Summer 6-15-2016

EXPLORING THE IMPACT OF READABILITY OF PRIVACY POLICIES ON USERS' TRUST

Tatiana Ermakova
University of Potsdam, tatiana.ermakova@uni-potsdam.de

Hanna Krasnova
University of Potsdam, krasnova@uni-potsdam.de

Benjamin Fabian
Humboldt-University Berlin, bfabian@wiwi.hu-berlin.de

EXPLORING THE IMPACT OF READABILITY OF PRIVACY POLICIES ON USERS' TRUST

Research

Ermakova, Tatiana, University of Potsdam, Potsdam, Germany, tatiana.ermakova@uni-potsdam.de

Krasnova, Hanna, University of Potsdam, Potsdam, Germany, krasnova@uni-potsdam.de

Fabian, Benjamin, Humboldt-Universität zu Berlin, Berlin, Germany, bfabian@wiwi.hu-berlin.de

Abstract

Empirical studies have repeatedly pointed out that the readability of a privacy policy is a potential source of trust of online users. Nevertheless, many online companies still keep the readability of their privacy policies at a low level. This could possibly coincide with a low compliance of their privacy policies with the guidelines of fair information practices and thus with users' privacy expectations. Against this background, this study seeks to clarify the role of perceived and actual readability of user-friendly and -unfriendly privacy policies in shaping user's trust in a mobile service provider. Tested for two different mobile service scenarios that differ in the sensitivity of user data (educational entertainment app vs. health app), our hypotheses are verified based on the responses of 539 online users. Our findings reveal that in the case of a user-unfriendly data-handling policy, the effect of actual readability of a privacy policy outweighs the effect of its perceived readability in forming users' trust. At the same time, for a user-friendly privacy policy, only perceived readability plays a significant role in promoting users' trust in the provider of an educational entertainment app. In a sensitive healthcare context, however, perceived and actual readability of privacy policies are almost equally important.

Keywords: Trust, Privacy, Privacy Policy, Readability.

Introduction

With the advancements in information technologies, personal data became easier to gather and utilize by online companies and, consequently, the subject of Internet users' growing concerns (Malhotra et al., 2004; Smith et al., 1996, 2011; Bélanger and Crossler, 2011; Pavlou, 2011; Reidenberg et al., 2015b). As of December 2013, 55% of British consumers moderately trusted most online companies to protect their personal information, and only one out of twenty (5%) perceived a high level of trust (TRUSTe, 2015).

Amidst these rather low levels of trust in online businesses, the content and presentation of privacy policies is gaining considerable attention. Indeed, privacy policies are often the only means to gain insights into companies' practices with regard to users' personal data (Vail et al., 2008; Reidenberg et al., 2015a). However, empirical evidence shows that about three out of four available privacy policies remain unread (Jensen et al., 2005; Acquisti and Gross, 2006). A possible reason may be rooted in their poor readability (Graber et al., 2002; Jensen and Potts, 2004; Pollach, 2005; Sheehan, 2005; Antón et al., 2004; Proctor et al., 2008; McDonald and Cranor, 2008; McDonald et al., 2009; Sunyaev et al., 2014; Ermakova et al., 2015; Cadogan, 2010), and this despite significant efforts directed at improving this situation (Kelley et al., 2009; Pan and Zinkhan, 2006; Vu et al., 2007). Nevertheless, by

publishing easy-to-read policies and encouraging users to read them (Milne and Culnan, 2004), online companies can strengthen their trust (Ermakova et al., 2014; Sultan et al., 2002; Bansal et al., 2008a, 2008b). Moreover, with a strong guarantee of security, privacy policies are even more effective than high-cost third-party seals (Peterson et al., 2007).

One of the explanations for this phenomenon could be that online privacy statements rarely fully comply with the guidelines of fair information practices such as those proposed by the Federal Trade Commission (FTC, 2000) (Adkinson et al., 2002; O'Connor, 2003; Peslak, 2005; Carrión et al., 2012; Goldman et al., 2000; Pollach, 2004; Ryker et al., 2002; Sheehan, 2005; Cranor et al., 2014) and, therefore, are unlikely to meet users' privacy expectations (Earp et al., 2005). This, in turn, may motivate online companies to obscure their content. Indeed, as a result of ambiguous wording typically used in privacy policies, the ability to communicate data-handling practices to the general public is impaired. However, the question of whether or not this possibly opportunistic behaviour is beneficial for companies remains unclear.

Against this background, our study seeks to clarify and empirically demonstrate the roles of perceived and actual readability of privacy policies in explaining users' trust in a mobile service provider in the context of user-friendly and user-unfriendly privacy policies. In this study, we refer to the perceived readability of a privacy policy as to the degree to which the policy is seen as clearly formulated; and to actual readability as to the extent to which the policy is correctly understood. Based on a survey with 539 online users located in Germany, we verify our hypotheses on the basis of two mobile service scenarios that differ with regard to the sensitivity of user information involved.

In what follows, theoretical foundations for studying readability of privacy policies and trust are established by reviewing prior relevant studies. The subsequent section introduces the reasoning underlying the developed research hypotheses before presenting them. The research method and results of data analyses are presented next, followed by a discussion of the key findings and practical implications.

1 Theoretical Background

1.1 Trust

The concept of trust has been extensively examined from a variety of perspectives (Mayer et al., 1995; Grabner-Kräuter and Kaluscha, 2003). This stream of research generally concludes that consumers' trust is an important source of their attitude towards online businesses (Jarvenpaa et al., 1999, 2000), their intentions to share information for transactions (Dinev and Hart 2006; Bansal et al., 2007, 2008a, 2008b, 2010; Malhotra et al., 2004) and to transact online (Gefen, 2000; Gefen et al., 2003; Gefen and Straub, 2004; Dinev et al., 2006). In a mobile environment, insufficient trust might result in user intention to terminate the relationship with the phone service provider (Mamonov and Koufaris, 2014). In one of the earlier empirical studies, Mayer et al. (1995) claim that trusting implies the trustor's willingness to be vulnerable to the trustee's actions being of importance to the trustor, regardless of her monitoring abilities. Mayer et al. (1995) distinguish trust from perceived trustworthiness of the trustee, and conceptualize trust as a composite of three dimensions - ability, benevolence, and integrity. Ability refers to the trustor's beliefs about the trustee's domain-specific competences. Benevolence measures the degree to which the trustee is anticipated to have good intentions apart from seeking profit. Integrity reflects the extent to which the trustee is expected to adhere to some principles acceptable for the trustor.

1.2 Privacy Policies

Privacy describes the ability of a person to manage when, how, and to what extent her personal information is revealed to others (Westin, 1967). Online privacy is addressed by several regulations such as Directive 95/46/EC by the European Parliament and Council (European Parliament and Council,

1995) and Fair Information Practice Principles (FIPP) by the United States Federal Trade Commission (FTC, 2000). Among other principles, they enforce that consumers should be given notice before any of their personal information is collected and should be enabled to make a choice related to secondary uses of any of their personal information (Bansal et al., 2008a; Xu et al., 2012; Reidenberg et al., 2015a). In practice, online privacy policies often represent the only medium to inform users how the company collects and uses their personal data and to enable them to decide whether to agree with these practices and engage with the company or not (Vail et al., 2008; Reidenberg et al., 2015a).

1.3 Readability

Readability reflects "*the ease of understanding or comprehension due to the style of writing*" (Klare, 1963). As such, readability can be viewed as an interaction between some characteristics of a text and a reader (Harris and Hodges, 1995). For a reader, these aspects include her knowledge, reading skills, interest and motivation. For example, Reidenberg et al. (2015a) demonstrate that expert, knowledgeable and typical users interpret privacy policies differently. For a text, they involve content, design, organization and style (DuBay, 2007). Klare (1963) differentiates between two ways researchers assess readability of a text: They either employ a readability test on readers (e.g., Milne and Culnan, 2004; Fanguy et al., 2004; Proctor et al., 2008; McDonald et al., 2009; Singh et al., 2011; Ermakova et al., 2014; Sultan et al., 2002; Bansal et al., 2008a, 2008b; Cadogan, 2010) or count language elements in the text such as syllables, words, and sentences (e.g., Graber et al., 2002; Jensen and Potts, 2004; Antón et al., 2004; Sunyaev et al., 2014; McDonald and Cranor, 2008; Ermakova et al., 2015; Cadogan, 2010). There are some well-established formulas to measure text readability based on language elements counts, which involve Flesch Readability Ease Score (FRES) (Flesch, 1948), Laesbarhedsindex (LIX) (Anderson, 1983), New Dale Chall Score (NDC) (Dale and Chall, 1995), Flesh-Kincaid Grade Level (FKG) (Kincaid et al., 1975), Readability Index (RIX) (Anderson, 1983), Simple Measure of Gobbledygook (SMOG) (McLaughlin, 1969), Coleman-Liau Index (CLI) (Coleman and Liau, 1975), Gunning Fog Index (GFI) (Gunning, 1952), Automated Readability Index (ARI) (Senter and Smith, 1967) and Fry Readability Graph (Fry) (Fry, 1963) (Shedlosky-Shoemaker et al., 2008). Nevertheless, their capabilities to measure the readability of text materials are rather limited. Singh et al. (2011) primarily criticize their underlying assumptions that imply that shorter sentences and words are easier to comprehend than longer ones. Especially related to a mobile environment, they argue that writing style, logical structure, display challenges, textual features (e.g., bullets, font size) and user-specific knowledge should be included into readability assessments.

1.4 Readability of Privacy Policies: Perceived vs. Actual Readability

Prior investigations based on the readability metrics repeatedly indicate that privacy policies generally suffer from poor readability (Graber et al., 2002; Jensen and Potts, 2004; Pollach, 2005; Antón et al., 2004; Proctor et al., 2008; McDonald and Cranor, 2008; McDonald et al., 2009; Sunyaev et al., 2014; Ermakova et al., 2015; Cadogan, 2010). This, however, can be intentional, since using ambiguous wording in privacy policies can weaken their ability to communicate undesirable data-handling practices to the general public. The latest large-scale empirical study demonstrates that a privacy-policy reader on average needs to have a college education or a formal education of 16 years, or the 13th reading grade level (Ermakova et al., 2015). Furthermore, Reidenberg et al. (2015a) show discrepancies in interpretation of privacy policies among expert, knowledgeable, and typical users.

In this research, we take the individual perspective and further distinguish between perceived and actual readability of a privacy policy. Perceived readability of a privacy policy aims to measure to what degree the policy is viewed as clearly formulated, while actual readability of a privacy policy relates to what extent individuals understand the policy correctly. Similar to Brecht et al. (2012), this differentiation can be supported by the suggestion that individuals might overestimate or underestimate their ability to process the information in the privacy notice.

The concept of perceived readability of privacy policy is captured through the concepts of existing models such as understandability (Bansal et al., 2008a), perceived comprehension (Milne and Culnan 2004), and perceived readability (Ermakova et al., 2014), and ease of finding information (McDonald et al., 2009). The concept of ease of finding information refers to individuals' ability to understand some policy (McDonald et al., 2009).

The constructs from other models that are mostly close to actual readability of privacy policy involve adequacy (Bansal et al., 2008a), actual readability (Ermakova et al., 2014; Fanguy et al., 2004; Singh et al., 2011), and comprehension (McDonald et al., 2009; Proctor et al., 2008) of privacy policy, where comprehension of privacy policy is measured by asking participants a series of multiple choice questions (McDonald et al., 2009; Proctor et al., 2008). Ermakova et al. (2014), Fanguy et al. (2004) and Singh et al. (2011) employ the so-called cloze test (Taylor, 1953) to find out how privacy policies were really understood. Specifically, participants had to replace blanks in the given notice with appropriate words, where a higher number of correctly filled in blanks were associated with better readability of the notice for that reader.

1.5 Readability of Privacy Policies and Trust

Among a variety of factors shaping trust between users and service providers, adequacy (Bansal et al., 2008a, 2008b), understandability (Bansal et al., 2008a, 2008b; Ermakova et al., 2014; Sultan et al. 2002) and presentation (Pan and Zinkhan, 2006) of privacy policies have been the subject of empirical investigations. Similarly to Ermakova et al. (2014), the present research relates the effects of both perceived and actual readability of a privacy policy to individual trust. In comparison to Ermakova et al. (2014), who conduct their investigations within the context of five renowned Internet services, this work concentrates on two examples of mobile services that deal with differently sensitive information.

2 Research Model and Hypothesis Development

2.1 Effect of Perceived Readability of Privacy Policies on Trust

A number of studies have dealt with the question of whether perceived readability of online privacy statements contributes to consumer trust towards the Web site (Ermakova et al., 2014; Sultan et al., 2002; Bansal et al., 2008a, 2008b; Pan and Zinkhan, 2006). However, the findings remain contradictory. In one of the earliest works on this issue, Sultan et al. (2002) show that having an easy-to-understand privacy policy helps e-businesses to earn their customers' trust. However, Pan and Zinkhan (2006) could not confirm the significance of the impact of the presentation of a privacy policy regarding its length and terminology on online shoppers' trust. Later, Bansal et al. (2008a, 2008b) concluded that in the health context people rely on the understandability of the privacy-policy statement to shape their trust in the website, but only in the presence of high privacy concerns. However, in the finance and e-commerce context, Bansal et al. (2008a) could not confirm this relationship. Recently, Ermakova et al. (2014) has observed a highly significant positive impact of perceived readability of privacy policies on online users' trust across five contexts they have investigated, i.e., eBay, Yahoo, Amazon, Facebook and Twitter.

In this research, we assume that consumers will be more likely to develop trust in the mobile application provider if they perceive that a corresponding privacy policy statement is written in a language that they can easily read and follow. Thus, we argue that:

Hypothesis 1: *Perceived readability of a privacy policy will be* ***positively*** *associated with trust in the mobile application provider*.

2.2 Effect of Actual Readability of Privacy Policies on Trust

There are some indications that actual readability of privacy policies might be essential for shaping online users' trust, as well (Bansal et al., 2008a, 2008b; Ermakova et al. 2014). For example, Ermakova et al. (2014) observe a positive and significant impact of actual readability of a privacy policy on online users' trust, however only in the context of Amazon. Furthermore, Bansal et al. (2008a) demonstrate that people significantly rely on the adequacy of the website privacy policy statement in establishing their trust in health, finance and e-commerce websites. This relationship did not hold only for highly concerned individuals in the health context, but was observed in the study by Bansal et al. (2008b). Peterson et al. (2007) conclude that a strong guarantee of security in the privacy policy statement enhances trust of online users to an even greater extent than third-party seals. Therefore, we include actual readability of privacy policies as a determinant of trust in our research model. We posit that the relationship between the extent to which the privacy policy statement was understood and trust in the mobile app provider will depend on the user-friendliness of the privacy policy statement:

Hypothesis 2a: *In case of a user-friendly privacy policy, its actual readability will be* ***positively*** *associated with trust in the mobile application provider.*

Hypothesis 2b: *In case of a user-unfriendly privacy policy, its actual readability will be* ***negatively*** *associated with trust in the mobile application provider.*

Figure 1 illustrates the developed research model. Here, we differentiate between user-friendly and user-unfriendly data-handling practices that underlie a specific privacy policy statement.

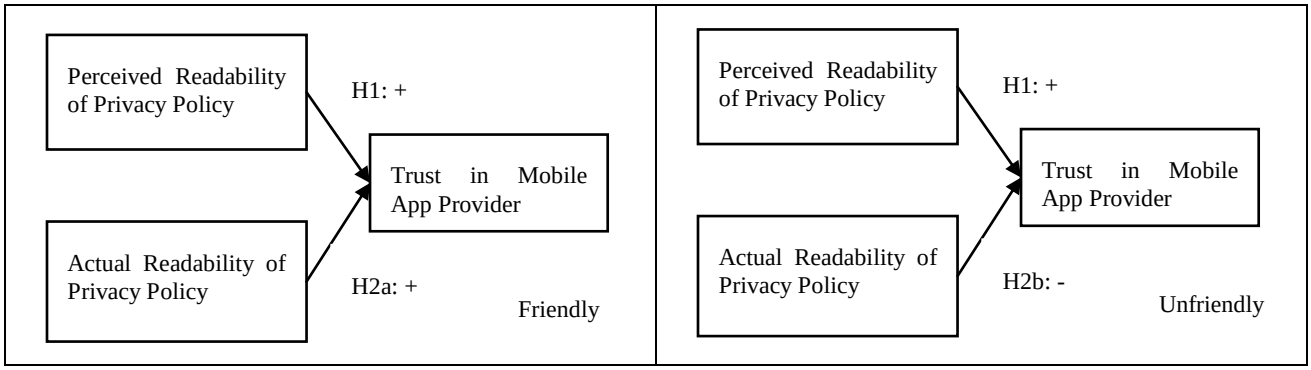

Figure 1. Research model.

3 Research Method

3.1 Experimental Design and Manipulation

A survey-based between-subject experimental study was conducted. A mobile app environment was chosen as a context of our study. This is because readability and presentation of privacy policies may be particularly important in the mobile environment, since mobile readers additionally have to deal with a smaller display, limited interface features and input facilities, as well as physical inconveniences resulting from their mobility, and higher costs for mobile Internet (Singh et al., 2011).

To vary the sensitivity of data involved, two mobile application scenarios were used - BloodScan and DropSpot. As presented to the respondents, the BloodScan mobile app allows users to easily import and store their (sensitive) healthcare data (e.g., blood or allergy tests), monitor their health as well as share health-related information with medical workers (see Figure 2). Positioned within the "educational entertainment" category, the DropSpot mobile app utilizes user location data to inform users about everything worth seeing on their way to work or during their holiday (see Figure 3). As part of

the app functionality, users are allowed to choose topics which interest them most (e.g., "history", "the greatest crime", "scientific discoveries", "movies"). While also valuable, location based-data as well as information about user preferences involved in the DropSpot app is likely to be perceived as less sensitive than health data (Laric et al., 2009).

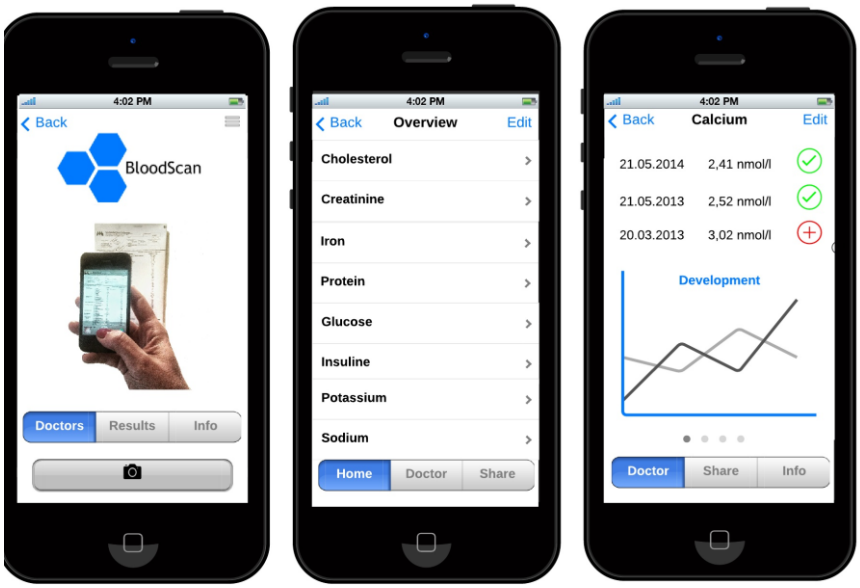

Figure 2. BloodScan mobile app.

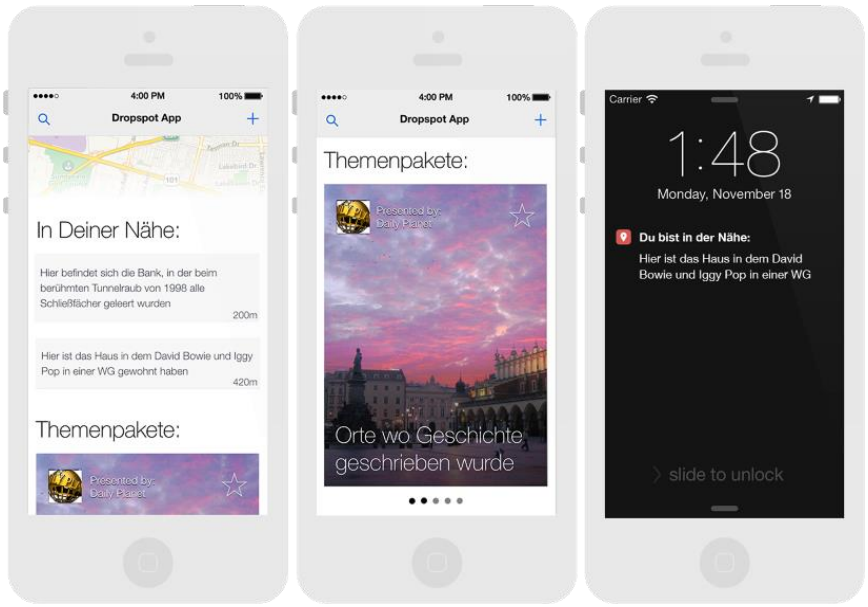

Figure 3. DropSpot mobile app.

To test our hypotheses, privacy policies with different data-handling practices (user-friendly and user-unfriendly) and different levels of readability (easy- and difficult-to-read) were developed, and their effects on the way how their perceived and actual readability impacted the trust of mobile app users were examined (see Table 1). Here, we relied on the eye-tracking-based findings of Vu et al. (2007) who show that when reading privacy policies, people first consult the section listings or, when these are not present, the headings and the very beginning of each paragraph throughout the entire privacy

policy statement. Furthermore, to ensure enough variation in both perceived and actual readability measures, we followed the finding of Pan and Zinkhan (2006) who argue that short, straightforward privacy policies are easier to comprehend than lengthy, legalistic ones. As shown in Table 1, the privacy policies were created so that they differed across four major dimension of user privacy concerns - data collection, (internal and external) unauthorized secondary use, unauthorized access and errors (Smith et al., 1996). Additionally, the data longevity dimension was covered, considering the salience of this issue in the context of new social media platforms (Prunty and Swartendruber, 2015). The privacy policies were developed in German, since German-speaking participants were the target group for our survey from the start.

Category	User-Friendly		User-Unfriendly	
Version	Easy	Difficult	Easy	Difficult
Collection	**Which information do I have to provide when I register on the app? For example, do I have to provide my full name?** When you register on our app, we will only ask you to provide a nickname. You do not need to provide your full name, birth date, email address or postal code.	When creating a user account for our application, you will be only requested to provide a nickname, without you being obliged to provide your full name, birth date or email address or postal code.	**Which information do I have to provide when I register on the app? For example, do I have to provide my full name?** When you register on our app, we will ask you to provide your true full name. You may also need to provide your birth date, email address and postal code.	When creating a user account for our application, you will be requested to provide your true full name, and may as well as be obliged to provide your birth date and email address as well as your postal code.
	What kind of information does the app collect? We only collect information that is needed to run the app. We do not store your interactions within the app. We also do not store any other information generated by using the app.	Since information collection is restricted to the amount that is necessary to achieve the intended purpose of the application, neither your interactions within the application will be stored, nor any other information provided by your usage of the application will be preserved.	**What kind of information does the app collect?** We will not only collect information which is needed to run the app. Where required, we may store your interactions within our app. We may also store any other information generated by using the app.	Since information collection is not restricted to the amount that is necessary to achieve the intended purpose of the application, your interactions within the application may be stored, and any other information provided by your usage of the application may be preserved.
Unauthorized Secondary Use (Internal)	**Do you use cookies from third parties?** No, we also do not use cookies from third parties.	Furthermore, in the course of your usage of the application we are not entitled to employ cookies from third parties.	**Do you use cookies from third parties?** We may also use cookies from third parties.	Furthermore, in the course of your usage of the application we are entitled to employ cookies from third parties.
Unauthorized Secondary Use (External)	**Do you share my information with third parties? Or use it for advertising purposes?** No, we do not share any of your personal or aggregated information with third parties such as research institutes, agencies and public authorities, or providers of products and services that are of interest to you. Also, we will not use your information for advertising purposes, market research or newsletters.	Moreover, you are hereby not granting us the right that your personal or aggregated information is shared with third parties, such as research institutes, agencies and public authorities, or providers of products and services that are of interest to you, or on our part may be used for purposes of advertising, market research or a newsletter providing you with further information optimally tailored to your interests.	**Do you share my information with third parties? Or use it for advertising purposes?** Yes, we may share your personal or aggregated information with third parties such as research institutes, agencies and public authorities, or providers of products and services that are of interest to you. Where required, we also use your information for advertising purposes, market research or newsletters.	Moreover, you are hereby granting us the right that your personal or aggregated information is shared with third parties, such as research institutes, agencies and public authorities, or providers of products and services that are of interest to you, or on our part may be used for purposes of advertising, market research or a newsletter providing you with further information optimally tailored to your interests.
Errors	**May I check my data at any time?**	You may at any time and without stating any reasons receive information	**May I check my data at any time?**	Only by declaring special conditions you may receive information about the data

	Yes, you may access and check your data any time, without stating a reason.	about the data that is stored in reference to your nickname and may verify them for correctness.	No, you may access and check your data under special conditions.	that is stored in reference to your person, or verify them for correctness.
Unauthorized Access	**How does the company handle my data?** Our employees may only access your data with your consent.	Any access to your data by our employees is only possible with your explicitly granted consent.	**How does the company handle my data?** Our employees may access your data when needed, even without your consent.	Any access to your data by our employees is possible when needed, even without your explicitly granted consent.
Data Longevity	**What happens to my data if I do not want to use the app anymore?** When you do not want to use our app anymore, we will delete your account and information forever.	Once your usage of our service ceases to be desired any further, your account and all related information will be irretrievably deleted.	**What happens to my data if I do not want to use the app anymore?** When you do not want to use our app any more, we will deactivate your account. Where required, your information is preserved.	Once your usage of our service ceases to be desired any further, your account will be deactivated; but we maintain the right to further preserve your information.

Table 1. Privacy policies (translation).

3.2 Operationalization of Variables and Pilot Study

To measure perceived readability of a privacy policy, the scales developed by Milne and Culnan (2004) and Bansal et al. (2008a) were adapted (see Table 2). To assess actual readability of privacy policy, we derived a set of questions close to the content of the privacy policies used within our study. In the evaluation phase, the score of right answers has been derived and used as an indicator of actual readability. Clearly, for friendly privacy policies higher scores indicated the higher number of "privacy"-friendly practices recipients actually understood and internalized with respect to the privacy policy they were presented. In contrast, for unfriendly privacy policies higher score indicated the higher number of "privacy"-unfriendly practices recipients understood. To measure trust, we relied on the operationalization by McKnight et al. (2002), focusing only on the benevolence and integrity dimensions. The items to measure perceived user-friendliness of privacy policy were inspired by Xu et al. (2008), and served as a manipulation check in our study. 7-point scales were used throughout the study, where applicable.

Construct	Items	Source
Perceived Readability of Privacy Policy	To what extent do you agree with the statements? The privacy policy of this app… 1. … is written in an unclear legal language. 2. … contains confusing terms. 3. … is hard to understand. 4. … is incomprehensibly formulated. *Answer Categories: Strongly agree – Strongly disagree*	Milne and Culnan (2004), Bansal et al. (2008a)
Actual Readability of Privacy Policy	1. For the app you need to specify only your nickname. 2. Your interactions within the app may be stored. 3. The app may use third-party cookies. 4. Your information may be shared with third parties. 5. Your information may be used for promotional purposes. 6. You can always access your data. 7. The staff of the app-provider may access your data only with your consent.	Self-developed

	8. When you terminate your use of the app, your information will be deleted by the app-provider. *Answer Categories: Yes – No – Not sure*	
Perceived User-Friendliness of Privacy Policy	The privacy policy of this app…. 1. … assures that my data will not be misused. 2. … reflects the commitment of the provider to privacy. 3. …is privacy friendly. 4. …signals the readiness of the provider to protect the privacy of my data. 5. …respects the privacy of my information. 6. …asserts that my information will be treated with confidentiality. *Answer Categories: Strongly disagree – Strongly agree*	Inspired by Xu et al. (2008)
Trust	I believe that the app provider… 1. … would do her best to help me if I need help. (Benevolence) 2. … would act in my best interest. (Benevolence) 3. … is interested in my well-being, not just her own. (Benevolence) 4. … is to be characterized as honest. (Integrity) 5. … appears sincere and genuine. (Integrity) 6. … would keep its commitments. (Integrity) *Answer Categories: Strongly disagree – Strongly agree*	McKnight et al. (2002)
Perceived Information Sensitivity	All in all, the information this app deals with is: 1. Not sensitive at all – Very sensitive 2. Not personal at all – Very personal	Self-developed

Table 2. Research model constructs and related questionnaire items.

3.3 Procedure and Task

Participants were randomly assigned to view the description of one of the mobile applications (BloodScan or DropSpot). Specifically, they were presented with a screenshot of the mobile application and given a short description of its main features. Participants were then asked about their sensitivities related to the information the mobile application dealt with ("perceived information sensitivity" construct, see Table 2). In the next step, participants were randomly assigned to one of the privacy policy conditions (friendly vs. unfriendly and easy- vs. difficult-to-read). Next, respondents rated their perceived readability of the privacy policy and their trust towards the mobile application provider, as well as answered a set of questions regarding data-handling practices of the mobile application provider based on the privacy policy they just read to assess actual readability. Additionally, respondents were asked to provide other information necessary for manipulation and control checks.

3.4 Participants

We conducted our online survey from February 22nd to March 7th 2015 and recruited study participants via university mailing lists. From a total of 810 participants who followed the provided link, 539 fully completed the questionnaire. The completion rate thus amounted to 59.14%. Table 3 displays sample sizes, demographics of the respondents and other characteristics across the specified groups.

Mobile application	BloodScan		DropSpot		Combined	
Type of privacy policy in terms of user-friendliness	Unfriendly	Friendly	Unfriendly	Friendly	Unfriendly	Friendly
Number of responses	116	123	157	143	273	266
Mean age (SD: Standard Deviation)	25.74 (6.21)	27.24 (8.22)	25.89 (6.19)	25.61 (6.28)	25.83 (6.19)	26.37 (7.28)
Gender: Female	66 (56.9%)	77 (62.6%)	87 (55.4%)	87 (60.8%)	153 (56%)	164 (61.7%)
Gender: Male	47 (40.5%)	44 (35.8%)	68 (43.3%)	53 (37.1%)	115 (42.1%)	97 (36.5%)
Gender: NA	3	2	2	3	5	4
Mean number of mobile applications users installed (SD)	3.66 (1.57)	3.71 (1.68)	3.49 (1.52)	3.67 (1.50)	3.56 (1.54)	3.69 (1.58)
Mean number of mobile applications regularly used (SD)	3.24 (1.05)	3.28 (1.09)	3.14 (1.06)	3.23 (1.00)	3.18 (1.05)	3.26 (1.04)

Table 3. Respondent demographics.

4 Data Analyses and Results

4.1 Manipulation and Control Checks

We used "perceived user-friendliness of privacy policy" measure to verify the effectiveness of our manipulation in terms of friendliness vs. unfriendliness (see Table 2). Mann-Whitney tests for the difference between the medians of two unpaired samples (Rees, 2013, pp. 171-173) confirmed that the treatment was manipulated effectively. Specifically, we found support that participants in the "user-friendly" treatment group more strongly believed that the privacy policy was friendly than participants in the "user-unfriendly" treatment group (0.1% significance level). Furthermore, participants in the "BloodScan" treatment group perceived the information the mobile app deals with as more sensitive and personal, compared to the "DropSpot" treatment group ("perceived information sensitivity" measure; 0.1% significance level). Finally, ANOVA tests (Rees, 2013, pp. 179-188) revealed that subjects within the various treatments did not vary significantly regarding their age, number of self-installed mobile applications, and number of regularly used mobile applications. Hence, it follows that the random assignment of subjects to the various treatments was effective.

4.2 Measurement Validation

Measurement model was assessed for friendly and unfriendly privacy policies separately (see Figure 1). Here, criteria for convergent and discriminant validity were assessed following generally accepted decision rules (Hulland 1999). As summarized in Table 4, all indicator loadings are greater than .707 (with only one exception of item loading of 0.64) and are statistically significant at 0.1% level, so item reliability is confirmed across both models we tested. To ensure internal consistency, we control that composite reliability (CR) and Cronbach's alpha are larger than 0.70 for all constructs in our models (see Table 5). We further check that average variances extracted (AVE) values for all constructs in our models are greater than 0.5. Together, we conclude that convergent validity is well established across both models. Further, the square root of AVE of any latent variable is higher than any of its correlations with other latent variables (see Table 5). Moreover, each indicator's loading on the construct it is supposed to measure exceeds any of its cross-loadings (see Table 4). This indicates that discriminant validity is also met.

Constructs	Perceived Readability	Trust	Actual Readability	Perceived Readability	Trust	Actual Readability
Model	Unfriendly			Friendly		
Perceived Readability	0.87	0.09	0.19	0.86	0.26	0.19
	0.88	0.07	0.17	0.83	0.21	0.10
	0.88	0.07	0.17	0.88	0.25	0.20
	0.93	0.14	0.11	0.84	0.28	0.08
Trust	0.04	0.86	-0.46	0.25	0.82	0.22
	0.05	0.83	-0.47	0.12	0.71	0.04
	0.05	0.86	-0.47	0.22	0.78	0.17
	0.02	0.82	-0.40	0.18	0.75	0.09
	0.28	*0.64*	-0.17	0.21	0.81	0.08
	0.13	0.74	-0.24	0.28	0.80	0.29
	0.16	0.82	-0.38	0.27	0.82	0.10
Actual Readability	0.17	-0.49	1.00	0.17	0.21	1.00

Table 4. Loadings and cross-loadings.

	AVE	Composite Reliability	Cronbach's Alpha	Actual Readability	Perceived Readability	Trust
Friendly				Correlations (Off-Diagonal) and SQRT AVE (Diagonal)		
Actual Readability	1.00	1.00	1.00	1.00		
Perceived Readability	0.80	0.94	0.92	0.17	0.89	
Trust	0.64	0.92	0.90	-0.49	0.11	0.80
Unfriendly				Correlations (Off-Diagonal) and SQRT AVE (Diagonal)		
Actual Readability	1.00	1.00	1.00	1.00		
Perceived Readability	0.73	0.92	0.88	0.17	0.85	
Trust	0.62	0.92	0.90	0.21	0.29	0.79

Table 5. Criteria of construct validity.

4.3 Testing the Structural Model

To get a more refined picture, we divided the collected observations into six datasets (friendly vs. unfriendly privacy policy in the context of the health app BloodScan, friendly vs. unfriendly privacy policy in the context of the educational entertainment service DropSpot, and combined samples for friendly-unfriendly privacy policies). For each of these datasets, we separately evaluated structural models. Table 6 provides the results of our structural model testing including the path estimates and significances.

Specifically, the examination of the results of structural model testing shows that the path coefficient expressing the effect of perceived readability of a privacy policy on users' trust in the mobile app pro-

vider is positive and highly significant in almost all investigated datasets (the only exception is the "privacy unfriendly" DropSpot dataset). Hence, hypothesis 1 is supported with some limitations, indicating that the stronger a mobile app user believes in the readability of the privacy policy, the higher he or she trusts the mobile app provider.

Mobile Application	BloodScan		DropSpot		Combined	
User Friendliness	Unfriendly	Friendly	Unfriendly	Friendly	Unfriendly	Friendly
Perceived Readability –> Trust	**0.312*** **	**0.214*** **	0.123	**0.333*** **	**0.201** **	**0.267*** **
Actual Readability –> Trust	**-0.496*** **	**0.217*** **	**-0.552*** **	0.124	**-0.520*** **	**0.164** **
R^2	28.1 %	10.1%	30.3%	14.5%	27.5%	11.3%

Table 6. Results of Structural Model Testing (t>1.96 '', t>2.576 '**', t>3.29 '***').*

A significant effect of actual readability of a privacy policy on trust in the mobile app provider could be confirmed across all datasets we evaluated, except in the "privacy friendly" DropSpot dataset. Furthermore, as we postulated in Hypothesis 2a, better actual readability of the user-friendly privacy policy actually resulted in increased trust in the mobile app provider (with the only exception of the DropSpot sample). This finding indicates that the more mobile app users learn about a mobile app provider's user-friendly data-handling practices, the more trust they gain towards the company. We also found support for hypothesis 2b which negatively related actual readability of a user-unfriendly privacy policy to users' trust in the mobile app provider. This result suggests that a higher level of knowledge of the mobile app provider's user-unfriendly data-handling practices makes people lose their trust towards the mobile app provider.

Remarkably, in a "privacy-friendly" DropSpot context, perceived readability of a privacy policy was the only predictor of trust in the mobile app provider, while the effect of actual readability was not significant. Vail et al. (2008) similarly observed that users perceived paragraph-form policies as being more secure although poorly comprehending them in comparison to other policy representations. However, in the "privacy-friendly" BloodScan dataset, the effects of perceived and actual readability were quite comparable, although the impact of actual readability was slightly larger. It appears that mobile app users take privacy policies more seriously, when it comes to their sensitive health data: They almost equally integrate their perceptions regarding readability of the privacy policy and its actual understanding (actual readability) when forming their trust perceptions towards a mobile service provider. These suggestions could reasonably explain the study results by Ermakova et al. (2014), where perceived readability of a privacy policy exerted a positive effect on trust across all explored contexts, while the effect of actual readability was significant and similarly strong only for the Amazon context that is typically associated with the provision of sensitive financial data for usage as well as disclosure of user preferences as a result of this usage.

For the case where data-handling policies were not user-friendly, the effect of actual readability of privacy policies dominated the effect of their perceived readability in predicting mobile users' trust. In the "privacy-unfriendly" DropSpot context, the effect of perceived readability on mobile users' trust was insignificant, allowing us to conclude that mobile users only incorporate their understanding of user-unfriendly privacy policies when forming their trust in the mobile application provider that deals with less sensitive information. Interestingly, the structural models explained a higher share of variance in trust in the unfriendly contexts compared to the friendly ones.

5 Conclusion

Following the stream of research on the content and presentation of privacy policies as a trust-shaping factor (Bansal et al., 2008a, 2008b; Pan and Zinkhan, 2006; Ermakova et al., 2014; Sultan et al. 2002), we investigated the joint effect of both perceived and actual readability of a privacy policy within the context of two different mobile services that deal with information of varying sensitivity levels.

Across both app contexts, the results of structural model testing confirmed a positive and significant impact of perceived readability of a privacy policy on users' trust in the mobile app provider in all except one investigated datasets. Furthermore, across almost all datasets we explored, we found support for a positive and significant influence of the actual readability of a "privacy-friendly" privacy policy on users' trust in the mobile app provider; as well as a negative and significant effect of the actual readability of a "privacy-unfriendly" privacy policy on users' trust in the mobile app provider.

Based on these findings, we argue that mobile app providers should take the process of writing privacy policies more seriously, in particular when it comes to sensitive health data. With respect to Internet users, both their perceptions regarding the presentation and the actual understanding of the content of a privacy policy are essential for their trust-related decisions.

In future research, the effect of readability can be explored in further contexts. The generalizability can be further enhanced by collecting empirical data from other countries and different user groups since students, who have been mainly reflected in our sample, may not be representative for the entire population in terms of understanding complex online texts.

References

Acquisti, A. and Gross, R. (2006). "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." In: *Proceedings of the 6th International Conference on Privacy Enhancing Technologies*.

Adkinson, W., Eisenrach, J. and Lenard, T. (2002). *Privacy Online: A Report of the Information Practices and Policies of Commercial Web Sites*. URL: http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf (visited on 04/04/2016).

Anderson, J. (1983). "Lix and Rix: Variations on a Little-Known Readability Index." *Journal of Reading* 26 (6), 490-496.

Antón, A.I., Earp, J.B., He, Q., Stufflebeam, W., Bolchini, D. and Jensen, C. (2004). "The Lack of Clarity in Financial Privacy Policies and the Need for Standardization." *IEEE Security and Privacy* 2 (2), 36–45.

Bansal, G., Zahedi, F. and Gefen, D. (2007). "The Impact of Personal Dispositions on Privacy and Trust in Disclosing Health Information Online." In: *Proceedings of the 13th Americas Conference on Information Systems*.

Bansal, G., Zahedi, F. and Gefen, D. (2008a). "The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation." In: *Proceedings of the 30th International Conference on Information Systems*.

Bansal, G., Zahedi, F. and Gefen, D. (2008b). "Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online." In: *Proceedings of the 14th Americas Conference on Information Systems*.

Bansal, G., Zahedi, F. and Gefen, D. (2010). "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online." *Decision Support Systems* 49 (2), 138–150.

Brecht, F., Fabian, B., Kunz, S. and Müller, S. (2012). "Communication Anonymizers: Personality, Internet Privacy Literacy and their Influence on Technology Acceptance." In: *Proceedings of the 20th European Conference on Information Systems*.

Cadogan, R. A. (2010). "An Imbalance of Power: The Readability of Internet Privacy Policies." *Journal of Business & Economics Research* 2 (3), 49-61.

Carrión, I., Fernández-Alema´n, J. L. and Toval, A. (2012). "Are Personal Health Records Safe? A Review of Free Web-Accessible Personal Health Record Privacy Policies." *Journal of Medical Internet Research* 14 (4), e114.

Coleman, M. and Liau, T. L. (1975). "A Computer Readability Formula Designed for Machine Scoring." *Journal of Applied Psychology* 60 (2), 283-284.

Cranor, L. F., Hoke, C., Leon P. G. and Au, A. (2014). "Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies." In: *Proceedings of the 42nd Research Conference on Communication, Information and Internet Policy*.

Dale, E. and Chall, J. S. (1995). *Readability Revisited: The New Dale-Chall Readability formula*. Cambridge, MA: Brookline Books.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. (2006). "Internet Users' Privacy Concerns and Beliefs about Government Surveillance: an Exploratory Study of Differences between Italy and the United States." *Journal of Global Information Management* 14 (4), 57–93.

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

DuBay, W.H. (2007). *Smart Language: Readers, Readability, and the Grading of Text*. BookSurge Publishing.

Earp, J.B., Anton, A. I., Aiman-Smith, L. and Stufflebeam, W. H. (2005). "Examining Internet Privacy Policies within the Context of User Privacy Values." *IEEE Transactions of Engineering Management* 52 (2), 227-237.

Ermakova, T., Fabian, B. and Babina, E. (2015). "Readability of Privacy Policies of Healthcare Websites." In: *Proceedings of the 12. Internationale Tagung Wirtschaftsinformatik.*

Ermakova, T., Baumann, A., Fabian, B. and Krasnova, H. (2014). "Privacy Policies and Users' Trust: Does Readability Matter?" In: *Proceedings of the 20th Americas Conference on Information Systems*.

Fanguy, R., Kleen, B. and Soule, L. (2004). "Privacy Policies: Cloze Test Reveals Readability Concerns." *Issue in Information Systems* 5 (1), 117-123.

Federal Trade Commission (2000). *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to the Congress*. URL: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (visited on 05/04/2016).

Flesch, R. (1948). "A New Readability Yardstick." *Journal of Applied Psychology* (32), 221-233.

Fry, E. (1968). "A Readability Formula that Saves Time." *Journal of Reading* 11 (7), 513-578.

Gefen, D. (2000). "E-Commerce: The Role of Familiarity and Trust." *Omega* 28 (6), 725–737.

Gefen, D. (2002). "Nurturing Clients' Trust to Encourage Engagement Success During the Customization of ERP Systems." *Omega* 30 (4), 287-299.

Gefen, D., Karahanna, E. and Straub, D. W. (2003). "Trust and TAM in Online Shopping: An Integrated Model." *MIS Quarterly* 27 (1), 51–90.

Gefen, D. and Straub, D. (2004). "Consumer Trust in B2C e-Commerce and the Importance of Social Presence: Experiments in e-Products and e-Services." *Omega* (32), 407–424.

Goldman, J., Hudson, Z. and Smith, R. (2000). *Privacy Report on the Privacy Policies and Practices of Health Web Sites*. Preliminary eHealth Ethics Summit Release, California HealthCare Foundation.

Graber, M. A., D'Alessandro, D. M. and Johnson-West, J. (2002). "Reading Level of Privacy Policies on Internet Health Web Sites." *The Journal of Family Practice* 51 (7), 642–645.

Grabner-Kräuter, S. and Kaluscha, E. A. (2003). "Empirical Research in On-line Trust: a Review and Critical Assessment." *International Journal of Human-Computer Studies* 58 (6), 783–812.

Gunning, R. (1952). *The Technique of Clear Writing*. New York: McGraw-Hill.

Harris, T. L. and Hodges, R. E. (1995). *The Literacy Dictionary: The Vocabulary of Reading and Writing*. Newark: International Reading Association.

Hulland, J. (1999). "Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies." *Strategic Management Journal* 20 (2), 195-204.

Jarvenpaa, S., Tractinsky, N., Saarinen, L. and Vitale, M. (1999). "Consumer Trust in an Internet Store: a Crosscultural Validation." *Journal of Computer-Mediated Communication* 5 (2).

Jarvenpaa, S., Tractinsky, N. and Vitale, M. (2000). "Consumer Trust in an Internet Store." *Information Technology and Management* 1 (1–2), 45–71.

Jensen, C. and Potts, C. (2004). "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 471–478.

Jensen, C., Potts, C. and Jensen, C. (2005). "Privacy Practices of Internet Users: Self-Reports versus Observed Behavior." *International Journal of Human-Computer Studies* 63 (1-2), 203-227.

Kelley, P. G., Bresee, J., Cranor, L. F. and Reeder, R. W. (2009). "A "Nutrition Label" for Privacy." In: *Proceedings of the 5th Symposium on Usable Privacy and Security*.

Kincaid, J. P., Fishburne, R. P., Rogers, R. L. and Chissom, B. S. (1975). *Derivation of New Readability Formulas (Automated Readability Index, Fog Count and Flesch reading Ease Formula) for Navy Enlisted Personnel*. Research Branch Report 8-75. Chief of Naval Technical Training: Naval Air Station Memphis.

Klare, G. R. (1963). *Measurement of Readability*. Iowa St.

Laric, M. V., Pitta, D. A., Katsanis, L. P. (2009). "Consumer Concerns for Healthcare Information Privacy: A Comparison of U.S. and Canadian Perspectives." *Research in Healthcare Financial Management* 12 (1), 93-111.

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

Mamonov, S. and Koufaris, M. (2014). "The Impact of Perceived Privacy Breach on Smartphone User Attitudes and Intention to Terminate the Relationship with the Mobile Carrier." *Communications of the Association for Information Systems* 34 (60), 1157-1174.

Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995). "An Integrative Model of Organizational Trust." *Academy of Management Review* 20 (3), 709–734.

McDonald, A. M. and Cranor L. F. (2008). "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society* 4 (3), 540–565.

McDonald, A. M., Reeder, R. W., Kelley, P. G. and Cranor, L. F. (2009). "A Comparative Study of Online Privacy Policies and Formats." *Privacy Enhancing Technologies* 5672, 37-55.

McKnight, D. H., Choudhury, V. and Kacmar, C. (2002). "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology." *Information Systems Research* 13 (3), 334–359.

McLaughlin, G. H. (1969). "SMOG Grading - a New Readability Formula." *Journal of Reading* 12 (8), 639-646.

Milne, G. R. and Culnan, M. J. (2004). "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices." *Journal of Interactive Marketing* 18 (3), 15–29.

O'Connor, P. (2003). "What Happens to my Information if I Make a Hotel Booking Online: An Analysis of On-Line Privacy Policy Use, Content and Compliance by the International Hotel Companies." *Journal of Services Research* 3 (2), 5–28.

Pan, Y. and Zinkhan, G. M. (2006). "Exploring the Impact of Online Privacy Disclosures on Consumer Trust." *Journal of Retailing* 82 (4), 331–338.

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

Peslak, A. R. 2005. "Privacy Policies of the Largest Privately Held Companies: A Review and Analysis of the Forbes Private 50." In: *Proceedings of the 2005 ACM SIGMIS CPR Conference on Computer Personnel Research*.

Peterson, D., Meinert, D., Criswell II, J. and Crossland, M. (2007). "Consumer Trust: Privacy Policies and Third-Party Seals." *Journal of Small Business and Enterprise Development* 14 (4), 654–669.

Pollach, I. (2004). "Online Privacy Statements: Are They Worth Reading?" In: Khosrow-Pour, M. (Ed.): *Innovations Through Information Technology*, 217–220.

Pollach, I. (2005). "A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent." *Journal of Business Ethics* 62 (3), 221–235.

Proctor, R., Ali, M. and Vu, K.-P. (2008). "Examining Usability of Web Privacy Policies." *International Journal of Human-Computer Interaction* 24 (3), 307-328.

Prunty, R. and Swartendruber, A. (2015). "Social Media and the Fourth Amendment Privacy Protections." In: Lind, N.S. and Rankin, E.T. (Eds.): *Privacy in the Digital Age: 21st-Century Challenges to the Fourth Amendment*. ABC-Clio.

Rees, D. G. (2013). *Essential Statistics*. 4th Edition. Chapmann & Hall/CRC.

Reidenberg, J. R., Breaux, T. D., Cranor, L. F., French, B., Grannis, A., Graves, J. T., Liu, F., McDonald, A. M., Norton, T. B., Ramanath, R., Russell, N. C., Sadeh, N. and Schaub, F. (2015a). "Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding." *Berkeley Technology Law Journal* 30.

Reidenberg, J. R., Russell, N. C., Callen, A. J., Qasir, S. and Norton, T. B. (2015b). "Privacy Harms and the Effectiveness of the Notice and Choice Framework." *I/S: A Journal of Law and Policy for the Information Society* 11 (485).

Ryker, R., Lafleur, E., Mcmanis, B. and Cox, K. C. (2002). "Online Privacy Policies: An Assessment of the Fortune E-50." *Journal of Computer Information Systems* 42 (4), 15.

Senter, R.J. and Smith, E.A. (1967). *Automated Readability Index*. Wright-Patterson Air Force Base, AMRL-TR-6620.

Singh, R. I., Sumeeth, M. and Miller, J. (2011). "Evaluating the Readability of Privacy Policies in Mobile Environments." *International Journal of Mobile Human Computer Interaction* 3 (1), 55-78.

Shedlosky-Shoemaker, R., Sturm A.C., Saleem, M. and Kelly, K.M. (2008). "Tools for Assessing Readability and Quality of Health-Related Web Sites." *Journal of Genetic Counseling* 18 (1), 49-59.

Sheehan, K. B. (2005). "In Poor Health: An Assessment of Privacy Policies at Direct-to-Consumer Web Sites." *Journal of Public Policy & Marketing* 24 (2), 273–283.

Smith, H. J., Milberg, J. S. and Burke, J. S. (1996). "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *MIS Quarterly* 20 (2), 167-196.

Smith, H. J., Dinev, T. and Xu, H. (2011). "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly* 35 (4), 989–1015.

Sunyaev, A., Dehling, T., Taylor, P. L. and Mandl, K. D. (2014). "Availability and Quality of Mobile Health App Privacy Policies." *Journal of the American Medical Informatics Association* 22 (e1), e28-33.

Sultan, F., Urban, G. L., Shankar, V. and Bart, I. Y. (2002). *Determinants and Role of Trust in e-Business: A Large Scale Empirical Study*. Working Paper 4282-02, MIT Sloan School of Management, USA. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=380404 (visited on 05/04/2016).

Taylor, W. L. (1953). "Cloze Procedure: A New Tool for Measuring Readability." *Journalism Quarterly* 30 (4), 415-433.

TRUSTe (2015). *TRUSTe 2014 GB Consumer Confidence Privacy Report: Consumer Opinion and Business Impact*. Research Report. URL: https://www.truste.com/resources/privacy-research/uk-consumer-confidence-index-2014/ (visited on 05/04/2016).

Vail, M. W., Earp, J. B. and Anton, A. I. (2008). "An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies." *IEEE Transactions on Engineering Management* 55 (3), 442–454.

Vu, K-P. L., Chambers, V., Garcia, F. P., Creekmur, B., Sulaitis, J., Nelson, D., Pierce, R. and Proctor, R. W. (2007). "How Users Read and Comprehend Privacy Policies." In: Smith, M. J. and Salvendy, G. (Eds.): *Human Interface and the Management of Information. Interacting in Information Environments Human Interface*. Part II. LNCS 4558, Springer, 802-811.

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*.

Xu, H., Teo, H. H., Tan, B. C. Y. and Agarwal, R. (2012). "Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services." *Information Systems Research* 23 (4), 1342–1363.