Government Information Quarterly 26 (2009) 559–566

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites

Ardion D. Beldad *, Menno De Jong [1], Michaël F. Steehouder [1]

University of Twente, Faculty of Behavioral Sciences, Department of Technical and Professional Communication, P.O. Box 217, 7500 AE Enschede, The Netherlands

ARTICLE INFO

Available online 29 July 2009

Keywords:
Online privacy
Online trust
Electronic government
Privacy law
Confidentiality of information
Municipal websites
Wet Bescherming Persoonsgegevens (Dutch Personal Data Protection Act)

ABSTRACT

Various studies show that the display of a privacy statement on an organization's website can be a potent, but simple way of acquiring clients' and users' trust, which results in the completion of transactions with the organization through its website. Empirical studies that analyze the contents of privacy statements on commercial websites are profuse, while privacy statements posted on the websites of non-commercial organizations have been largely ignored by researchers. In this study, the contents of privacy statements on Dutch municipal websites are analyzed. Using the important provisions of the Wet Bescherming Persoonsgegevens (WBP) or the Dutch Personal Data Protection Act, the study also looked into the conformity of the contents of privacy statements with the existing law on privacy protection in the Netherlands. We also looked into the availability and *findability* of privacy statements on Dutch municipal websites. Three important findings resulted from this study: first, not all municipal websites bother to post privacy statements on their websites; second, most municipalities do not ensure that their online privacy statements are findable; and third, privacy statements on Dutch municipal websites emphasize diverging assurances and promises—with some privacy policies containing all the important provisions of the WBP, and others offering only general, and sometimes rather vague, guarantees.

1. Introduction

Two uncertainties exist in online transactions: the risk of losing one's money during the exchange and the threat of having one's private sphere penetrated. Although the first risk suffices to discourage some clients from engaging in an online exchange, the possibility of having the privacy of their personal data compromised contributes substantially to clients' disinclination to embark on online transactions. (Miyazaki & Fernandez, 2001).

The complexity in the collection and dissemination of data over the internet (Milne, Rohm & Bahl, 2004) spawns a spectrum of privacy concerns that are far from negligible: the bombardment of the clients' mailbox with spam emails, the placement of cookies on the clients' computer to track their internet usage history and preferences, the application of malicious technologies enabling third parties to access clients' personal files, and the inability of clients to control the usage and processing of their personal information disclosed to an online organization (Wang, Lee & Wang, 1998). What is even worse is the possibility of identity theft as a consequence of the mishandling of personal data by whoever is collecting it (Fernback & Papacharissi, 2007).

Efforts to win the clients' trust to engage in various exchanges with online organizations include the posting of the privacy statements on the organizations' websites (Pan & Zinkhan, 2006). Clients assess the trustworthiness of online organizations based on the presence of privacy protection guarantees (Earp & Baumer, 2003; Liu, Marchewka, Lu & Yu, 2005; Aiken & Bausch, 2006; Arcand, Nantel, Arles-Dufour & Vincent, 2007), even if the privacy statement would not be read thoroughly (Vu, Chambers, Garcia, Creekmur, Sulaitis, Nelson, Pierce & Proctor, 2007) or even consulted (Jensen, Potts & Jensen, 2005; Arcand et al., 2007). However, one criticism regarding an organization's promise to protect the personal information of its clients is that it is purely tactical—fortifying commercial advantage or eluding legal penalties—rather than ethical. Pursuing the protection of collected personal data from clients is just the right thing to do (Markel, 2005).

Since personal data are becoming valued commodities (Franzak, Pitta & Fritsche, 2001; Turner & Dasgupta, 2003; Olivero & Lunt, 2004), one can never be assured that they will stay untouchable inside a confidentiality chest since they are also susceptible to exploitation for a cornucopia of purposes by those who collect and store them. The notion that data can be effortlessly recycled for unknown purposes, which could jeopardize clients' online privacy rights, only exacerbates clients' reluctance to provide personally-identifiable information, thereby spurring them to drop their plans of engaging in online exchanges. However, in some cases, the convenience of online transaction trumps privacy concerns, especially when the benefits of an electronic exchange outweigh the value of privacy (Woo, 2006).

* Corresponding author. Fax: +31 53 489 4259.
E-mail addresses: a.beldad@utwente.nl (A.D. Beldad), m.d.t.dejong@utwente.nl (M. De Jong), m.f.steehouder@utwente.nl (M.F. Steehouder).
[1] Fax: +31 53 489 4259.

0740-624X/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.giq.2009.05.002

In this study, the primary interests are the analysis and the categorization of the contents of the privacy statements on Dutch municipal websites. The assurances and notifications of those statements are also scrutinized using the provisions of Wet Bescherming Persoonsgegevens (WBP) or the Personal Data Protection Act of the Netherlands. The aforementioned law implements Directives 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data). The study also looks into the ease of finding the privacy statements on the websites of municipalities—considering that not only the availability of a privacy statement but also its *findability* should be taken into account when appraising an online organization's compliance with the 'notice principle' of fair information practices (OECD, 2002).

2. Online privacy as a matter of control and restricted access

Although the association of privacy with control is prominent in the writings of both Westin (1967, 2003) and Fried (1984), Moor (1997) has argued that control alone does not guarantee the protection of one's online privacy. Personal data, once digitized, slide rapidly through computer systems around the world. His control/restricted access conception of privacy signifies that different people (or organizations) should be given different levels of access to different types of personal information at different times (Moor, 1997). Tavani and Moor (2001) advanced that control of information does not suffice to conceptualize the right to privacy. Instead, the right to privacy is better understood in terms of a theory of restricted access. Assuming centrality in the aforementioned theory is the need to create privacy zones to protect people's privacy, especially when they lack control over information about themselves.

It is emphasized that in managing one's privacy, one does not need absolute control over information about oneself. Some degree of control can already be achieved through choice, consent, and correction. Managing one's privacy through choice, as an aspect of limited control, involves prudency in defining the flow of one's personal information and determining the level of access other parties have to that same information; whereas consent, as an element of limited control, implies that people waive their right to privacy and provide others with access to their information. The management of one's privacy is incomplete if the person concerned is not provided with access to his or her data and the opportunity to correct them if necessary (Tavani & Moor, 2001).

2.1. Privacy policies—defensive or protective?

Even if clients do not bother to read or consult online privacy statements (Jensen et al., 2005; Arcand et al., 2007; Vu et al., 2007), online organizations still resort to the posting of privacy statements on their websites to placate clients who are anxious about providing their personal data for the transaction (Fernback & Papacharissi, 2007). Empirical studies showed that clients use the presence of an online privacy statement as one criterion in assessing the trustworthiness of an online organization (Earp & Baumer, 2003; Liu et al., 2005; Aiken & Bausch, 2006; Arcand et al., 2007).

Privacy statements provide clients with the necessary information about the organization's information practices (Milne & Culnan, 2004). By emphasizing the benefits of disclosure, organizations may even use their privacy statements to convince their clients to disclose personal information necessary for the completion of a transaction (LaRose & Rifon, 2006).

However, an analysis of 97 privacy statements revealed that they do not guarantee the protection of personal information, but instead serve as legal safeguards for the company by specifying the usage of collected information. A majority of online organizations used privacy statements to make vague promises of how personally-identifiable information would be protected and to assert their right to collect and trade non-personally-identifiable data. (Papacharissi & Fernback, 2005). Pollach's first study (2005), an analysis of communicative strategies in privacy statements, showed that organizations resort to both rational and emotional appeals in the construction of more credible arguments to persuade clients that their personal data would be responsibly handled. The findings of Pollach's second study (2007) suggested that privacy statements are motivated more by efforts to avoid potential lawsuits than by the obligation to uphold the principles of fair information practice.

One study (Earp, Anton, Aiman-Smith & Stufflebeam, 2005) disclosed the apparent conflict between the guarantees of organizational privacy statements and what their clients' expect to be emphasized in those statements. The study found that privacy statements emphasized the security and protection of collected data, procedures of data collection (direct or indirect), and the choice for clients to determine the types of information about them that can be processed and used by the organization. However, clients were most concerned about the transfer of data by the organization (whether the data would be shared, rented, or sold), about the usage of their information by the organization, and about how disclosed data will be stored by the organization. These findings extend full support to the results of another study (Phelps, Nowak & Ferrell, 2000)—that clients would like more information about how organizations use their personal information.

The demand for further information on the usage of collected personal data is an indication that clients do not trust that online organizations will stick to what they are guaranteeing in their privacy statements, and this lack of trust springs from clients' belief that online organizations do not share their value about information privacy in the online environment (Hoffman, Novak & Peralta, 1999).

3. Legal protection of online privacy in the European Union and in the Netherlands

With the ease in the collection and transmission of data as a result of the advances in technology, the European Union saw the urgency of implementing legislation that would protect European citizens' right to privacy, especially regarding the processing of their personal data. Enacted in 1995 and effective in 1998, Directive 95/46/EC, substantiating the effort to regulate and institutionalize data protection, is founded on the perspective that the government should assume an important role in protecting its constituents from social harm (Strauss & Rogerson, 2002) and is a strong manifestation of the European view that the privacy of personal information is a fundamental human right that merits legal protection (Markel, 2006). Since Directive 95/46/EC is broadly applicable to privacy practices in general, Directive 2002/58/EC was adopted in 2002 to extend further protection for internet users (Baumer, Earp & Poindexter, 2004).

Directive 95/46/EC clearly states that EU member states should protect the fundamental rights and freedoms of natural persons (identified or identifiable natural persons), in particular their right to privacy with respect to the processing of their personal data (European Union, 1995a,b). Bergkamp (2002) argued that, unlike the selective U.S. legislative approach, the European Commission laws impose onerous sets of requirements on all sectors of industry, from financial institutions to consumer goods companies, and from list brokers to any employer.

Elgesem (1999) asserted that two ideals surfaced from Directive 95/46/EC: the ideal of predictability and the ideal of justifiability. The ideal of predictability concerns data subjects' ability to form reasonable expectations on how their personal data will be processed, which is grounded on the Directive's provisions on data quality and security. The ideal of justifiability pertains to questions about the justifications of the different kinds of data processing.

Directive 2002/58/EC furthers the EU's determination to uphold the internet users' right to privacy. An important stipulation in that directive

is the provision on the necessity on the part of the organization to inform users' about the usage of cookies and the right of the users to refuse cookies (European Union, 2002). Cookies pose a potential harm in the sense that collected information from the users' computers through cookies may be used by the organization or company in so many ways that could have unpleasant consequences for the users (Debussere, 2005). Cookies can be used for potentially unethical procedures such as linking online behavior to personally-identifiable information and re-selling this information without the user's consent (Kierkegaard, 2005).

In the Netherlands, Directive 95/46/EC is implemented through the Wet Bescherming Persoonsgegevens (Personal Data Protection Act), which was enacted on September 1, 2001. WBP replaced the old Wet Persoonsregistraties, which dated from December 28, 1988 (European Commission, 2008). Borking and Raab (2001) presented a summary of significant points concerning the Wet Bescherming Persoonsgegevens (WBP):

1. Reporting the processing—the Data Protection Board or a privacy officer must be informed of the processing of personal data.
2. Transparent processing—the person concerned must be notified of the identity of the data processor and the purpose(s) of the processing.
3. 'As required' processing—the collection of personal data must be founded on specific, explicit, and legitimate purposes and data should not be processed in ways incompatible with the specified purposes.
4. Lawful basis for the data processing—the processing of personal data must be grounded on provisions contained in WBP, such as permission, agreement, legal obligation, and justified interest. Processing of special categories of data, such as racial/ethnic information and health information, have stringent rules.
5. Data quality—the correctness and accuracy of personal data is important. Personal data should be sufficient, to-the-point, and not excessive.
6. Rights of parties involved—parties involved have the right to check and correct their data and they also have the right to raise objections.
7. Data traffic with countries outside the EU—the transfer of personal data to a non-EU country is permitted only if adequate protections are offered in that country.
8. Processing personal data by a processor—a data processor should observe the instructions of the data controller if the processing is outsourced to the processor.
9. Protection against loss and unlawful processing of personal data—lawful data processing requires the use of appropriate security measures to ensure the protection of personal data.

4. Research questions

Text and content analyses had been carried out to scrutinize the contents of privacy statements on U.S. based-commercial websites (Earp et al., 2005; Markel, 2005; Papacharissi & Fernback, 2005; Pollach, 2005, 2007; Schwaig, Kane & Storey, 2006; Fernback & Papacharissi, 2007). These analyses aimed at either exposing the flaws in the statements or assessing their compliance or non-compliance to the principles of fair information practice. While it is evident that previous studies have concentrated on the dissection of the privacy statements of commercial websites, the privacy statements of non-commercial organizations—such as those on the websites of government agencies—have been spared from enquiry. However, the absence of a comprehensive online information privacy protection law in the U.S. makes it impossible to check whether online privacy policies conform to the provisions of a privacy law. The case is different in any EU member state where EU Directives on privacy protection are implemented through the privacy laws in member states. This study aims at dissecting the contents of the privacy policies on municipal websites and determining whether the contents of privacy statements on Dutch municipal websites coincide with the significant provisions in the Wet Bescherming Persoonsgegevens.

In the United States, for instance, it has been cited that the emphasis of most online privacy statements often clash with what clients expect to read in privacy statements (Earp et al., 2005), which corroborates the claim that online organizations do not share the clients' value about information privacy in the online environment (Hoffman et al., 1999). According to a study by Earp et al. (2005), online privacy statements often underscore the application of security measures and the methods for the collection of data, whereas clients would like to have more information about the further usage and the storage of their personal information. Schwaig et al. (2006) also cited that organizations focus their efforts on different aspects of fair information practice (notice, access, choice, security, enforcement) and they follow diverging approaches in the selection of the privacy protections they extend to their clients. The differences in the content, structure, and focus of online privacies on commercial websites resulted in an interest to study the content and focus of privacy statements on government websites, which prompted the first research question.

(1) What are the guarantees contained in the privacy statements on Dutch municipal websites?

The publication of a privacy statement on the organization's website is already a standard practice and is used either as a trust-building mechanism (Araujo, 2005) or as a legal safeguard (Fernback & Papacharissi, 2007). However, the presence of such a statement is not a guarantee that the organization will conform to it (Earp et al., 2005; Markel, 2005) or that the privacy statement corresponds to the tenets of fair information practice (Schwaig et al., 2006). The failure of an online organization to provide its clients with any information about its privacy statements is tantamount to depriving them of the information necessary for them to act autonomously (Markel, 2005) and an indication of that organization's inability to observe 'notice'—the first principle of fair information practices (Schwaig et al., 2006).

When people want to know whether a website has a privacy statement or not, they must first deal with the task of finding it. And this brought us to pose our second question:

(2) How easy (or difficult) is it to find the privacy statements on Dutch municipal websites?

The second question of this study is not centered on whether the website has a privacy statement or not but on whether the statement is findable. For this study, the *findability* of the privacy policy is defined in terms of the ease of locating the statement within the website—whether it is located on the main page or hidden somewhere within the website and whether it is labeled or not.

5. Research methodology

Privacy statements used for this study were obtained from 100 municipal websites (specifically, the websites of the first 100 municipalities ranked according to their population size). The decision to select the first 100 municipalities, starting from the most populated, was founded on the premise that bigger municipalities (in terms of population size) would be conscientious in providing their users with the option to know how their personal data will be used and protected, although it should not be interpreted that small municipalities are not concerned about the privacy concerns of their users.

An initial survey of the contents of privacy statements on thirty Dutch municipal websites (not included in the sample) allowed for the creation of a code book classifying the different assurances and notifications contained in the privacy statements. The code book was then used to survey the contents of the first half of the sample, which,

in order to accommodate new items that were not found in the initial survey, also necessitated the constant revision of the code book. The second half of the sample was then analyzed using the revised code book, which was also subjected to a second revision.

The entire sample of seventy-seven privacy statements (out of 100 websites) was then re-analyzed using the expanded code book. Two raters were tasked to code the different parts of the selected privacy policies. The first rater coded the different parts of the entire sample of privacy statements ($n=77$), while the second rater worked independently with 40% of the sample ($n=31$). Inter-rater agreement is pegged at 84%. Disagreements in the analyses were settled through a discussion between the raters.

6. Data analysis and results

6.1. What do privacy policies promise?

6.1.1. Catching the clients' trust right at the start

In the construction of online privacy statements, organizations seem to be capitalizing on the impact of the 'first paragraph' as rhetorical strategies are prominently employed in the introductory part to temper users' anxiety of having their privacy zones invaded after their decision to share personal data. The majority of the privacy statements of municipal websites ($n=53$ of 77; 69%) commenced with an assurance that the municipality respects and values the privacy of its users.

This first overarching guarantee is further strengthened with a supporting promise that collected personal information from users will be handled confidentially and with utmost care, with thirty-two (42%) online privacy statements containing this guarantee. The strategic positioning of the aforementioned broader promises appears to confirm the findings of an experiment (Vu et al., 2007) that readers paid particular attention to the first sentences of a privacy statement, aside from the first few words of each paragraph. Thus, an online organization must, right at the start, capture the trust of clients for the organization's commitment to protect privacy, before clients decide to discontinue reading the rest of the policy.

Table 1 shows four overarching guarantees that can be found in the privacy statements of municipal websites.

6.1.2. Notification of the purposes for data collection

Wet Bescherming Persoonsgegevens (WBP) or the Personal Data Protection Act stipulates that the collection of personal data should be performed in accordance with the law and in an appropriate and careful manner (Article 6) and founded on specified, explicit, and legitimate purposes (Article 7).

Online organizations, therefore, are expected to spell out their rationales for collecting personal data from their clients. Fifty privacy statements from municipal websites stated the purposes for the collection of personal information, but only thirty-nine of the fifty (78%) indicated that collected personal data will only be used for the purposes that they were collected for. This guarantee is in accordance with Article 9 of the Personal Data Protection Act, which states that personal data shall not be further processed in a way incompatible with the purposes for which they have been obtained.

Additional points related to the notification of purposes for data collection are shown in Table 2.

6.1.3. On the collection of data related to website visit

Thirty percent ($n=23$ of 77; 30%) of the municipal websites emphasized in their privacy statements that users do not have to supply personal information when visiting the website, therefore implying that clients can visit the website anonymously, for instance to search for information without having to disclose personal data. However, the privilege of an anonymous visit is revoked when users decide to place a request for a document (for instance a driver's license) through the municipal website. Such a request necessitates the disclosure of personally-identifiable information such as the user's complete name, physical address, telephone number, and e-mail address.

Privacy statements on municipal websites ($n=51$ of 77; 68%) apportioned a section to articulate their purpose/s for the collection of information concerning users' visit to the website such as the time of visit to the website, the most visited pages, the frequency of visit, and the IP address. Those that register data related to website visit, such as the IP address, emphasized that the collection of such data will only be used for technical supports and statistical purposes and will not be exploited to identify the individual user.

However, one piece of data related to the users' visit to a municipal website is rather controversial. According to the Dutch Data Protection Act Guidelines (2007), an IP address is classified as a piece of personal data since an internet service provider can easily trace this information to the originating person—the internet subscription customer—and it does not matter whether or not the organization collecting the IP address will be using it to identify the user. In fact, one municipal website cited that in certain circumstances, for instance in criminal cases, the service provider can be requested to reveal relevant information about an IP address, which could eventually link to an individual.

6.1.4. On the collection of special personal data

Articles 16 to 24 of the Personal Data Protection Act specify prohibitions on the processing of special personal data such as those that pertain to the users' religion, philosophy, race, political persuasion, health and/or sexual life, as well as data concerning trade union membership, criminal behavior, or unlawful or objectionable conduct. The articles also identify cases for which prohibitions on the collection of special personal data are not applicable.

One municipal website (1%) guaranteed that it will not collect special personal data from its users. The absence of such a guarantee in 99% of the analyzed privacy statements could be attributed to the fact that municipal websites only ask for contact information such as the user's name, physical address, telephone number, and e-mail address when the user decides to request a document or apply for a particular service through the municipal website.

6.1.5. On data processing and usage

A fraction of municipal websites ($n=2$ of 77; 3%) explicitly guaranteed that users' consent will be requested whenever their

Table 1
Overarching guarantees in the privacy policies of municipal and commercial websites.

Statements of guarantees and/or notifications	$n=77$
Respect for the users' privacy and the confidentiality of their personal information	53 (69%)
Assurance that collected personal information from the users will be handled confidentially and treated with care	32 (42%)
The collection, processing, and usage of personal information are in accordance with existing legislations on information privacy protection	36 (47%)
The organization's procedures for the collection and usage of users' personal data have been reported to a government agency tasked to oversee the processing of data by organizations	3 (4%)

Table 2
Additional assurance and notification related to the collection of personal data.

Statements of guarantees and/or notifications	50 collect personal information
Only voluntarily disclosed personal information will be processed and used	8 (16%)
Notification of the types of personal information that will be collected from the user	3 (6%)

personal information will be processed. In an effort to placate users' concerns over the torrent of spam mails in their mail boxes, one municipal website promised that it will not send spam mails to its users. Such a promise is relevant, especially when municipal websites are requesting their users' e-mail addresses.

6.1.6. On the disclosure of personal data to third parties

Article 41 (3) of the Personal Data Protection Act states that responsible parties who are planning to provide personal data to third parties should take appropriate steps to notify users of the option they have to object to the disclosure of their data to third parties.

The recognition of personal data as valued commodities (Olivero & Lunt, 2004) and the potential for abuse of disclosed data shape users' concern that whatever data they will disclose to an organization might be traded with other commercial entities or could be used for purposes that could have damaging consequences for them. Such anxiety results in their unwillingness to divulge the necessary personal data. To counter such apprehension, municipal websites have resorted to the deployment of two common rhetorical strategies: an assurance that personal data will not be relayed to third parties ($n=8$, 10%) and an assurance that they will not be rented or sold ($n=1$, 1%).

Only 3% ($n=2$ of 77) of the municipal websites studied indicated in their privacy statements the conditions for the possibility of disclosing their users' personal information to third parties. The rationale for indicating that there is the possibility of data disclosure to third parties is anchored on the municipality's obligation to supply the police and other government agencies with users' data when necessary.

Table 3 contains three additional notifications concerning the disclosure of personal data to third parties.

6.1.7. Storage and retention of collected data

Of the fifty municipal websites that collected personal data from their users, only five (10%) stressed in their privacy statements that collected information will be stored in the organization's database. Article 10 (1) of the Personal Data Protection Act states that personal data should not be kept in a form which allows the data subject to be identified for any longer than is necessary for achieving the purposes for which they were collected or processed subsequently, except (Article 10:2) when data are used for historical, statistical, or scientific purposes.

In accordance with Article 10 (1), 15 (30%) municipal website privacy statements emphasized that data will be destroyed after usage. However, this still leaves the fate of the data collected by 30 municipalities unknown since nothing is said about what will happen to them after they have been used for the purpose(s) for which they have been obtained.

6.1.8. Users' right of access to their personal data

One of the essential principles of fair information practices is the provision of access that enables users to review, rectify, or remove whatever data they have disclosed to an online organization. This principle is significantly accommodated in Article 36 of the Personal Data Protection Act.

Table 3
Further notifications related to the disclosure of personal data to third parties.

Statements of guarantees and/or notifications	3 disclose personal information
Notification of the users' right to object to the disclosure of data to third parties	2 (67%)
Notification of the types of thirds parties to whom personal data will be disclosed	1 (33%)

Only two of the ten (20%) municipal websites that store their users' personal data on a database cited in their privacy statements that users have the right to check and rectify information collected from them. The inclusion of a guarantee that collected data will be destroyed after they have been used for the purpose(s) for which they have been collected might explain why the provision on the right of access is not so popular in most privacy statements.

6.1.9. Security of personal data

The Personal Data Protection Act obliges online organizations to implement appropriate technical and organizational measures to secure personal data against loss or any form of unlawful processing (Article 13). This study shows that 20% ($n=10$ of 50) of the municipal websites that collected personal data from their users emphasized in their privacy statements that collected personal data are assured of protection as security technologies, such as the secure socket layer (SSL) protocol, are utilized.

6.1.10. Notification of the usage of cookies

According to Article 2 (1), the Personal Data Protection Act, applies to fully or partly automated processing of personal data and to the non-automated processing of personal data entered in a file or intended to be entered therein. This corresponds to Article 11 of Directive 95/46/EC, which states that where data are not directly obtained from the data subject, the data controller must inform the data subject of the data collection at the time of recording of personal data or, if a disclosure to a third party is envisaged, no later than the time when the data are disclosed. According to Kierkegaard (2005), even if the issue of cookies is not specifically mentioned, almost all aspects and features of the cookie concept can be used to violate the Directive's principles on access restriction and user transparency (European Union, 2002).

Directive 2002/58/EC, however, contains a provision that concerns the usage of cookies. According to Article 5(3) of the Directive 2002/58/EC:

> The use of electronic communications network to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with a clear and comprehensive information in accordance with Directive 95/46 EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.

Two important legal requirements are underscored in this provision: a notification of the purpose of the processing and a notification of the users' right to object to such processing. In the analysis of paragraphs that contain information on the usage of cookies, the two legal requirements noted above correspond to (a) the notification of the purpose(s) of cookies, and (b) the notification of the users' right to refuse the usage of cookies.

In accordance with the recommendation of the Article 29 Working Party with regards to the online collection of data, an online privacy statement should include information regarding the automatic data collection procedures, such as the use of cookies (Dutch Data Protection Act Guidelines, 2007). Twelve out of seventy-seven (16%) municipal websites informed their users that they are using cookies. However, only 67% ($n=8$) of municipal websites that reported using cookies stated the purposes for using cookies. Only four municipal websites notified their users that they have the possibility to block or refuse the usage of cookies, but only two indicated that the blockage or refusal of cookies may result in the user's inability to use certain sections of the website.

Concerns regarding the perceived potency of the cookie technology to invade privacy and the belief that cookies might harm the user's system (Ha, Al Shaar, Inkpen & Hdeib, 2006) are often confronted with

a dosage of rhetoric. For instance, of the twelve privacy statements that stated that cookies are used, seven (58%) provided brief explanations about what cookies are, and three (43%) of which used the adjective 'small' in the definition. According to Pollach (2005), by emphasizing the small size of cookies (e.g. 'cookies are small pieces of information….'), companies and organizations are mitigating their questionable practices by implying that cookies are harmless and no cause for concern.

As the only guarantee in a privacy statement that can be verified by the user of a municipal website, the researchers used the cookie tracking tool of the web browser, Firefox 3, to determine if municipal websites that do not indicate cookie usage in their privacy statements do not really use cookies. Of the seventy-seven visited municipal websites, seventy-five used cookies, whereas only twelve municipal websites cited in their privacy statements that cookies were being used. One municipal website did not mention using cookies, and it is confirmed using Firefox 3, as cookies were not traced. Most municipal websites used session cookies, while a few used a combination of session cookies and temporary cookies. While the former expires at the end of the session, the latter does not—with the expiration dates set some days after the session.

Table 4 is allotted for a number of other relevant assurances and notifications related to the usage of cookies.

6.1.11. Revisions in the privacy statements

Eleven (14%) municipal websites indicated that they reserve the right to revise their privacy statements, but only six (55%) were assuring that they would post the revised privacy statements. Municipal websites that cited the necessity for revising their privacy statements underscored the notion that such revision is in line with the need to adapt the policy statements to certain circumstances.

One municipal website only advised its users to consult the organizations' privacy statements for updates and changes. According to Jensen et al. (2005), such advice places the burden of monitoring changes in the privacy statements on the users. This implies that online organizations should take the necessary step in providing their users with the convenience of being informed about revisions in their privacy statements, for instance by citing the latest date of revision of a particular privacy statement on the website.

6.1.12. Contact possibilities for inquiries regarding the privacy policies

An important requirement of fair information practices is the provision of contact information to the organization's users that will afford them the appropriate channels necessary for seeking answers to questions regarding the organization's privacy practices, and that will enable them to exercise their rights of choice and access (Strauss & Roberson, 2002). The implication of this provision is the online organization's recognition of the indispensability of transparency in fomenting users' trust. The result of the analysis of privacy statements of municipal websites is not promising—with only 16% ($n = 12$ of 77) of the municipal websites indicating relevant contact information within their privacy statements.

Table 4
Other assurances and notifications related to the usage of cookies.

Statements of guarantees and/or notifications	Statements of guarantees and/or notifications
Data collected through cookies will stay in the users' computer	3 (25%)
Cookies will not track and store personally-identifiable information	6 (50%)
Cookies will not cause harm to the users' computer	1 (8%)
Notification of the types of cookies used	5 (42%)

6.2. Are privacy policies available and findable?

Only 77% ($n = 77$) of the 100 selected Dutch municipal websites contained privacy statements. In terms of the fundability of the privacy statements on the websites, only 23% ($n = 18$) of the 77 municipal websites provided a conspicuous link (labeled as 'privacy' and displayed both on the lower section of the homepage and on succeeding pages) to the privacy statements, while 77% ($n = 59$) of the privacy statements can be found in other links within the websites (e.g. proclaimed/disclaimer, colophon, about the site, or contact).

The figures indicate a very high difficulty rating for finding a privacy statement since users may end up having to try a lot of links before they can actually locate and read the privacy statement of the municipal website, unless they know exactly that the said statement is located, for instance, in the disclaimer.

7. Discussion

Privacy statements of municipal websites may lump all possible forms of notifications and assurances in a piece that could be too legalistic for an average reader (Milne & Culnan, 2004). In addition, they could still miss important points that users might expect to read. For instance, over 50% of the 100 municipal websites analyzed for this study contained notifications of the purposes of the collection of both personal data and information related to the users' visits to a municipality's website, but a remarkable percentage of those statements did not mention that users are entitled to have access to personal data they have disclosed to the organization and that necessary security measures are employed to ensure that their confidential data are protected.

Though most municipal websites observed the principle of notice by explaining the purposes for the collection of personal data from their users, their inability to extend a guarantee that allows users the option of reviewing, rectifying, and even removing their data, can result in a significantly incomplete privacy policy. Operators of those municipal websites that do not extend the right of access to their users may contend that since they are not storing collected personal data, as data would be destroyed after they have been used for a designated purpose, there is no justification for enabling users to have access to their personal data that are stored in the organization's database. However, the provision of the right of access is so fundamental (especially if organizations admit that they store collected data from users) that its non-inclusion in any privacy statement would indicate half-hearted compliance with the principles of fair information practice, and even more importantly with the existing legislation on the protection of information privacy.

The failure on the part of 80% of municipal websites to guarantee that necessary security technologies are employed to ensure the protection of collected personal data not only heightens users' apprehension about the possible misuse of their data but also signifies a loose conformity with the legal requirements on the application of security measures. The omission of an assurance of security in a privacy statement may stir users to think that their personal data are susceptible to potential abuse, and this could discourage them from supplying the necessary personal data to complete a transaction online. Even if municipal websites are indeed employing the required technology to ensure the security of personal data, from a communication perspective, such practices should at least be indicated in the privacy statement to assure users that personal data they will be asked to disclose for the completion of an online transaction with the municipality are secured and protected from unwarranted abuse.

While most municipal websites indicated that they collect personal data, only a few mentioned that collected data will be stored in a database and will be destroyed after usage. Even if users are informed of the purposes for the collection of their personal data, there would still be questions on what will happen to the data after

usage. Therefore, an assurance that data will be destroyed or deleted after they have been used for a particular purpose may help in dispelling users' fear about the fate of their personal data.

What is evident is that despite the many assurances and guarantees contained in the privacy statements of municipal websites, there are points that are highlighted in some statements but not included in others. When privacy statements do not include a particular guarantee or notice, two interpretations are possible—it could be that they find that saying something about what they are not doing is irrelevant, or that they just opt not to say something about what they are actually doing. The second statement is more likely in the case of cookie usage. While almost all municipal websites that have privacy statements ($n = 77$) used cookies, only a quarter cited in their policy statements that cookies are being used.

While some privacy statements are considerably long to the point of including all possible guarantees that are in accordance with the Personal Data Protection Act of the Netherlands; other privacy statements are relatively short, with only one or two sentences. Such differences in length and structure could be attributed to the increasing application of the multilayered format, which Article 29 of Directive 95/46/EC recommends (Article 29 Data Protection Working Party, 2004). The multilayered format has three structures: layer 1 (short notice) contains minimal information, primarily the identity of the data controller and the purpose(s) of the processing; layer 2 (condensed notice) presents the following information: the name of the company, the purpose of the data processing, the recipients of the data, the choices available for the users with regards to responding to questions and the consequences of such choices, the possibility of transfer to third parties, and the users' right of access; and layer 3 (full notice) should include all national legal requirements and specificities (Article 29 Data Protection Working Party, 2004).

Privacy statements of municipal websites also heavily rely on the use of rhetorical devices, which we call 'overarching assurances' at the beginning of almost all privacy statements as an attempt to catch the users' trust even before the decision is made to continue or discontinue the reading of the entire privacy policy. Some examples of such 'overarching assurances' include the following: the organization respects the privacy of its users; collected data from users will be handled confidentially and treated with utmost care. The strategic placement of those broad assurances appears to confirm the result of an experiment that clients tend to read the first few sentences in the privacy statement (Vu et al., 2007), while leaving the remaining parts of the policy uninspected.

The selection of the first hundred municipal websites in the Netherlands, ranked according to the population size of the municipalities, was rooted on the premise that big municipalities will be conscientious in notifying their users about how their privacy will be protected. However, as shown previously, privacy statements were still missing in the websites of 23% of municipalities selected for this study. Further, even though the majority of the municipal websites had privacy statements, a great number of those statements were difficult to find. Thus, users who are curious about a municipality's privacy statements will have to do some kind of a treasure hunt. An available privacy statement is bordering on insignificance if finding it demands herculean efforts from users.

8. Conclusion and future directions

Differences in the contents of privacy statements suggest differences in organizational practices that are adopted to ensure that the privacy of clients' data is maintained. These differences in contents also reflect differences in interpretations, on the part of organizations, of what users are expecting to read in privacy statements. This premise could be a starting point for exploring what users are really expecting to read in privacy policies of municipal websites and for determining which assurances and notifications are most important for them. While it is evident that the structure, content, and focus of the privacy policies on Dutch municipal websites vary significantly, the privacy statements should be constructed in a way that their contents and foci are aligned with the provisions contained in the existing laws on privacy protection.

As the present study also reveals that municipalities do not pay sufficient attention to the significance of making privacy statements findable on their websites, it would also be interesting to look into the impact of highly findable privacy statements on the formation of trust among users on engaging in an online transaction with municipalities. The finding is also surprising because it would be expected that government agencies should lead in the practice of posting privacy statements on their websites and in making them findable—not only for the sake of acquiring their users' trust, but also as a response to an ethical obligation of informing users about how their personal data will be handled.

While empirical studies on trust in online commercial exchanges are abundant, investigations on trust in e-government transactions are still sparse. An area that should be further explored is the relationship between (a) trust in a government organization and the decision to disclose personal data through its online channel as a prerequisite for an online transaction, (b) trust in the government organization's commitment and ability to protect the personal data of its client and the client's intention to read the privacy statement on the institution's website before the decision to disclose personal data, and (c) the contents of the privacy statement on a government organization's website and the decision to disclose personal data.

Acknowledgments

We would like to thank Mr. Hans Kits of ROC van Twente (the Netherlands) for his assistance in the coding of a number of privacy statements used in this study. Our acknowledgement also extends to the two anonymous reviewers for their comments and suggestions.

References

Aiken, K. D., & Bausch, D. M. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of internet signals. *Journal of the Academy of Marketing Science*, *34*, 308–323.

Araujo, I. (2005). Privacy mechanisms supporting the building of trust in e-commerce. Proceedings of the 21st International Conference on Data Engineering (ICDE '05), IEEE Computer Society.

Arcand, M., Nantel, J., Arles-Dufour, M., & Vincent, A. (2007). The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review*, *31*(5), 661–681.

Article 29 Data Protection Working Party (2004). WP 100—Opinion on more harmonized information provisions. Retrieved January 2009, from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf

Baumer, D. L., Earp, J. B., & Poindexter, J. C. (2004). Internet privacy law: A comparison between the United States and the European Union. *Computers & Security*, *23*, 400–412.

Bergkamp, L. (2002). The privacy fallacy: Adverse effects of Europe's data-protection policy in an information-driven economy. *Computer Law & Security Report*, *18*(1), 31–47.

Borking, J.J. & Raab, C.D. (2001). Laws, PETs, and other technologies for privacy protection. Journal of Information, Law, and Technology, 1. Retrieved January 2009, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking

Debussere, F. (2005). The EU e-privacy directive: A monstrous attempt to starve the cookie monster? *International Journal of Law and Information Technology*, *13*(1), 70–97.

Dutch Data Protection Authority (2007). Dutch DPA guidelines—Publication of personal data on the Internet. Retrieved May 2008, from http://www.dutchdpa.nl/downloads_overig/en_20071108_richtsnoeren_internet.pdf?refer=true&them=purple

Earp, J. B., Anton, A., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, *52*(2), 227–236.

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM*, *46*(4), 81–83.

Elgesem, D. (1999). The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. *Ethics and Information Technology*, *1*, 283–293.

European Commission (2008). Eleventh Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy

in the European Union and in third countries. Retrieved January 2009, from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf
European Union (1995a). Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data. Retrieved May 2008, from http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
European Union (1995b). Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data. Retrieved May 2008, from http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf
European Union (2002). Directive 2002/58 EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. Retrieved May 2008, from http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf
Fernback, J., & Papacharissi, Z. (2007). Online privacy as legal safeguard: The relationship among consumer, online portal, and privacy policies. *New Media and Society*, *9*(5), 715—734.
Franzak, F., Pitta, D., & Fritsche, S. (2001). Online relationships and the consumer's right to privacy. *Journal of Consumer Marketing*, *18*(7), 631—641.
Fried, C. (1984). Privacy: A moral analysis. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology* Cambridge: Cambridge University Press.
Ha, V., Al Shaar, F., Inkpen, K., & Hdeib, L. (2006). An examination of user perception and misconception of internet cookies. In *CHI 2006 extended abstracts on human factors in computing systems, Montreal, Canada, Association for Computer Machinery*, 833–838.
Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Information privacy in the marketplace: Implications for the commercial uses of anonymity on the web. *The Information Society*, *15*, 129—139.
Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*, 203—227.
Kierkegaard, S. M. (2005). How the cookies (almost crumbled): Privacy & lobbyism. *Computer Law & Security Report*, *21*, 310—322.
LaRose, R., & Rifon, N. (2006). Your privacy is assured—of being disturbed: Websites with or without privacy seals. *New Media & Society*, *8*(6), 1009—1029.
Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—A privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, *42*, 289—304.
Markel, M. (2005). The rhetoric of misdirection in corporate privacy-policy statements. *Technical Communication Quarterly*, *14*(2), 197—214.
Markel, M. (2006). Safe harbor and privacy protection: A looming issue for IT professionals. *IEEE Transactions of Professional Communication*, *49*(1), 1—11.
Milne, G. R., & 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.
Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumer's protection of online privacy and identity. *Journal of Consumers Affairs*, *38*(2), 217—232.
Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, *35*(1), 27—43.
Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers and Society*, *27*(3), 27—32.
Olivero, N., & 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*, 243—262.
Organization for Economic Cooperation and Development. (2002). OECD guidelines on the protection of privacy and transborder flows of personal data Paris: OECD.
Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331—338.
Papacharissi, Z., & Fernback, J. (2005). Online privacy and consumer protection: An analysis of portal privacy statements. *Journal of Broadcasting & Electronic Media*, *49*(3), 259—281.
Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27—41.
Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power, and informed consent. *Journal of Business Ethics*, *62*, 221—235.
Pollach, I. (2007). What's wrong with online privacy policies? *Communications of the ACM*, *50*(9), 103—108.
Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information & Management*, *43*, 805—820.
Strauss, J., & Rogerson, K. S. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics*, *19*, 173—192.
Tavani, H. T., & Moor (2001). Privacy protection, control of information, and privacy-enhancing technologies. *Computers and Society*, *31*(1), 6—11.
Turner, E. C., & Dasgupta, D. (2003). Privacy on the web: An examination of user concerns, technology and implications for business organizations and individuals. *Information Systems Management*, *20*(1), 8—18.
Vu, K. P., Chambers, V., Garcia, F., Creekmur, B., Sulaitis, J., Nelson, D., Pierce, R., & Proctor, R. (2007). How users read and comprehend privacy policies. In M. J. Smith, & G. Salvendy (Eds.), *Human interface, Part II* (pp. 802—811). Berlin-Heidelberg: Springer-Verlag.
Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about internet marketing. *Communications of the ACM*, *41*(3), 63—70.
Westin, A. F. (1967). Privacy and freedom New York: Atheneum.
Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431—453.
Woo, J. (2006). The right not to be identified: Privacy and anonymity in the interactive media environment. *New Media and Society*, *8*(6), 949—967.

Ardion Beldad is pursuing his PhD at the Department of Technical and Professional Communication, University of Twente, The Netherlands. His main research concerns trust and privacy issues in online transactions, specifically in the context of electronic government. Contact a.beldad@utwente.nl.

Menno De Jong is an associate professor of communication studies at the University of Twente, the Netherlands. His main research interest concerns the methodology of applied communication research. Contact m.d.t.dejong@utwente.nl.

Michael Steehouder is the chair of the Technical and Professional Communication Department at the University of Twente. His research interests include document design and rhetoric. Contact m.f.steehouder@utwente.nl