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