenbaum 2010 p. 140) which "render certain attributes appropriate or inappropriate in certain contexts, under certain conditions" (p. 143).

To test the concept of purpose specificity, we ascertain in our experiment that certain types of requested information (e.g. interests, job skills, health record) match the purpose of the websites that requests them (a blogging community, job search website, or health insurer, respectively). Purpose specificity can then be expressed as an interaction between type of information and website: perceived risk is lower and perceived relevance higher when the type of information and the website match in purpose.

H3 The perceived risk of disclosing a certain item depends on the interaction between the type of item and the type of website that requests it, specifically:
- For a given website, perceived risk is lower for the type of information that clearly matches the purpose of that website than for information that does not match.
- For a given type of information, perceived risk is lower for the website that has a clear purpose for requesting the information than for websites that do not have such purpose.

H4 The perceived relevance of a certain item depends on the interaction between the type of item and the type of website that requests it, specifically:
- For a given website, perceived relevance is higher for the type of information that clearly matches the purpose of that website than for information that does not match.
- For a given type of information, perceived relevance is higher for the website that has a clear purpose for requesting the information than for websites that do not have such purpose.

Taken together, H1-H4 paint a purpose-specific picture of the privacy calculus: People consider the perceived relevance and perceived risk of disclosure in their decisions (privacy calculus), and these perceptions are in turn influenced by the congruence between the type of item and the type of website that is requesting the item (purpose specificity). In effect, people are more likely to disclose items that match the purpose of the website, and withhold information that does not match the website's purpose.

Control: increasing the decision burden or stimulating the privacy calculus?

Control over one's disclosure is a necessary requisite for the privacy calculus: An adequate amount of control is needed to implement the outcome of the risk versus relevance trade-off. Giving people control over their information disclosure decisions has several downsides and shortcomings though (Brandimarte et al. 2013; Compañó and Lusoli 2010; Knijnenburg et al. 2013a). Exacting control can be a burden (Compañó and Lusoli 2010), and people may lack the level of self-efficacy required to take control over their disclosure decisions (Larose and Rifon 2007; Mohamed and Ahmad 2012; Yao et al. 2007), or they may simply not be motivated to make the effort (Bamberger and Mulligan 2011; Besmer et al. 2010; Bonneau and Preibusch 2010; Larose and Rifon 2007). For example, Larose and Rifon (2007) find that privacy seals influence disclosure tendencies, but only for participants that are either motivated or have a high self-efficacy. Similarly, Besmer et al. (2010) employ social navigation cues to influence users' information disclosure on Facebook, and they too find that participants were only influenced if they already had a tendency to change their settings.

To reduce the burden of information disclosure, modern Internet browsers have a form auto-completion feature, known as "AutoComplete"[3], "AutoFill"[4,5], or "Auto Form Fill"[6]. Auto-completion tools reduce the required amount of typing, and help users to recall the correct information (Bicakci et al. 2011; Trewin 2006). Usability experts therefore recommend to web developers to build their forms in a way that enables them to be recognized by these auto-completion aids (Garrido et al. 2011; Wroblewski 2008). There even exist a number of third-party tools such as RoboForm[7], LastPass[8], and Dashlane[9], which provide more comprehensive (e.g. cross-device) auto-completion features.

Despite the apparent benefits of auto-completion, Preibusch et al. (2012) warn that since these tools typically fill *all* the fields on a form (even optional fields), they could increase the risk of over-disclosure. In this paper we therefore introduce two alternative auto-completion tools that arguably make it easier for users to control their information disclosure without giving up the convenience of a regular auto-completion tool. Specifically, we compare three auto-completion tools:

1. A traditional auto-completion tool that automatically fills all fields (Auto);
2. A tool that fills all fields by default like traditional auto-completion but has "remove" buttons next to each field to easily remove entries (Remove);
3. A tool that leaves the form empty by default, but has "add" buttons to easily fill fields (Add).

The buttons of these latter two tools toggle between "Add" and "Remove", and hence the main difference between them is whether fields are filled or empty by default. Research in human decision-making suggests that this could lead to a "default effect" (Johnson et al. 2002; Lai and Hui 2006; Thaler and Sunstein 2008). More specifically, the "remove" tool puts users in a "reject frame" (i.e., they have to think of reasons to reject disclosure), while the "Add" version puts users in an "accept frame" (i.e., they have to think of reasons to accept disclosure). Researchers have shown that decision-makers need to feel more committed in order to make an "accept" decision than a "reject" decision, and we thus expect disclosure to be lower for the "Add" tool than for the "Remove" tool (Ganzach 1995; Meloy and Russo 2004; Wedell 1997).

---

[3] http://windows.microsoft.com/en-us/windows7/fill-in-website-forms-and-passwords-automatically
[4] http://support.google.com/chrome/bin/answer.py?hl=en&answer=142893
[5] http://support.apple.com/kb/PH5044
[6] http://support.mozilla.org/en-US/kb/control-firefox-automatically-fills-in-forms
[7] http://www.roboform.com/
[8] https://lastpass.com/features_free.php
[9] https://www.dashlane.com/en/features/smartformfilling

H5 The disclosure will be higher for the "Remove" auto-completion tool than for the "Add" auto-completion tool.

The effort to change the default has been shown to increase the default effect (Johnson and Goldstein 2003; Samuelson and Zeckhauser 1988). The traditional auto-completion tool does not have convenient buttons to change the disclosure, and may thus suffer from an even stronger default effect. Therefore, we expect it to have higher disclosure rates than our alternative tools.

H6 The disclosure will be higher for the traditional auto-completion tool than for the "Remove" and "Add" auto-completion tools.

Not only are users of the traditional auto-completion tool subjected to a stronger default effect; this tool may also render it so easy to submit a fully completed form that users become less likely to engage in a privacy calculus. So instead of carefully selecting what information to disclose based on their perceptions of relevance and risk, users of the traditional auto-completion tool may refrain from making any changes to the form. In contrast, since it is much easier to change the default values in the "Remove" and "Add" auto-completion tools, these tools allow (and even encourage) their users to reinstate the privacy calculus.

H7 The type of auto-completion tool moderates the effect of perceived risk on disclosure. Specifically, the effect of perceived risk on disclosure will be stronger for the "Remove" and "Add" auto-completion tools than for the traditional tool.

H8 The type of auto-completion tool moderates the effect of perceived relevance on disclosure. Specifically, the effect of perceived relevance on disclosure will be stronger for the "Remove" and "Add" auto-completion tools than for the traditional tool.

Finally, we hypothesize that users of the alternative auto-completion tools will appreciate the ability to make more rational decisions. Users of the alternative tools will thus be more satisfied with the tool than users of the traditional tool.

H9 Users' satisfaction with the "Remove" and "Add" auto-completion tools is higher than users' satisfaction with the traditional auto-completion tool.

Considering all hypotheses together, we postulate a theory about why traditional auto-completion tools are problematic: Although people typically engage in a purpose-specific privacy calculus, the traditional auto-completion tool has such a strong default effect that it holds people back from engaging in this privacy calculus. In contrast, our "Remove" and "Add" tools allow users to reinstate the privacy calculus.

Experimental setup

To test our hypotheses, we conducted an online user experiment with mock-ups of the three proposed auto-completion tools. After being randomly assigned to one of the three tools, participants provided the tool with a wide range of personal information (general contact information, personal interests, job skills, and health record), and then "tested" the tool on a randomly selected website (also mock-ups) which requested some of the information participants had provided to the auto-completion tool. Each of the three websites presented some kind of personalized service, and each was chosen to correspond to a particular subset of the personal information requested by the auto-completion tool: A blogging community matched personal interest items, a job search website matched job skills items, and a health insurer matched health record items. However, in our experiment these websites did not just ask for these "matching" items, but also the items that did not clearly match the purpose of the website (e.g. health record items requested by the blogging community). Requesting both matching and non-matching items on the website provided a within-subjects manipulation (see below) that allowed us to measure the purpose specificity of disclosure in each of the three auto-completion tools.

Participants

543 participants were recruited via Amazon Mechanical Turk, a popular recruitment tool for user experiments (Kittur et al. 2008). Participation was restricted to US participants with a high "worker reputation". 17 participants were removed after data quality checks, and another 66 were removed because they said it was "obvious" that the target website described below was a fake. The remaining 460

participants generally matched the US Internet population demographics: we found no deviations in geographical location, income (median personal income: $25K-50K), level of employment (68% employed, 12% students, 8% looking for work, 11% not looking for work, 2% unable to work or retired) and education (16% high school, 31% some college, 40% undergraduate degree, 13% post-graduate degree), and a slight overrepresentation of younger (median age: 31) and female (254) participants.

System and procedure

Participants were recruited to test "FormFiller, a new tool that makes it easier to fill out forms on websites". They were promised a $2 payment for their efforts. Upon accepting the task, participants were randomly assigned to one of the experimental conditions (see Manipulations). Next, they were instructed about the experimental procedures and the workings of the assigned version of the form auto-completion tool. Their comprehension of these instructions was tested, and they were not allowed to proceed until they correctly answered all comprehension questions.

In the next step participants filled out their personal information in the FormFiller tool (Figure 1a). To avoid any privacy concerns at this stage, they were explicitly ensured that their information would only be stored locally and temporarily.

Participants were then randomly transferred to one of the three mock websites, "to test the FormFiller tool". To disguise the fact that this website was a mock-up (i.e., to make it look like a legitimate third-party website), it had its own domain name and a design that was clearly different from the FormFiller tool (see Figures 1bcd). We also delayed the transfer from FormFiller to the external site by a 3-second "loading" screen. The website welcomed participants with a short description of its personalized service and the task that participants would perform (i.e. fill out their information elicitation form).

On the next screen, the FormFiller tool popped up, stating that it had detected a form, and that it had taken the appropriate action (i.e. filled the form, filled the form and added "remove" buttons, or added "add" buttons, depending on the condition). The tool reminded the participant that he/she was allowed to clear, fill, or change any fields, according to what he/she wanted to submit to this third-party website. After participants submitted the form, the external site would indicate that it would not provide any personalized "results" to the user, as to not "interfere with your test of the FormFiller".

Finally, participants were transferred back to the FormFiller website, where they would fill out a number of questionnaires evaluating the FormFiller, their trust in the external website, their reasons for disclosing or not disclosing each requested item, and their concerns with the collection of and control over their personal information.

Manipulations

Between subjects, we manipulated the **type of auto-completion tool** by creating three versions of the Formfiller (quoted text is from explanations presented to participants):

- The **Auto** FormFiller is a traditional auto-completion tool and serves as our baseline. This version "will automatically fill in the form fields with the data in your local profile. You can remove or change the info manually if you like."
- The **Remove** FormFiller is like the auto FormFiller, but "[i]f you do not want to submit the information, you can easily remove it from the field with the click of a button. You can also change the info manually if you like."
- The **Add** FormFiller does not fill out the form automatically, but "adds a button to each form field. With a click on that button, FormFiller will fill in that field with the data in your local profile. You can enter or change the info manually if you like."

Also between subjects, we manipulated the **website** on which participants tested the FormFiller tool. We made sure that the presented personalized service would be matched with one of the requested information types (see below), but that it would not be completely implausible for the website to request the non-matching information types:

- **BlogHeroes** (Figure 1b) was presented as an online blogging network that uses the users' personal information to categorize them into "guilds" of bloggers that have similar interests. This

website matched the Interests information type, but we argued that some bloggers also blogged about their jobs or health conditions.

- **I♡WRK** (Figure 1c) was presented as a job search website that uses the users' personal information to find jobs. This website matched the Job Skills information type, but we argued that the system would also use other personal characteristics.
- **Codacare** (Figure 1d) was presented as a health insurance company that uses the users' personal information to tailor their health care to their personal needs and preferences. This website matched the Health Record information type, but we argued that the other information types would help as well, e.g. to find a primary care physician that the user can get along with.

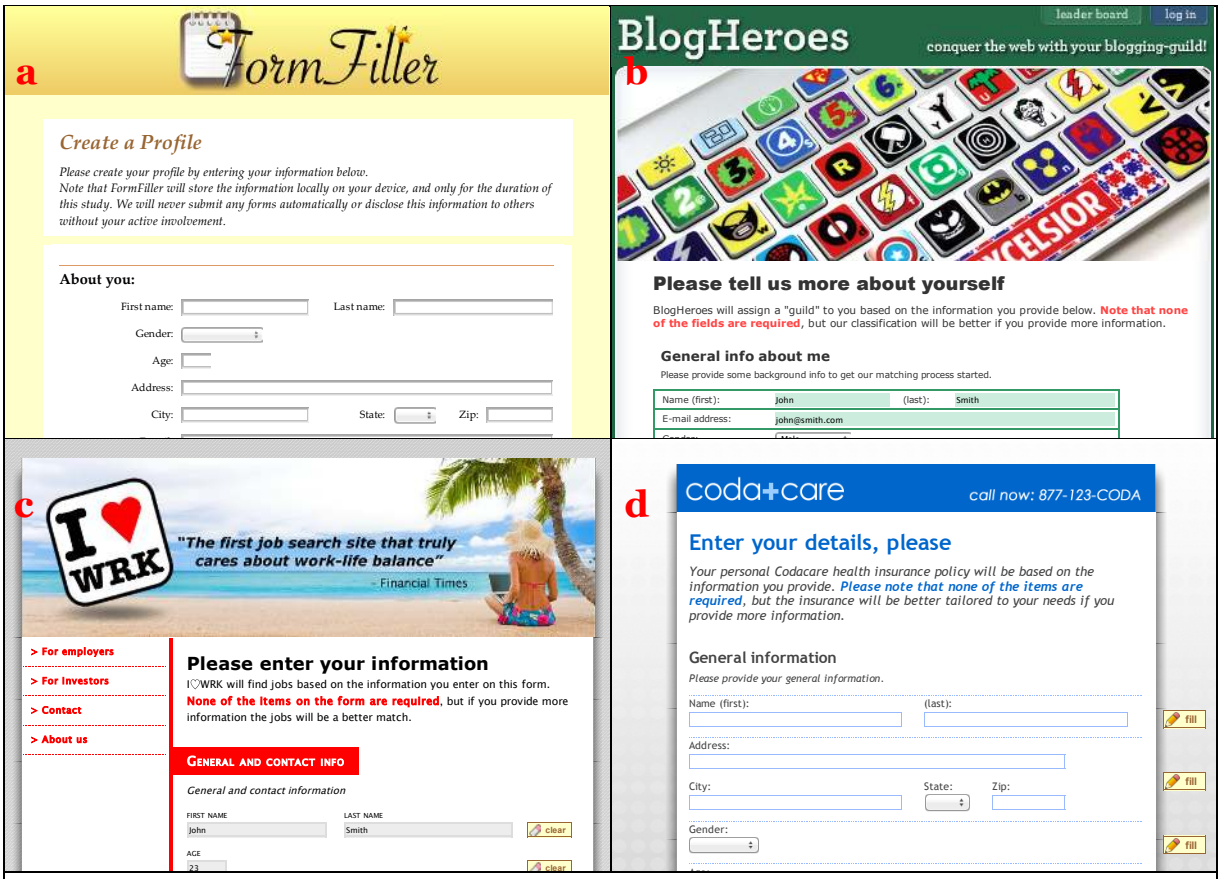

Figure 1. The websites used in the experiment: a) the FormFiller website, b) the BlogHeroes website with the Auto FormFiller, c) the I♡WRK website with the Remove FormFiller, d) the Codacare website with the Add FormFiller.

On the FormFiller, participants provided 24 pieces of personal information, divided into four **item types**: **Contact Info**, **Interests**, **Job Skills**, and **Health Record** (see Table 1 for the specific items). To increase the realism of our study, one item from each category was not requested by the external website. Specifically, the website always first requested five Contact Info items, and then the other item types in random order. The order in which item types were presented did not have significant effects in our analysis, so this variable is excluded from further analysis. To increase contrast between the FormFiller and the external websites, items were ordered and worded slightly differently within each type on each website.

For the purpose of our analysis, the study was set up as a repeated 3-by-3-by-4 mixed factors experiment with 460 participants that are divided into 3×3 between-subjects conditions (type of tool and website), and 4 within-subjects conditions (i.e. four item types) that are repeated 5 times per participant (i.e. five items per type).

Dependent variables

Our main dependent variable of interest was **disclosure** to the external website, a dichotomous (yes/no) variable that was measured 20 times for each participant. If participants changed their answer between the FormFiller and the external website we counted it as a 'yes' nonetheless, unless the answer was completely bogus. Items that were only partially disclosed (e.g. a first name but no last name) were counted as a 'no'. The specific 20 items that were used are listed in Table 1. They were inspired by our previous work (Knijnenburg et al. 2013b), where we used exploratory and confirmatory factor analysis (CFA) to demonstrate that these items have the expected four-dimensional structure. We confirmed this structure on the current data using a CFA, which showed a good[10] fit ($\chi^2(164) = 281.977$, $p < .001$; *CFI* = .993, *TLI* = .992; *RMSEA* = .040, 90% CI: [.032, .047]). Moreover the factors had a good convergent and discriminant validity[11]. Table 1 shows the factor loadings; only the item "Current/previous job title and sector" showed some misfit. In the remainder of our analysis we retain this item for the sake of completeness.

Table 1. The items requested on the website

Type of data	Item	Level of disclosure	Factor loading	Factor correlation
Contact info	First and last name	420 (91.3%)	0.839	
	Gender	446 (97.0%)	1.003	Interests: .697
Alpha: 0.77	Age	437 (95.0%)	1.068	Job skills: .822
AVE: 0.843	Address, city, state and zip	342 (74.3%)	0.817	Health record: .776
	E-mail address	387 (84.1%)	0.844	
Interests	Favorite movie	432 (93.9%)	0.934	
	Favorite band/artist	433 (94.1%)	0.953	Contact info: .697
Alpha: 0.94	Favorite food	434 (94.3%)	0.952	Job skills: .844
AVE: 0.948	Favorite weekend pastime	433 (94.1%)	1.007	Health record: .863
	Political views	418 (90.9%)	1.023	
Jobs skills	Current/previous job title and sector	344 (74.8%)	0.585	
	Employment status	434 (94.3%)	0.977	Contact info: .822
Alpha: 0.82	Works experience	428 (93.0%)	0.991	Interests: .844
AVE: 0.844	Income level	413 (89.8%)	0.993	Health record: .909
	Highest completed degree	437 (95.0%)	0.977	
Health record	Overall health	433 (94.1%)	0.987	
	Dietary restrictions	433 (94.1%)	0.934	Contact info: .776
Alpha: 0.90	Weight	415 (90.2%)	0.955	Interests: .863
AVE: 0.925	Birth control usage	413 (89.8%)	0.982	Job skills: .909
	Medical conditions	422 (91.7%)	0.950	

As part of the post-study questionnaires, we asked participants for each of the 20 items how they perceived the act of disclosing the item in terms of perceived risk, perceived relevance, expectedness, anticipated benefit, and desired and actual secrecy, each on a 7-point scale. **Perceived risk** (i.e. the statement "Providing [item] to [website] is:" rated on a 7-point scale from "very safe" to "very risky") and **perceived relevance** (i.e. the statement "The fact that [website] asked for [item] was:" rated on a 7-point scale from "very inappropriate" to "very appropriate") had the highest correlation with Disclosure, and accounted for more than 80% of the variance explained by all aspects taken together. Based on these findings and the fact that our hypotheses revolve around the concept of perceived risk and perceived relevance, we disregard the other variables in the current study.

[10] A good model has a χ^2 that is not statistically different from a saturated model ($p > .05$). However, this statistic is regarded as too sensitive, and researchers have proposed other fit indices (Bentler and Bonett 1980). Hu and Bentler (1999) propose cut-off values for these indices to be: *CFI* > .96, *TLI* > .95, and *RMSEA* < .05, with the upper bound of its 90% CI falling below 0.10.

[11] A criterion for convergent validity is that the average variance extracted (AVE) should be greater than 0.5, and Chronbach's alpha should be greater than .7 (acceptable), .8 (good) or .9 (excellent). For discriminant validity, the square root of the AVE should be higher than the correlations between factors.

Finally, we measured **satisfaction** with the FormFiller tool using a scale (Alpha: .93, AVE: .791) adapted from (Knijnenburg and Kobsa 2013a; Knijnenburg et al. 2012), with the following 6 items, measured on a 7-point scale from "completely disagree" to "completely agree":

- "I would use FormFiller if it was available"
- "Based on what I have seen, FormFiller is useful"
- "Using FormFiller makes me happy"
- "So far, I am satisfied with FormFiller"
- "I would recommend FormFiller to others"
- "I would quickly abandon using FormFiller"

Results

Overview of hypothesized effects

We test H1-H8 using the path model described in Figure 2. Two effects that were not hypothesized are added to the model (dotted lines in Figure 2): a residual correlation between Perceived Risk and Perceived Relevance (accounting for the fact that items perceived as irrelevant are often also perceived as risky), and a main effect of Type of information on Disclosure (accounting for an inherent difference in disclosure tendency between these types of information that goes beyond perceived risk and relevance).

Moreover, since H7 and H8 moderate the effects of H1 and H2 as well as H5 and H6, these effects are estimated in separate path models (dashed lines in Figure 2). This allows us to first evaluate the main-effect hypotheses before turning to the question of effect moderation.

Finally, H9 is tested using a Multiple Indicators and Multiple Causes (MIMIC) model, where the Satisfaction factor scores are regressed on the Tool type.

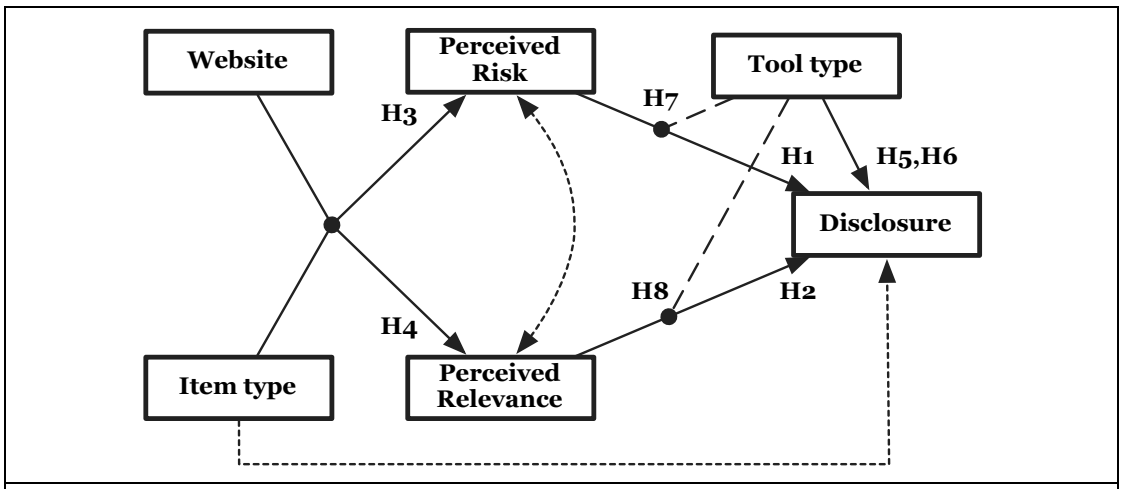

Figure 2. Experimental model. H7-H8 describe a moderating effect on H1-H2.

Hypotheses 1 through 6

H1-H6 are tested using the path model described in Figure 2 *without* the dashed lines (H7-H8). This repeated measures model, estimated with MPlus using a weighted least squares estimator, has an excellent fit ($\chi^2(12) = 11.929$, $p = .451$; *CFI* = 1.00, *TLI* = 1.00; *RMSEA* < .001, 90% CI: [.000, .011]).

H1+H2. Perceived Risk + Perceived Relevance → Disclosure

Table 2 shows the rightmost part of the model, i.e. the regression of Disclosure. Controlling for Perceived Relevance, Item type, and Tool type (and assuming the modeled order of causality), a 1 point increase in Perceived Risk (on a 7-point scale) leads to 19.2% lower odds of Disclosure. This is a significant ($p < .001$) medium-sized ($r = .245$) effect. H1 is thus supported.

Likewise, controlling for Perceived Risk, Item type, and Tool type (and assuming the modeled order of causality), a 1 point increase in Perceived Relevance (on a 7-point scale) leads to 7.9% lower odds of Disclosure. This is a significant ($p < .001$) small ($r = .125$) effect. H2 is thus supported as well.

Finally, note that these effects exist in the context of a main effect of Item type on disclosure: Controlling for Perceived Risk, Perceived Relevance and Tool type, the disclosure of Interests and Health record items is higher than the disclosure of Contact info and Job skills.

Table 2. Regression of Disclosure (path model excl. H7-H8)

Independent variable	*Disclosure odds ratio*	*(95% CI)*	*p-value*	*Effect size*
Intercept	4.225	(3.287, 4.225)		
Perceived Risk[12]	0.818	(0.782, 0.856)	< .001	$r = .245$
Perceived Relevance	1.079	(1.042, 1.118)	< .001	$r = .125$
Item type				
Contact info	1.0			
Interests	1.292	(1.023, 1.631)	.031	
Job skills	0.946	(0.795, 1.127)	.536	
Health record	1.320	(1.096, 1.591)	.004	
Tool type				
Auto	1.0			
Remove	0.760	(0.580, 0.996)	.047	$d = .165$
Add	0.811	(0.619, 1.063)	.130	$d = .107$

H3+H4. Website × Item type → Perceived Risk + Perceived Relevance

Tables 3 and 4 show the means of Perceived Risk and Perceived Relevance per Website and Item type. Figure 3 shows these means graphically for a better overview. We gathered some qualitative feedback from participants about the reasons for certain information being risky and relevant. As for risk, participants' main reasons were identity theft ("It provides the first step to finding your identity"), spam ("It can fill up my inbox with unwanted junk e-mails"), differential pricing or hiring decisions (mainly for the I♡WRK website; "If the information gets to employers, it could impact hiring decisions"), fear of becoming the subject of ridicule ("exposed to criticism by movie snobs"), and being the request being inappropriate or weird ("it is inappropriate to ask for my birth control usage"). As for relevance, participants came up with various laymen's explanations of why certain information could be useful for personalization purposes, but they would not take the relevance at face value: many qualitative comments were in the line of "It can't be useful".

Tables 3 and 4 also show the results of a series of post-hoc tests to qualify the interaction between Website and Item type: the second line of each cell compares each non-matching item type for that website to the matching item type (e.g. for I♡WRK, Interests are perceived as significantly more risky as Job skills, with $p = .029$); the third line of each cell compares each non-matching website for that item type to the matching website (e.g. Interests are perceived as significantly more risky for I♡WRK than for BlogHeroes, with $p = .008$).

Regarding perceived Risk, we find that the interaction between Website and Item type is significant ($\chi^2(6) = 246.41$, $p < .0001$). Moreover, for each website, the non-matching item types are perceived as significantly more risky than the matching item type. Also, for each item type, the non-matching websites are perceived as significantly more risky than the matching website[13]. H3 is thus supported.

[12] The correlation between Perceived Risk and Perceived Relevance is -.536, which is a significant ($p < .001$) large effect.

[13] To adjust for multiple comparisons, we compared the *p*-values in Table 3 and Table 5 against Bonferroni-Holm corrected α levels; see http://en.wikipedia.org/wiki/Holm-Bonferroni_method.

Likewise, the interaction between Website and Item type is also significant for Perceived Relevance ($\chi^2(6) = 913.47$, $p < .0001$). For each website, the non-matching item types are perceived as significantly less relevant than the matching item type (except Contact info for BlogHeroes and Codacare), and for each item type, the non-matching websites are perceived as significantly less relevant than the matching website. H4 is thus supported as well.

Table 3. Mean Perceived Risk (range: -3 to +3) per Website and Item type

	BlogHeroes	I♡WRK	Codacare
Contact info	-0.692 (cf. Interests: $p < .001$)	-1.019 (cf. Job skills: $p < .001$)	-1.268 (cf. Health rec.: $p = .008$)
Interests	**-1.683**	-1.293 (cf. Job skills: $p = .029$) (cf. BlogHeroes: $p = .008$)	-1.065 (cf. Health rec.: $p < .001$) (cf. BlogHeroes: $p < .001$)
Job skills	-0.752 (cf. Interests: $p < .001$) (cf. I♡WRK: $p < .001$)	**-1.512**	-0.930 (cf. Health rec.: $p < .001$) (cf. I♡WRK: $p < .001$)
Health record	-0.519 (cf. Interests: $p < .001$) (cf. Codacare: $p < .001$)	-0.044 (cf. Job skills: $p < .001$) (cf. Codacare: $p < .001$)	**-1.585**

Table 4. Mean Perceived Relevance (range: -3 to +3) per Website and Item type

	BlogHeroes	I♡WRK	Codacare
Contact info	0.994 (cf. Interests: p = .024)	1.346 (cf. Job skills: p < .001)	1.819 (cf. Health rec.: p = .423)
Interests	**0.761**	-1.180 (cf. Job skills: p < .001) (cf. BlogHeroes: p < .001)	-1.394 (cf. Health rec.: p < .001) (cf. BlogHeroes: p < .001)
Job skills	0.091 (cf. Interests: p < .001) (cf. I♡WRK: p < .001)	**1.820**	0.516 (cf. Health rec.: p < .001) (cf. I♡WRK: p < .001)
Health record	-1.158 (cf. Interests: p < .001) (cf. Codacare: p < .001)	-1.724 (cf. Job skills: p < .001) (cf. Codacare: p < .001)	**1.906**

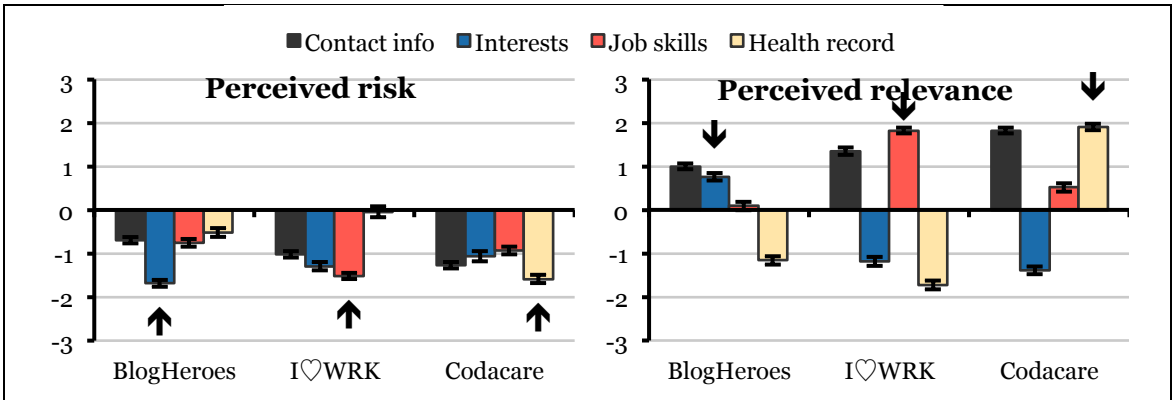

Figure 3. Perceived Risk and Perceived Relevance per Website and Item type. The arrows point to the matching item types. Error bars are ± 1 Standard Error.

H5+H6. Tool type → Disclosure

The last row in Table 2 presents the effect of Tool type on Disclosure. Controlling for Perceived Risk, Perceived Relevance, and Item type, the odds of Disclosure are 6.3% *higher* for users of the Add tool than for users of the Remove tool, although this effect not significant (p = .631). Surprisingly then, H5 is rejected: there is no significant difference in Disclosure between the Add and Remove tools.

The planned contrast between the traditional Auto tool and the alternative tools is significant ($\chi^2(1)$ = 4.037, p = .045). Controlling for Perceived Risk, Perceived Relevance, and Item type, the odds of Disclosure are 24.0% lower for users of the Remove tool compared to users of the Auto tool, a small (d = .165) but significant (p = .047) effect. The odds of Disclosure are 18.9% lower for users of the Add tool compared to users of the Auto tool, a small (d = .107) effect that is not significant (p = .130). H6 is thus partially supported: Disclosure is indeed significantly higher for the Auto tool than for the Remove tool.

Hypotheses 7 and 8

To test H7 and H8, we introduce the interaction between Tool type and Perceived Risk and Relevance (dashed lines) to the path model described in Figure 2. Unfortunately, due to the high correlation between Perceived Risk and Perceived Relevance, we were unable to fit a model that includes *both* effects. We therefore introduce each effect to the model separately.

H7. Tool type × Perceived Risk → Disclosure

To model the interaction between Tool type and Perceived Risk, we create a multiple group model, comparing the Add and Remove groups against the Auto group, fixing all parameters except for the intercept and the effect of Perceived Risk. This model again has an excellent fit ($\chi^2(86)$ = 99.443, p = .152; *CFI* = .990, *TLI* = .988; *RMSEA* = .007, 90% CI: [.000, .013]).

Table 5. Regression of Disclosure, based on our path model (Figure 2, including H7 but not H8)

Independent variable	*Disclosure odds ratio*	*(95% CI)*	*p-value*	*Effect size*
Intercept				
Auto	3.773	(2.570, 5.541)		
Remove	2.804	(1.978, 3.974)		
Add	3.740	(2.876, 4.863)		
Perceived Risk				
Auto	0.863	(0.816, 0.914)	< .001	*r* = .361
Remove	0.754	(0.682, 0.833)	< .001	*r* = .371
Add	0.811	(0.761, 0.866)	< .001	*r* = .330
Perceived Relevance	1.073	(1.037, 1.109)	< .001	*r* = .115
Item type				
Contact info	1.0			
Interests	1.225	(0.966, 1.553)	.093	
Job skills	0.937	(0.790, 1.111)	.452	
Health record	1.346	(1.142, 1.587)	< .001	

Table 5 shows the regression on Disclosure, with three different intercepts and effects of Perceived Risk. The effect of Perceived Risk on Disclosure for the Auto tool is notably lower than for the Remove and Add tools. The planned contrast between the traditional Auto tool and the alternative tools is significant ($\chi^2(1)$ = 5.017, p = .025).

Controlling for Perceived Relevance and Item type (and assuming the modeled order of causality), a 1 point increase in Perceived Risk leads to 13.7% lower odds of Disclosure in for users of the Auto tool. For users of the Remove tool, the odds of Disclosure are 24.6% lower per 1 point increase in Perceived Risk, and this is a significantly stronger effect than for the Auto tool (p = .025). For users of the Add tool, the odds of Disclosure are 18.9% lower per 1 point increase in Perceived Risk, but this effect is not significantly stronger than for the Auto tool (p = .179). H7 is thus partially supported: The effect of Perceived Risk on Disclosure is indeed significantly stronger for the Remove tool than for the Auto tool.

H8. Tool type × Perceived Relevance → Disclosure

To model the interaction between Tool type and Perceived Relevance, we create a multiple group model, comparing the Add and Remove groups against the Auto group, fixing all parameters except for the intercept and the effect of Perceived Risk. This model again has an excellent fit ($\chi^2(86) = 95.140$, $p = .235$; *CFI* = .993, *TLI* = .992; *RMSEA* = .006, 90% CI: [.000, .012]).

Table 6. Regression of Disclosure, based on our path model (Figure 2, including H8 but not H7)

Independent variable	*Disclosure odds ratio*	*(95% CI)*	*p-value*	*Effect size*
Intercept				
Auto	3.777	(2.557, 5.579)		
Remove	2.732	(1.916, 3.895)		
Add	3.800	(2.905, 4.970)		
Perceived Risk	0.816	(0.786, 0.847)	< .001	$r = .266$
Perceived Relevance				
Auto	0.989	(0.927, 1.055)	.736	$r = .026$
Remove	1.133	(1.064, 1.206)	< .001	$r = .285$
Add	1.114	(1.057, 1.175)	< .001	$r = .208$
Item type				
Contact info	1.0			
Interests	1.260	(0.998, 1.591)	.051	
Job skills	0.959	(0.809, 1.137)	.629	
Health record	1.409	(1.188, 1.671)	< .001	

Table 6 shows the regression on Disclosure, with three different intercepts and effects of Perceived Risk. The effect of Perceived Risk on Disclosure for the Auto tool is notably lower than in the Remove and Add tools. The planned contrast between the traditional Auto tool and the alternative tools is significant ($\chi^2(1) = 10.526$, $p = .001$).

Controlling for Perceived Risk and Item type (and assuming the modeled order of causality), a 1 point increase in Perceived Relevance leads to a negligible ($p = .736$) 1.1% lower odds of Disclosure for users of the Auto tool. For users of the Remove tool, the odds of Disclosure are 13.3% higher per 1 point increase in Perceived Relevance, and this is a significantly stronger effect than for the Auto tool ($p = .003$). For users of the Add tool, the odds of Disclosure are 11.4% higher per 1 point increase in Perceived Relevance, and this effect is also significantly stronger than for the Auto tool ($p = .006$). H8 is thus supported.

Hypothesis 9

The MIMIC model for Satisfaction regressed on Tool type has a good fit ($\chi^2(19) = 45.574$, $p = .001$; *CFI* = .998, *TLI* = .997; *RMSEA* = .012, 90% CI: [.000, .017]). The planned contrast between the traditional Auto tool and the alternative tools is not significant ($\chi^2(1) = 2.293$, $p = .130$). Users of the Add tool are significantly more satisfied ($\beta = .238$, $p = .046$) than users of the Auto tool, but users of the Remove tool are not significantly more satisfied ($\beta = .095$, $p = .466$). H9 is thus partially supported.

Discussion

With all of our hypotheses except H5 supported, we can make a number of overarching statements about people's privacy decision making. Combining our hypotheses regarding the privacy calculus (H1, H2) with our hypotheses regarding purpose specificity (H3, H4), we can derive a ***purpose-specific theory of privacy calculus****:* The disclosure of a certain item in a certain context depends on the interaction between the type of information and the type of website, mediated by perceived risk and relevance. More specifically, when the type of information clearly matches the purpose of the website, people perceive the item as more relevant and its disclosure as less risky, and they will therefore be more likely to disclose it. Figure 4 shows that this is indeed the case.

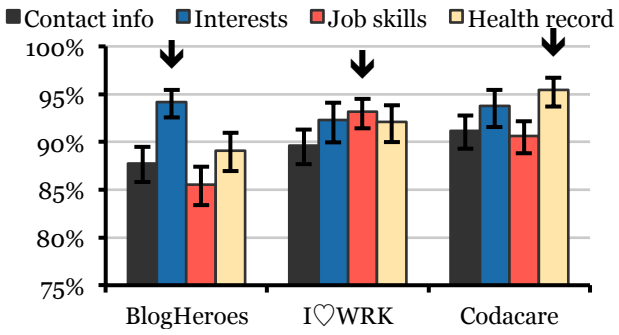

Figure 4. Disclosure rate per Website and Item type. The arrows point to the matching item types. Error bars are ± 1 Standard Error.

Against our expectations, **the alternative Remove and Add tools do not suffer from a default effect**. Despite the established behavioral differences between accept and reject frames (Ganzach 1995; Meloy and Russo 2004; Wedell 1997), we find that users in the Add condition disclose just as much as users in the Remove condition (Remove: 89.7%; Add: 90.4%). One reason for this may be that people are forced to think about positive consequences in the add frame, but negative consequences in the reject frame (Shafir 1993); research has shown that encouraging people to think about the positive consequences of a request makes them more likely to accept it (Dinner et al. 2011).

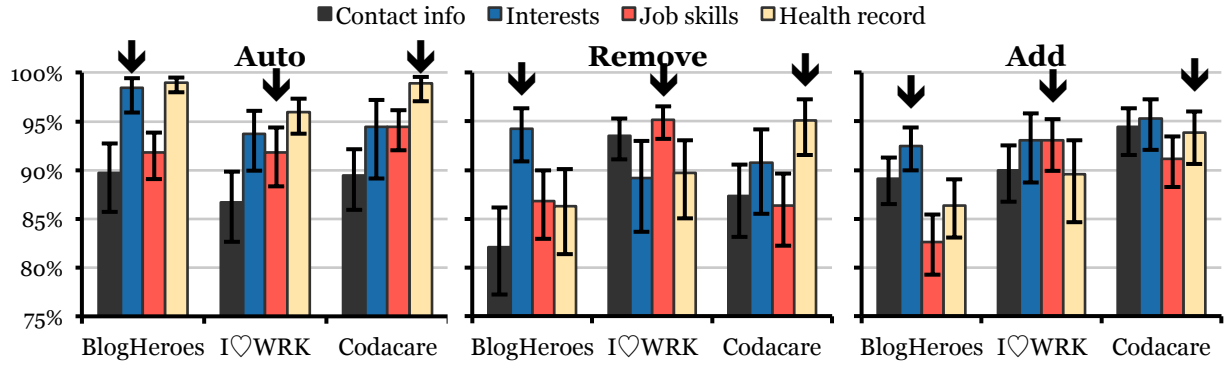

Figure 5. Disclosure rate per Website and Item type, for each of the three tools. The arrows point to the matching item types. Error bars are ± 1 Standard Error.

Because users in the Add condition disclose quite a lot of information, one might expect this tool to lack convenience compared to the other tools, because users have to press a button to fill it out each field they want to disclose (which comes to about 18 on average). Interestingly though, **the Add tool is more satisfying than the Auto tool**. This indicates that the lack-of-convenience argument does not hold ground. The observation that people prefer the accept frame, especially for personal judgments, is in line with our findings (Heller et al. 2002; Levin et al. 2000).

As expected, participants using the traditional FormFiller tool (Auto: 93.5%) disclosed significantly more than the participants using the alternative tools, which indicates that **the alternative tools reduce the strong default effect of the traditional auto-completion tool**. Moreover, H7 and H8 show that users of the Remove and Add auto-completion tools are more likely to consider Perceived Risk and Perceived Relevance when making their decisions. Combining this finding with our purpose-specific theory of privacy calculus, we expect disclosure to be higher when the website and item type match than when they do not match, but *only* for users of the Remove and Add tools. Figure 5 shows that this is

indeed the case, especially for the Remove tool. In other words, **the alternative auto-completion tools make people more considerate of the website's purpose in their disclosure decisions**.

Conclusion and Future work

In this paper we investigated the effect of form auto-completion on users' privacy calculus and purpose-specific information disclosure. Our study shows that users of traditional auto-completion tools are held back from engaging in the privacy calculus: we demonstrate that they are less likely to consider perceived risk and relevance in their decision to disclose, and they thus neglect the purpose specificity of the requested information. To remedy these problems, we introduced two alternative tools. Our study shows these tools indeed help users consider the perceived risk and relevance of each item in their decision making process. Consequently, users of these tools make decisions that are less biased and more purpose-specific.

Surprisingly, we found no default effect between the Add and Remove tool, even though disclosure requires more commitment in the Add condition (accept frame) than in the Remove condition (reject frame). In the discussion we argued that another effect could be counteracting this "commitment to accept" effect: the Add tool may have forced participants to think about the potential *positive* consequences of disclosure while the Remove tool forced them to consider the *negative* consequences. The effect of these positive and negative queries on decision-making have been extensively studied (Dinner et al. 2011). Future work could try to disentangle these opposing effects by changing one of the effects while keeping the other constant. One could for instance subtly change the required commitment to accept by making it a little harder (or even easier) to add/remove form field entries, or one could nudge users to think of positive or negative consequences of disclosure via query-supporting justifications (cf. Knijnenburg and Kobsa 2013a).

An unfortunate finding of our study is that we attain the best purpose specificity with the Remove tool (see Figure 5), while users are most satisfied with the Add tool. Is there a middle ground between these two versions? One option is to use a different default for each type of item, based on the specific purpose of the website: The FormFiller could automatically fill in the fields that match the purpose of the website, and leave all other fields blank. This FormFiller could derive the purpose of the website from some kind of ontology of websites, or simply ask the user. This tool would be purpose-specific by default, which means that users would not be required to engage in a privacy calculus any longer.

Despite the universal nature of context specificity, users may arguably still differ from one another with regards to what items they want to disclosure to which website (cf. Knijnenburg et al. 2013b). Having the "add" and "remove" buttons available will empower users to still tweak their disclosure beyond the purpose specific default. An additional step would be to learn from these adjustments, and make the default *user-adaptive* (Knijnenburg and Kobsa 2013b; Kobsa 2001; Wang and Kobsa 2007). We intend to explore the implications of "specific-by-default" and "fully-adaptive" form auto-completion in our future work.

References

Acquisti, A., and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), pp. 26–33.

Acquisti, A., and Grossklags, J. 2008. "What Can Behavioral Economics Teach Us About Privacy?," in *Digital Privacy: Theory, Technologies, and Practices*, A. Acquisti, S. De Capitani di Vimercati, S. Gritzalis, and C. Lambrinoudakis (eds.), Taylor & Francis, pp. 363–377.

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13–28.

Bamberger, K. A., and Mulligan, D. K. 2011. "Privacy on the Books and on the Ground," *Stanford Law Review* (63), pp. 247–316.

Bansal, G., Zahedi, F., and Gefen, D. 2008. "The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation," in *Proceedings of the 29th International Conference on Information Systems*, Paris, France, December 14, pp. 1528–1546.

Bentler, P. M., and Bonett, D. G. 1980. "Significance Tests and Goodness of Fit in the Analysis of Covariance Structures," *Psychological Bulletin* (88:3), pp. 588–606.

Besmer, A., Watson, J., and Lipford, H. R. 2010. "The impact of social navigation on privacy policy configuration," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, Redmond, Washington, July.

Bettman, J. R., Luce, M. F., and Payne, J. W. 1998. "Constructive consumer choice processes," *Journal of consumer research* (25:3), pp. 187–217.

Bhatnagar, A., Misra, S., and Rao, H. R. 2000. "On risk, convenience, and Internet shopping behavior," *Communications of the ACM* (43:11), pp. 98–105.

Bicakci, K., Atalay, N. B., and Kiziloz, H. E. 2011. "Johnny in internet café: user study and exploration of password autocomplete in web browsers," in *Proceedings of the 7th ACM workshop on Digital identity management*, Chicago, IL, pp. 33–42.

Bonneau, J., and Preibusch, S. 2010. "The Privacy Jungle:On the Market for Data Protection in Social Networks," in *Economics of Information Security and Privacy*, T. Moore, D. Pym, and C. Ioannidis (eds.), New York, NY: Springer US, pp. 121–167.

Borcea-Pfitzmann, K., Pfitzmann, A., and Berg, M. 2011. "Privacy 3.0 := Data Minimization + User Control + Contextual Integrity," *it - Information Technology* (53:1), pp. 34–40.

Brandimarte, L., Acquisti, A., and Loewenstein, G. 2013. "Misplaced Confidences: Privacy and the Control Paradox," *Social Psychological and Personality Science* (4:3), pp. 340–347.

Compañó, R., and Lusoli, W. 2010. "The Policy Maker's Anguish: Regulating Personal Data Behavior Between Paradoxes and Dilemmas," in *Economics of Information Security and Privacy*, T. Moore, D. Pym, and C. Ioannidis (eds.), New York, NY: Springer US, pp. 169–185.

Consolvo, S., Smith, I., Matthews, T., LaMarca, A., Tabert, J., and Powledge, P. 2005. "Location disclosure to social relations: why, when, & what people want to share," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Portland, OR, April, pp. 81–90.

Culnan, M. J. 1993. "'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), pp. 341–363.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104–115.

Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323–342.

Cunningham, S. 1967. "The major dimensions of perceived risk," in *Risk Taking and Information Handling in Consumer Behavior*, D. Cox (ed.), Boston, MA: Division of Research, Graduate School of Business Administration, Harvard University, pp. 82–108.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. "Privacy calculus model in e-commerce - a study of Italy and the United States," *European Journal of Information Systems* (15:4), pp. 389–402.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61–80.

Dinner, I., Johnson, E., Goldstein, D., and Liu, K. 2011. "Partitioning Default Effects: Why People Choose Not to Choose," *Journal of Experimental Psychology: Applied* (17:4), pp. 332–341.

EU. 1995. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data," No. L. 281, European Parliament.

Featherman, M. S., and Pavlou, P. A. 2003. "Predicting e-services adoption: a perceived risk facets perspective," *International Journal of Human-Computer Studies* (59:4), pp. 451–474.

Fishbein, M., and Ajzen, I. 1975. *Belief, attitude, intention, and behavior: an introduction to theory and research*, Reading, MA: Addison-Wesley Pub. Co.

FTC. 2000. "Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress," Federal Trade Commission.

Ganzach, Y. 1995. "Attribute Scatter and Decision Outcome: Judgment versus Choice," *Organizational Behavior and Human Decision Processes* (62:1), pp. 113–122.

Garrido, A., Rossi, G., and Distante, D. 2011. "Refactoring for Usability in Web Applications," *IEEE Software* (28:3), pp. 60–67.

Hann, I.-H., Hui, K.-L., Lee, S.-Y., and Png, I. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13–42.

Heller, D., Levin, I. P., and Goransson, M. 2002. "Selection of strategies for narrowing choice options: Antecedents and consequences," *Organizational Behavior and Human Decision Processes* (89:2), pp. 1194–1213.

Hine, C., and Eve, J. 1998. "Privacy in the Marketplace," *The Information Society* (14:4), pp. 253–262.

Hoffman, D. L., Novak, T. P., and Peralta, M. 1999. "Building consumer trust online," *Communications of the ACM* (42:4), pp. 80–85.

Hsu, C. (Julia). 2006. "Privacy concerns, privacy practices and web site categories: Toward a situational paradigm," *Online Information Review* (30:5), pp. 569–586.

Hu, L., and Bentler, P. M. 1999. "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1–55.

Jacoby, J., and Kaplan, L. B. 1972. "The Components of Perceived Risk," in *Proceedings of the Third Annual Conference of the Association for Consumer Research*, M. Venkatesan (ed.), Chicago, IL, pp. 382–393.

Johnson, E. J., Bellman, S., and Lohse, G. L. 2002. "Defaults, Framing and Privacy: Why Opting In ≠ Opting Out," *Marketing Letters* (13:1), pp. 5–15.

Johnson, E. J., and Goldstein, D. 2003. "Do Defaults Save Lives?," *Science* (302:5649), pp. 1338–1339.

Johnson, M., Egelman, S., and Bellovin, S. M. 2012. "Facebook and privacy: it's complicated," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, Pittsburgh, PA.

Kairam, S., Brzozowski, M., Huffaker, D., and Chi, E. 2012. "Talking in circles," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Austin, TX, pp. 1065–1074.

Keeney, R. L., and Raiffa, H. 1976. *Decisions with Multiple Objectives: Preferences and Value Trade-Offs*, New York: Wiley.

Keith, M. J., Babb, J. S., Paul Benjamin Lowry, Furner, C. P., and Abdullat, A. 2011. "The Roles of Privacy Assurance, Network Effects, and Information Cascades in the Adoption of and Willingness to Pay for Location-Based Services with Mobile Applications," in *2011 Dewald Roode Information Security Workshop*, Blacksburg, VA, September.

Kim, D. J., Ferrin, D. L., and Rao, H. R. 2008. "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision Support Systems* (44:2), pp. 544–564.

Kittur, A., Chi, E. H., and Suh, B. 2008. "Crowdsourcing user studies with Mechanical Turk," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Florence, Italy, April, pp. 453–456.

Knijnenburg, B. P., and Kobsa, A. 2013a. "Making Decisions about Privacy: Information Disclosure in Context-Aware Recommender Systems," *ACM Transactions on Interactive Intelligent Systems* (3:3).

Knijnenburg, B. P., and Kobsa, A. 2013b. "Helping users with information disclosure decisions: potential for adaptation," in *Proceedings of the 2013 ACM international conference on Intelligent User Interfaces*, Santa Monica, CA, March, pp. 407–416.

Knijnenburg, B. P., Kobsa, A., and Jin, H. 2013a. "Preference-based location sharing: are more privacy options really better?," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Paris, France, pp. 2667–2676.

Knijnenburg, B. P., Kobsa, A., and Jin, H. 2013b. "Dimensionality of information disclosure behavior," *International Journal of Human-Computer Studies* .

Knijnenburg, B. P., Willemsen, M. C., Gantner, Z., Soncu, H., and Newell, C. 2012. "Explaining the user experience of recommender systems," *User Modeling and User-Adapted Interaction* (22:4-5), pp. 441–504.

Kobsa, A. 2001. "Tailoring Privacy to Users' Needs (Invited Keynote)," in *User Modeling 2001*, Lecture Notes in Computer Science, M. Bauer, P. J. Gmytrasiewicz, and J. Vassileva (eds.), Springer Verlag, pp. 303–313.

Lai, Y.-L., and Hui, K.-L. 2006. "Internet Opt-In and Opt-Out: Investigating the Roles of Frames, Defaults and Privacy Concerns," in *Proceedings of the 2006 ACM SIGMIS CPR Conference on Computer Personnel Research*, Claremont, CA, pp. 253–263.

Larose, R., and Rifon, N. J. 2007. "Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior," *Journal of Consumer Affairs* (41:1), pp. 127–149.

Laufer, R. S., Proshansky, H. M., and Wolfe, M. 1973. "Some Analytic Dimensions of Privacy," in *Proceedings of the Lund Conference on Architectural Psychology*, R. Küller (ed.), Lund, Sweden.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22–42.

Lederer, S., Hong, J. I., Dey, A. K., and Landay, J. A. 2004. "Personal privacy through understanding and action: five pitfalls for designers," *Personal and Ubiquitous Computing* (8:6), pp. 440–454.

Levin, I. P., Huneke, M. E., and Jasper, J. D. 2000. "Information Processing at Successive Stages of Decision Making: Need for Cognition and Inclusion–Exclusion Effects," *Organizational Behavior and Human Decision Processes* (82:2), pp. 171–193.

Li, H., Sarathy, R., and Xu, H. 2010. "Understanding situational online information disclosure as a privacy calculus," *Journal of Computer Information Systems* (51:1), pp. 62–71.

Li, H., Sarathy, R., and Xu, H. 2011. "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors," *Decision Support Systems* (51:3), pp. 434–445.

Li, X., and Santhanam, R. 2008. "Will it be Disclosure or Fabrication of Personal Information? An Examination of Persuasion Strategies on Prospective Employees," *International Journal of Information Security and Privacy* (2:4), pp. 91–109.

Li, Y. 2012. "Theories in online information privacy research: A critical review and an integrated framework," *Decision Support Systems* (54:1), pp. 471–481.

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

Meloy, M. G., and Russo, J. E. 2004. "Binary choice under instructions to select versus reject," *Organizational Behavior and Human Decision Processes* (93:2), pp. 114–128.

Metzger, M. J. 2007. "Communication privacy management in electronic commerce," *Journal of Computer-Mediated Communication* (12:2), pp. 335–361.

Milne, G. R., and Gordon, M. E. 1993. "Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract Framework," *Journal of Public Policy & Marketing* (12:2), pp. 206–215.

Mohamed, N., and Ahmad, I. H. 2012. "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Computers in Human Behavior* (28:6), pp. 2366–2375.

Nissenbaum, H. 2004. "Privacy as Contextual Integrity," *Washington Law Review* (79), pp. 119–157.

Nissenbaum, H. F. 2010. *Privacy in context : technology, policy, and the integrity of social life*, Stanford, CA: Stanford Law Books.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100–126.

OECD. 1980. "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," Organization for Economic Co-operation and Development.

Olivero, N., and Lunt, P. 2004. "Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control," *Journal of Economic Psychology* (25:2), pp. 243–262.

Olson, J. S., Grudin, J., and Horvitz, E. 2005. "A study of preferences for sharing and privacy," in *Extended abstracts on Human factors in computing systems*, Portland, OR, pp. 1985–1988.

Pavlou, P. A. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce* (7:3), pp. 101–134.

Pavlou, P. A. 2011. "State of the Information Privacy Literature: Where Are We Now and Where Should We Go," *MIS Quarterly* (35:4), pp. 977–988.

Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*, Albany, NY: State University of New York Press.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing* (19:1), pp. 27–41.

Preibusch, S., Krol, K., and Beresford, A. R. 2012. "The Privacy Economics of Voluntary Over-disclosure in Web Forms," in *10th Annual Workshop on the Economics of Information Security*, Berlin, Germany.

Rust, R. T., Kannan, P. K., and Peng, N. 2002. "The Customer Economics of Internet Privacy," *Journal of the Academy of Marketing Science* (30:4), pp. 455–464.

Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., and Rao, J. 2009. "Understanding and capturing people's privacy policies in a mobile social networking application," *Personal and Ubiquitous Computing* (13:6), pp. 401–412.

Samuelson, W., and Zeckhauser, R. 1988. "Status quo bias in decision making," *Journal of Risk and Uncertainty* (1:1), pp. 7–59.
Shafir, E. 1993. "Choosing versus rejecting: why some options are both better and worse than others," *Memory & cognition* (21:4), pp. 546–556.
Sheehan, K. B., and Hoy, M. G. 2000. "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy & Marketing* (19:1), pp. 62–73.
Simon, H. A. 1959. "Theories of Decision-Making in Economics and Behavioral Science," *The American Economic Review* (49:3), pp. 253–283.
Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. J. 2006. "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7:1).
Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989–1015.
Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167–196.
Stone, D. L. 1981. "The effects of the valence of outcomes for providing data and the perceived relevance of the data requested on privacy-related behaviors, beliefs, and attitudes," PhD Thesis, Purdue University.
Stone, E. F., and Stone, D. L. 1990. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8), pp. 349–411.
Thaler, R. H., and Sunstein, C. 2008. *Nudge : improving decisions about health, wealth, and happiness*, New Haven, NJ & London, U.K.: Yale University Press.
Trewin, S. 2006. "Physical usability and the mobile web," in *Proceedings of the 2006 international cross-disciplinary workshop on Web accessibility (W4A): Building the mobile web: rediscovering accessibility?*, Edinburgh, U.K., pp. 109–112.
Wang, Y., and Kobsa, A. 2007. "Respecting Users' Individual Privacy Constraints in Web Personalization," in *User Modeling 2007*, Lecture Notes in Computer Science, C. Conati, K. McCoy, and G. Paliouras (eds.), Corfu, Greece: Springer Berlin / Heidelberg, pp. 157–166.
Watson, J., Besmer, A., and Lipford, H. R. 2012. "+Your circles: sharing behavior on Google+," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, Pittsburgh, PA.
Wedell, D. H. 1997. "Another look at reasons for choosing and rejecting," *Memory & Cognition* (25:6), pp. 873–887.
White House. 2012. "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy," Washington, D.C.: White House.
White, T. B. 2004. "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework," *Journal of Consumer Psychology* (14:1&2), pp. 41–51.
Wilson, D., and Valacich, J. 2012. "Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus," in *Proceedings of the International Conference on Information Systems*, Orlando, FL, December 14.
Wroblewski, L. 2008. *Web Form Design: Filling in the Blanks*, Brooklyn, NY: Rosenfeld Media.
Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the formation of individual's privacy concerns: Toward an integrative view," in *Proceedings of the 29th International Conference on Information Systems*, Paris, France, pp. 1981–1996.
Xu, H., Luo, X. (Robert), Carroll, J. M., and Rosson, M. B. 2011. "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decision Support Systems* (51), pp. 42–52.
Xu, H., Teo, H.-H., and Tan, B. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk," in *Proceedings of the International Conference on Information Systems*, Las Vegas, NV, December 31, pp. 861–874.
Xu, H., Teo, H.-H., Tan, B., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135–174.
Yao, M. Z., Rice, R. E., and Wallis, K. 2007. "Predicting user concerns about online privacy," *Journal of the American Society for Information Science and Technology* (58:5), pp. 710–722.
Youn, S. 2009. "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents," *Journal of Consumer Affairs* (43:3), pp. 389–418.

Zhou, T. 2012. "Examining Location-based Services Usage from the Perspectives of Unified Theory of Acceptance and Use of Technology and Privacy Risk," *Journal of Electronic Commerce Research* (13:2), pp. 135–144.