Business Ethics: A European Review
Volume 20 Number 1 January 2011

Online privacy as a corporate social responsibility: an empirical study

Irene Pollach

Aarhus School of Business, University of Aarhus, Aarhus, Denmark

Information technology and the Internet have added a new stakeholder concern to the corporate social responsibility (CSR) agenda: online privacy. While theory suggests that online privacy is a CSR, only very few studies in the business ethics literature have connected these two. Based on a study of CSR disclosures, this article contributes to the existing literature by exploring whether and how the largest IT companies embrace online privacy as a CSR. The findings indicate that only a small proportion of the companies have comprehensive privacy programs, although more than half of them voice moral or relational motives for addressing online privacy. The privacy measures they have taken are primarily compliance measures, while measures that stimulate a stakeholder dialogue are rare. Overall, a wide variety of approaches to addressing privacy was found, which suggests that no institutionalization of privacy practices has taken place as yet. The study therefore indicates that online privacy is rather new on the CSR agenda, currently playing only a minor role.

Introduction

Since the 1990s, companies striving to be good corporate citizens have had to devise strategies to address issues such as pollution, energy use, waste production, animal testing, child labor, sweatshops, workforce diversity, or advertising to children. It has become a *de-facto* standard for very large corporations to publish social reports documenting how they address these issues in the marketplace, the workplace, the supply chain, and the community in order to fulfill their role as good corporate citizens (Snider *et al*. 2003). The advent of the Internet has not only revolutionized many business models but has also redefined what it means to be a good corporate citizen (Post 2000), as most of the above issues are of little relevance to companies dealing with data and technology. One issue of public concern that has become highly relevant for IT companies is online privacy (De George 2000, Johnson 2006).

Information privacy denotes an individual's right to decide what information is made available to others (Westin 1967). Privacy is thus guaranteed only if individuals know that data are collected about them and if they have control over this data collection and the subsequent use of the data (Foxman & Kilcoyne 1993, Caudill & Murphy 2000). In the United States, privacy-related legislation exists only for health care, financial services, and children on the Internet (Bowie & Jamal 2006), while many aspects of data collection and user control in electronic commerce are still unregulated (Fernback & Papacharissi 2007). Countries of the European Union, meanwhile, protect privacy more strictly (Baumer *et al*. 2004), which has proven to be a hurdle for US technology companies operating in Europe. In 2008, for example, technology giant Google encountered problems in several European countries with its data handling practices (O'Brien 2008). Despite legislative efforts in Europe, data privacy violations have occurred in a number of

doi: 10.1111/j.1467-8608.2010.01611.x

Business Ethics
A EUROPEAN REVIEW

large organizations, including, for example, the largest German bank, DeutscheBank (Neate 2009), or T-Mobile UK (Wray 2009). The problems with privacy legislation are that it is difficult to identify violations of these laws and that the law may lag behind what is technologically feasible.

For the above reasons, global companies have some discretion over how much privacy they grant users and how much they reveal about their data handling practices to their users. This discretion adds extra complexity to the moral issue of whether companies take advantage of their powerful position by collecting and using data from users to further their own business interests, for example by sending out unsolicited promotional e-mails or selling user data (Pollach 2005).

The discretion companies can exercise when it comes to information privacy and the ethical implications of this discretion entail that information privacy is a question of corporate morality. While theoretical work on corporate social responsibility (CSR) suggests that privacy could be a meaningful addition to a corporate CSR program, little is known about corporate practices. This paper therefore sets out to explore whether and how companies whose core business is based on data and technology are embracing information privacy as a CSR. The findings suggest that information privacy is emerging as an element of CSR programs, but that there is a great deal of variety regarding the adoption of privacy as a CSR. The paper first discusses the moral issues behind information privacy on the Internet, reviews the literature on corporate responses to people's privacy concerns, and then looks at the literature on privacy as a CSR. After describing the sample and the methodology underlying this study, the results are presented and their implications are discussed.

The ethics of information privacy

The very core of electronic and mobile commerce revolves around technology, digitization, and the exchange of information, which poses a number of ethical problems (Zonghao 2001). A particular challenge to information handling in electronic commerce is the trade-off between collecting data for the sake of transparency and not collecting data for the sake of privacy (Introna & Pouloudi 1999). Another challenge is the trade-off between collecting data for the sake of profits and not collecting data for the sake of privacy.

As commercial transactions on the Internet or through mobile phones are commonly based on credit-card payments and the shipment of goods to the buyer's home address, the balance is tipped towards the need for disclosure rather than the safeguard of privacy. However, companies collect not only personally identifying information (PII) from transactions but also collect PII when users register themselves, use online services, participate in sweepstakes or surveys, or send inquiries to the company. In addition to PII, companies collect anonymous click-stream 1/2 data and compile anonymous user profiles when Internet users navigate the companies' websites (Kelly & Rowland 2000). Through the collection of IP addresses, PII can also be combined with anonymous click-stream data in order to obtain very comprehensive user profiles (Payne & Trumbach 2009). The easier access to and increased mobility of data have made information a commodity that is bought and sold by data brokers (Spinello 1998). It is therefore also possible for companies to buy datasets of user information from data brokers and merge them with the data they have collected themselves.

Companies may use the data they collect from customers and visitors on their websites merely to execute transactions, recognize users when they return to the site, and improve their website design based on users' interests. But companies may equally use such data for purposes other than those they were collected for. For example, they may target banner ads at users, harass users with unsolicited commercial e-mails, or share this information with third parties (Han & Maclaurin 2002). A growing body of literature documents people's concerns about privacy violations in online transactions (e.g. Culnan & Armstrong 1999, Phelps *et al*. 2000, Sheehan 2002, Norberg & Horne 2007, Norberg *et al*. 2007). Essentially, these concerns stem from the imbalance in power between companies as data collectors and users as data providers. While companies have superior knowledge of what user data are collected and how they are

handled, users may not even be aware that data are collected, let alone that they are combined into user profiles.

Corporate response to privacy

At the turn of the century, some companies began to introduce chief privacy officers (Awazu & Desouza 2004). Their tasks include gathering information about social and legal aspects of privacy, devising the company's privacy strategy, disseminating information about corporate data handling practices to internal and external stakeholders, and representing the company's commitment to privacy (Kayworth *et al*. 2005). Another corporate response to information privacy is privacy policies posted on commercial websites (Sama & Shoaf 2002). The original idea behind privacy policies on websites was that companies would disclose how they handle the data they collect from users, while users would carefully read through the explanation of the company's data handling practices, understand their consequences, and then make an informed decision about divulging personal data or not (Ciocchetti 2007). In reality, privacy policies contain legalese, tech-speak, and other obfuscating language patterns that obscure questionable data handling practices (Pollach 2005, Fernback & Papacharissi 2007). Internet users have been found not to read privacy policies for the above reasons (Milne & Culnan 2004). Privacy policies are sometimes supplemented with privacy seals awarded by private-sector institutions (e.g. BBBOnline, TRUSTe, WebTrust) or accounting firms. These seals indicate that companies comply with responsible standards of data handling, as defined by the awarding institution (Smith & Rupp 2004). Consumers still have to read and understand the privacy policy, as the seal alone does not guarantee that the data handling practices of the company comply with an individual's privacy preferences (Rifon *et al*. 2005). The problem with privacy seals is also that they do not effectively protect users from privacy breaches. The seal-awarding institution may not know about a privacy breach or, if it does learn about it, can only revoke the seal, but has no means to help people regain lost privacy (Shapiro & Baker 2001). These measures are thus not suited to enhance user privacy or engender trust among Internet users.

Information privacy as a CSR

Carroll (1979) categorized corporate social responsibilities into economic, legal, ethical, and philanthropic responsibilities, arguing that making a profit is the quintessential responsibility of companies, together with their adherence to legal regulations. According to this classification, information privacy can be categorized as an ethical responsibility, given that legislation is insufficient to govern corporate decision making in all areas of data handling. This is elaborated on by Mintzberg (1983), who suggested that areas where CSR comes into play are those 'where existing legislation needs compliance with its spirit as well as its letter [and] where the corporation can fool its customers or suppliers or the government through its superior knowledge' (p. 12).

If a company decides to address information privacy, it may not just do so because privacy is an ethical corporate responsibility. Rather, Aguilera *et al*. (2007) argue that companies accept responsibility for social issues for three different reasons: (1) moral reasons determined by morality-driven values; (2) relational reasons driven by the company's concern about stakeholder relationships; and (3) instrumental reasons driven by corporate self-interest. Moral motives are enacted particularly by individuals with organizational decision-making power who have strong morality-based values. Relational motives are grounded in a company's desire to promote and balance stakeholder interests, thereby building trust, maximizing stakeholder wealth, and gaining social legitimacy (Aguilera *et al*. 2007). Instrumental approaches are self-interest driven, seeking to achieve greater competitiveness and protecting the corporate reputation (Aguilera *et al*. 2007). The latter approach corresponds to Jones' (1995) argument that companies that manage to earn the trust of their stakeholders will be able to secure a competitive advantage through savings on monitoring costs, bonding costs, transaction costs, and search costs arising from managing the various corporate stakeholder groups. Instrumental motives

can also be driven by the desire to preempt costly government regulations (Aguilera *et al*. 2007).

The strategy literature follows the instrumental approach to CSR, arguing that companies to which a particular responsibility is highly relevant can benefit from integrating this responsibility into their overall strategies. Burke & Logsdon (1996) list the following conditions in order for CSR to bring strategic advantages to the firm: the chosen CSR issue is central to the company's mission, is voluntarily embraced, brings benefits to both the firm and to the public at large, is addressed in a proactive manner, and is visible to external stakeholders. It has also been argued that CSR initiatives can bring sustainable competitive advantages in the form of a first-mover advantage (Lieberman & Montgomery 1998). However, for this advantage to emerge, the company must not only be the first one to address a particular CSR comprehensively but must also continuously seek to enhance what it has achieved in order to secure this advantage (Tetrault Sirsly & Lamertz 2008).

The strategy literature therefore suggests that companies in the information technology industry could benefit from embracing online privacy as a CSR, especially if they make this commitment visible to external audiences. Although theory suggests that privacy could be a relevant CSR theme for particular companies, very few empirical studies have addressed the link between information privacy and CSR. They include Sharfman *et al*.'s (2000) survey among managers on how important they consider a number of social issues, including the protection of privacy. However, in the exploratory factor analysis they conducted, privacy was eliminated from further analyses. Fukukawa & Moon (2004) included information privacy as an indicator of CSR in their study of CSR activities reported by companies in Japan. In addition, Chaudhri's (2006) case study of global citizenship at Hewlett-Packard mentions privacy as one area the company has included in its CSR agenda. In previous theoretical work, Carroll (1998) has highlighted the protection of online privacy rights as one area where the law lags behind ethical thinking and morality comes into play. Finally, Post (2000) examined the changing role of corporate citizenship in the 21st century and pointed to customer privacy as a new issue of CSR. To date, there is no article that empirically studies in what ways information privacy is actually addressed as a CSR.

Research design

This study explores whether and how companies are embracing online privacy as a social responsibility, focusing on what measures they claim to have taken and how they communicate these to their external stakeholders in their CSR disclosures. In view of the lack of previous research in this area, this study is exploratory in nature. Accordingly, its goal is to identify the variety of corporate practices rather than to compare and contrast companies. The starting point for the analysis are the three processes of CSR included in Basu & Palazzo's (2008) process model of sense-making: (1) the reasons a company states for engaging in specific CSR activities, (2) the kind of behavior a company displays to live up to its CSR commitments, and (3) the way in which a company regards its relationships with its stakeholders. This section first describes the sample and the data and then goes on to explain the methodology that was applied to analyze the data.

Sample

The sample consists of the largest companies from IT-related industries, as they are most closely intertwined with information through the hardware, software, or services they provide. To them, information privacy could be a meaningful strategic element of their CSR programs in two different ways. First, they may embrace privacy as a social responsibility in the way they collect and use data. Second, technology does not just violate privacy, it can also enhance privacy. Accordingly, IT companies may engage in corporate social innovation and develop privacy-enhancing products or commit themselves to educating consumers about privacy protection. Clearly, other large companies, such as retailers, operate online as well, but were not considered for this study, as data and information are not at the core of their activities. Large companies were chosen, as these companies are believed to serve as lead innovators in their industries. All IT-related companies from Europe

and the United States listed among the *Fortune Global 500* and the first 1,000 companies of the *Forbes 2000* company rankings were included in the sample. Neither of the two rankings includes 'information technology' as an industry. Rather, both include a number of industries that deal with information and technology. These include Computer and Data Services, Computer Software, Computers & Office Equipment, Network and Other Communications Equipment, and Telecommunications from the *Fortune Global 500* list and Software & Services, Technology Hardware & Equipment, and Telecommunications Services from the *Forbes 2000* list. A few IT companies listed in these two rankings could not be included in the analysis, as they had been acquired by another company since the publication of the rankings. Also, the two rankings overlap to a substantial extent, so that the final sample amounted to a total of 95 IT companies.

On each company's website, the CSR section was accessed. If there was no such section, sections dedicated to the company background, mission and values, or ethics were accessed. The goal was to download all texts pertaining at least loosely to CSR and, if available, the latest CSR report. An important criterion was that privacy-related information was collected only if it was framed as a CSR issue. Privacy policies, which are a standard element of every commercial website, were not collected, as their existence alone does not represent a commitment to social responsibility. Of the 95 companies in the initial sample, 30 companies mention privacy in their CSR discourse. The analysis is thus based on these companies (see Appendix A). Their texts range from 21 to 2,367 words in length.

Methods

This exploratory study draws on both a positivist approach and a constructivist approach in order to look at the data as holistically as possible (cf. Jick 1979). When studying textual data, the fundamental difference between the two traditions is that the positivist tradition sees language as a transmitter of information, while the social constructionist tradition holds that people consciously and unconsciously create social realities when they use language. Accordingly, the textual data were first studied using quantitative content analysis, which systematically records the frequency of particular content features. Because of its quantitative, systematic nature, content analysis de-contextualizes the words from the discourse that is examined and therefore has no means to interpret its findings within a wider context. The findings of the content analysis were therefore combined with a discourse analysis and are presented together. The combination of content analysis and discourse analysis has also been suggested by researchers in linguistics (van Dijk 1985, Herring 2004), sociology (Markoff *et al.* 1974), and information systems (Trauth & Jessup 2000). In this study, the results of both analyses together provide a much richer picture of corporate practices than one analysis alone could furnish. This is important, given the absence of previous research on privacy and CSR.

Content analysis systematically condenses texts into content categories by applying a coding scheme that produces quantitative indices of textual content (Krippendorff 1980, Weber 1985, Kolbe & Burnett 1991, Neuendorf 2002). The content analysis conducted as part of this study records in a systematic and exhaustive manner which companies in the sample have implemented which measures to improve user privacy. The approach chosen for this analysis uses factual codes, which capture precisely defined facts, as opposed to thematic codes, which capture themes addressed in a predefined textual unit (Kelle & Laurie 1995). The factual codes pertain to privacy measures companies have actually taken, but exclude those that companies plan to implement in the future. With no existing coding scheme available, a preliminary coding scheme was developed from the data by examining the texts in the sample inductively (cf. Strauss & Corbin 1990) for measures that companies have taken to secure user privacy. Overall, 41 different measures were identified. The measures were recorded dichotomously as being either present (1) or absent (0). They are listed in Table 2 together with the results.

The qualitative approach chosen here was discourse analysis, following a social constructionist tradition, which views discourse as a social action that is shaped by and shapes the context in which it occurs (van Dijk 1997a). Discourse analysis is a

method of textual analysis that focuses on how and why language is used in a particular way (van Dijk 1997b). It is based on the premise that people intentionally and unintentionally construct social realities when they engage in discourse. They use language in their roles as members of particular social groups, professions, institutions, or communities but also construct such roles when they use language in social situations (van Dijk 1997a). Similarly, organizational texts can be constructive and constitutive of realities just like text or speech of individuals (Fairclough 2005). Discourse analysis typically pays attention to language features such as repetitions, pronouns, passive voice, nominalizations, modal verbs, agent–patient relations in sentences, and attitudinal lexis in order to study the roles assigned to the participants in the discourse, the power relations between them, and the foregrounding or the backgrounding of concepts and events. The discourse analysis conducted here examines how companies present themselves as responsible companies when it comes to privacy and data handling.

Basu & Palazzo's (2008) process model of CSR has guided the analysis and therefore also provides the structure of the results section. Accordingly, the results section starts with the companies' reasons for including privacy in their CSR programs, then presents privacy measures companies have taken as part of their CSR initiatives, and ultimately studies the relationships with the various stakeholders that are affected by the company's privacy practices. The reasons for including privacy and the stakeholder relationships are analyzed in the form of a discourse analysis. The analysis of the privacy measures is based on a content analysis, but enhanced with qualitative insights, as needed.

Results

Reasons for privacy as CSR

The texts were examined for indications of why the companies include privacy in their CSR programs. Only 13 companies voiced their motivation for engaging in privacy protection, presenting different reasons why they engage in CSR. The communicated motives have been grouped according to Aguilera *et al.*'s (2007) classification of moral, relational, and instrumental CSR motives. Table 1 shows this categorization together with the text passages where these motives were expressed. The moral motives found include the understanding that Internet users have privacy rights, which the company wants to observe, and the acknowledgement that the company has the responsibility to protect the data they gather from Internet users. Relational motives include the recognition that customers have a desire for privacy, which the company seeks to meet, and the expectation that privacy protection will help the company win customers' trust. Ultimately, one company expects to benefit from its privacy program in that it expects to gain a reputational advantage from privacy protection.

CSR behavior

The content analysis revealed 41 different measures companies had taken to support user privacy (see Table 2). They have been grouped into four categories, which are discussed below. One company has implemented 19 of these measures, and nine companies have implemented eight, nine, or 10 different measures. At the other end of the spectrum, there are two companies that have not implemented a single measure, but still talk about privacy in the context of CSR. Further, eight companies have implemented one or two measures, and nine companies have implemented between three and seven measures. Most commonly, a measure was taken by only one company (19 measures) or two companies (six measures). The measure taken most frequently was taken by 15 companies. Thus, there is a broad variety in how companies address privacy. It is also worth noting that it is not necessarily the biggest companies in the industry that have taken lead roles in protecting user privacy. When ranking all companies according to their ranks on the *Forbes 2000* and the *Fortune Global 500* lists, one can see that the company with the highest number of privacy measures ranks among the top three on both the *Forbes* and the *Fortune* list. The other two companies among the top three in the *Fortune* and *Forbes* rankings have implemented only one and three measures, respectively. The three companies

Table 1: Communicated motives for corporate privacy programs

Motive	Explanation	Quotations
Moral	Three companies acknowledge that people have a right to privacy	'To us, the right to privacy includes the right of individuals to have a voice in the use and dissemination of their personal information.'
		'A person has the right to control what information about him or her is collected and to determine how that information is used.'
		'Confidentiality and security of consumer data . . . are areas safeguarded by PT in order to respect the freedom and basic rights of each individual'
	Four companies hold that they have a responsibility to protect the data they gather from Internet users	'We feel a strong responsibility to help ensure a safer, more enjoyable Internet, while addressing the challenges to privacy and security posed by today's new media.'
		'Companies have a responsibility to ensure that the information they hold about their customers and employees is protected, stored, transferred, and used in a responsible manner.'
		'Microsoft takes seriously its responsibility to help address the security and privacy challenges of the information-based society, from viruses and spyware to spam and online identity theft.'
		'Respect for privacy is part of our commitment to observe high standards of integrity and ethical conduct in all our operations'
Relational	Two companies recognize that customers have a desire for privacy that needs to be met	'Protecting our customers' privacy is a priority. We understand and respect your desire to protect your personal information.'
		'The protection of personal information is a very high expectation among our customers, and to meet it, we . . ..'
	Four companies view privacy protection as a means to winning customer trust	'Externally, Sabre is committed to building customer relationships based on trust, and that includes recognizing the importance of protecting personal information.'
		'Consumer trust and confidence is critical to Cisco's business and to any technology and Internet-related business; as a result, the industry must protect citizens' privacy.'
		'[We] have to acquire a 'license to operate' by conducting our business in a decent and responsible way.'
		'Security and reliability form the basis of Telekom Austria Group's stable and successful customer relationships. The Group therefore gives top priority to protecting the integrity and confidentiality of sensitive data.'
Instrumental	One company states that it expects to gain a reputational advantage from its privacy program	'Main opportunities: Enhance customer and employee trust, . . . support brand/reputation.'

that have implemented the second highest number of privacy measures occupy ranks #77, #87, and #173 on the *Fortune Global 500* list and ranks #49, #518, and #782 on the *Forbes 2000* list, which indicates that it is not necessarily the biggest companies in the IT industries that embrace information privacy. An investigation of the relationship between the number of measures taken and length of the privacy text on the corporate website revealed a correlation of 0.77. This suggests that text length is an indicator of how important the issue is to a company. At the same time, it also shows that the companies generally do not talk at length about privacy without having taken relevant measures.

One category of measures pertains to the companies' internal affairs. They address processes, employee conduct, and, to a small extent, suppliers. The measures mentioned most frequently are the

Table 2: The content of corporate privacy programs

Internal	Physical protection of data	6	
	Procedural/administrative protection of data	2	
	Electronic/technical protection of data	3	
	Privacy policy	15	
	Privacy is part of the code of conduct	8	
	Privacy office(r)	7	
	Privacy board/working group	3	
	Employee training	9	
	Disciplinary action for employee misconduct	1	
	Privacy newsletter for employees	1	
	Employee monitoring	1	
	Privacy included in employment contract	1	
	Online resources for employees	1	
	Ethics hotline for privacy questions	1	
	Internal privacy campaign	1	
	Limited employee access to data	3	
	Online reporting of privacy incidents	1	
	Regular review of systems and processes	5	
	Regular review of privacy policy	3	
	Binding third parties to privacy agreements	5	
	Reviewing third-party privacy practices	2	79
External	Privacy newsletter for customers	1	
	Guidance/information for consumers	10	
	Resources for parental control & child safety	5	
	Privacy e-mail address	2	
	Integrating privacy into product development	8	
	Privacy blog	1	
	Involving stakeholders in design of privacy policy	1	
	Supporting IS education at schools and universities	1	
	Publishing privacy research papers	1	30
Collaborations	Supporting law making	2	
	Supporting industry self-regulation	1	
	Working with industry	5	
	Working with governments	6	
	Working with NGOs, think tanks	10	
	Political action committee (PAC)	1	25
Compliance	Compliance with laws	11	
	Exceeding laws	1	
	Compliance with Safe Harbor	4	
	Compliance with GRI	1	
	Privacy seal	4	21

existence of a privacy policy and privacy training, privacy being part of the code of conduct, privacy officers, physical data protection, and regular review of systems and processes. All other measures taken internally were taken by one, two, or three companies each, for example measures encouraging employees to report privacy violations and to comply with relevant guidelines. Two different measures pertaining to suppliers or other third parties were identified, namely that the company reviews privacy practices of those partners and that these outsiders are bound to a privacy agreement.

The second category of measures contains those directed towards external stakeholders. They include

primarily guidance for consumers regarding Internet privacy. Five companies take measures that address parents' concerns about their children's privacy. In addition to providing information, companies also solicit consumer feedback on privacy matters. Two companies highlight that they have an e-mail address to which people can send privacy concerns and inquiries, and one company involves stakeholders in the design of its privacy policy. The inclusion of privacy considerations in product development was embraced by eight companies.

Another group of measures pertain to the participation in industry initiatives and collaborations. Ten companies mention a variety of privacy forums, centers, associations, think tanks, and institutes in which they are involved, including for example, the Electronic Privacy Group, the European Privacy Officers Forum, or the Liberty Alliance. Some of them also state that they cooperate with other companies and governments. However, the nature of this cooperation remains unclear, and in some places, the cooperating institutions are not even mentioned. Ultimately, a few US companies express their views on privacy legislation. As part of the measures they have taken, three companies take an active stance for either privacy legislation or self-regulation. Both of these viewpoints are visions at this point, as there is neither privacy legislation nor a functioning model of self-regulation in the United States. The two viewpoints are as follows:

> 'We also believe that governments must find improved ways to enforce laws against data breach, misuse and fraud, and help consumers pursue those who mishandle their personal information. ... HP was one of the first companies to embrace the idea of a comprehensive U.S. privacy law.'

> 'Because disparate and multiple privacy rules place a heavy burden on global companies, we support a model of industry self-regulation (as opposed to government intervention) in which innovative tools give consumers greater choice in both protecting their personal data and understanding how it may be collected and used.'

Even companies that do not take a stance on the legislation vs. self-regulation debate emphasize compliance with legislation. Eleven companies state that they comply with all relevant privacy laws. As compliance with laws is a legal rather than an ethical responsibility according to Carroll's (1979) classification of corporate responsibilities, only going beyond the law can qualify as a CSR initiative. Dressing up a legal responsibility as an ethical responsibility casts doubt over the sincerity of these efforts. In fact, one of these 11 companies has implemented no other privacy measure apart from legal compliance. There is only one company that vows to exceed legal requirements: 'HP is pioneering an approach to the protection and responsible use of personal information. This effort goes beyond compliance with the law.' Only a minority of companies have adopted the privacy standards of outside organizations, such as GRI or privacy seal programs.

Stakeholder relationships

The measures identified above relate to a number of internal and external stakeholder groups, including employees, consumers, parents, industry, suppliers, governments, advocacy groups, and the community at large. However, the analysis of the measures does not reveal anything about the relationships with stakeholders, and in some cases, the stakeholder group to which a particular measure was addressed was not even mentioned. This section therefore focuses specifically on the stakeholder groups to which the companies express some form of consideration. This could be in the form of protection measures, information provision, cooperation, or merely by expressing an awareness of their stakes in privacy. In addition to an account of these overt commitments to stakeholders, a discourse analysis is used to uncover discursively constructed relationships with stakeholders.

Table 3 lists the various stakeholder groups identified, together with their stake in privacy, the number of companies that made a commitment toward each stakeholder group, and an example of such a commitment. This table is different from the results presented in Table 2 in that it was not concrete actions that guided this analysis, but the awareness of stakeholder concerns. We find that companies recognize primarily the stakes of their customers and employees, who exercise a direct and economic influence on the company and can therefore be labeled

Table 3: Addressing stakeholder concerns

Stakeholder Group	Stake	#	Example
Primary			
Customers/ Users	Protection of their data	25	'In order to help our customers address these issues, we have begun to develop guidance documents to help customers understand which parts of our technology may have privacy applications.'
Employees	Training	14	'We work hard to ensure that Sun employees have the information they need to apply our privacy protection standards in their work.'
Suppliers/ Vendors	Guidelines	6	'When it is necessary for business reasons to share a person's information with third parties such as network service providers and marketing campaign partners, we work together to ensure that we maintain the highest privacy standards.'
Secondary			
Government	Compliance with laws; expertise in data handling	6	'We met with government officials and regulators in all regions to understand their concerns and initiatives and to help them fully appreciate the potential implications for privacy of new technologies.'
Industry	Cooperation	6	'We are working with other industry participants . . . to develop solutions that help us reach both of these objectives.'
Advocacy groups	Cooperation	3	'In 2007, we formed our Stakeholder Advisory Council (SAC) comprising respected experts from a variety of nongovernmental organizations.'
Parents	Protection of their children's data	5	'Symantec is committed to helping parents keep their kids cybersafe. We believe that in the same way that we educate our children about the risks of drugs, smoking, or violence, it is critical that we educate them about the importance of safe computing.'
Schools/ communities	Expertise	1	'We tap this internal resource to offer programs that benefit our local schools and communities. We are also in the process of implementing an employee-led education program.'

'primary stakeholders' according to Ansoff (1965). However, there are also companies that talk about privacy in a CSR context, but do not voice a commitment to these two primary stakeholder groups. Of the 30 companies, five do not state that they do anything to improve the privacy situation of their customers and 16 do not make such a commitment toward their employees. Suppliers, who are also primary stakeholders, are addressed to a smaller extent. We can also see that the companies in the sample largely neglect their secondary stakeholders, i.e. those groups who do not directly influence a company's core business (Ansoff 1965). Only a maximum of six companies interact with each secondary stakeholder group, such as parents or governments.

On the surface, all companies studied engage in a discourse characterized by care and concern for privacy. In particular, emotion-laden words like *help*, *understand*, *respect*, *concern*, and *safe* abound across all texts studied. For example:

> 'Protecting our customers' privacy is a priority. We understand and respect your desire to protect your personal information.'

> 'And as the 24 × 7 demands of the Internet Age threaten to overwhelm customers with complexity, they need trusted and reliable companies to help them make sense of technology and put it to use to make their lives better.'

The tone becomes even more concerned when companies address their relationship with parents and children:

> 'We understand the responsibility and concern of parents who worry about their children's exposure to inappropriate content and potentially dangerous interactions on the Web.'

> 'Protecting our children . . . We believe that in the same way that we educate our children about the risks of drugs, smoking, or violence, it is critical

that we educate them about the importance of safe computing.'

In the second example, the pronoun 'we/our' adds to the concerned tone by promoting a sense of collegiality and shared affection. The same is also achieved in other places, when companies use this inclusive form of 'we' to reduce the distance between themselves and their outside stakeholders: 'Our individual sensitivities about how our information is treated . . . are not uniform' or 'Sun is committed to investigating and addressing the privacy challenges . . . associated with our increasingly digital way of life.' In such statements, companies reduce the power distance between themselves and their stakeholders. The inclusive 'we' is also an indicator of positive politeness (Brown & Levinson 1987), indicating how writers conceptualize their audiences and what kind of distance writers create between themselves and their audience. While some companies use the inclusive 'we,' others talk about companies in general, e.g. 'all businesses are responsible for . . .,' which includes themselves only implicitly and distances themselves from these events. Mostly, though, companies make themselves the causal agents: 'we must address these concerns by helping to protect . . ..' Notably, one company draws its audiences into the discourse by always addressing them directly, e.g. 'We understand and respect your desire to protect . . ..' All together, the different voices present in these texts suggest that companies have different levels of self-awareness and different understandings of their role in this process. Less variety exists in the distance to the audience, which is – apart from one exception – not explicitly present in the discourse. This suggests that companies do not consider their CSR activities to be dialogic in nature.

Another kind of discourse is found in 10 of the companies' texts studied. This discourse reveals that some companies are actually interested in finding a balance between users' privacy interests and their own business interests rather than protecting privacy unconditionally. They seek to achieve a balance between customers' privacy interests and 'business priorities,' 'business requirements,' 'business needs,' their 'values,' or their 'ability . . . to reap the benefits of online interactions.' Business interests are also communicated implicitly: 'our goal is simple: to balance the interests and concerns of our customers' private information with their interest in receiving quality service and information about useful new products.' Alternatively, one company mentions only one weight of the balance, without saying what the other weight is: 'that we are striking the right balance for our customers' and 'to reach balanced results.' The discourse of balance is a manifestation of the companies' power, given that it is they who decide when this balance is reached. Interestingly, this kind of discourse has nothing to do with the motivations they express. Two companies, for example, have voiced moral motives, but also engage in this discourse of balance, as does the one company that has indicated an instrumental motive. It is also worth noting that not a single European company in the sample engages in this discourse of balance.

Discussion

The literature review has highlighted that users are concerned about privacy and that companies do not respond in a manner that eases stakeholder concerns. The companies chosen for this study are all active in the hardware, software, or telecommunications industries, in which data play a crucial role. Thus, information privacy, and in particular online privacy, is a central issue in their business conduct. The content analysis has revealed that only a small proportion of the largest IT companies comprehensively address privacy as a social responsibility. In the sample, we find both companies that have taken a number of relevant actions to address user privacy and companies that have only taken one or two concrete measures, but nevertheless present privacy as part of their CSR program. A substantial proportion of the measures they have taken fall into the area of compliance and employee conduct (e.g. guidelines, policies, monitoring, and reporting), while measures that stimulate a stakeholder dialogue or represent corporate social innovation are found less frequently. Further, some companies reveal that they seek to strike a balance between their own business interests and their stakeholders' privacy needs. The sample even contains companies that

voice moral motives for framing online privacy as a CSR, while at the same time indicating that they are interested in striking a balance between users' privacy interests and their own business interests. We have also seen that some of the privacy measures are actually intended to fulfill legal responsibilities rather than ethical ones. Thus, some companies in the sample voice concerns and a commitment to help, but do not take privacy to the level of an ethical responsibility (cf. Carroll 1991). At the same time, companies load their privacy discourse with emotive terms suggesting concern, commitment, and a desire to help. While this kind of language is typical of CSR messages and can almost be expected (cf. Pollach 2003), it is still in contrast to the results of the content analysis, which has shown that comprehensive privacy programs are for the most part non-existent.

The findings also indicate that companies have chosen a wide variety of approaches to information privacy. In fact, many of the different measures identified were taken by one, two, or three companies only. Thus, little mimicry and no institutionalized practices have emerged yet. In uncertain environments, companies have a tendency to model themselves after other companies that are more successful or more respected. This mimicry leads to institutionalized practices that help companies to obtain legitimacy (DiMaggio & Powell 1983). The environment in which the sample companies operate can be characterized as uncertain, as there is no comprehensive privacy legislation as yet and privacy is, to some extent, at each company's discretion. For mimicry behavior to occur, it must be clear to the firm that adopting a certain practice brings competitive advantages (DiMaggio & Powell 1983). In the case of privacy, an institutionalization of voluntary privacy practices could mean that privacy regulation is preempted. However, as not every company in the sample, and maybe in the industry as a whole, is pro self-regulation, some companies may decide not to adopt privacy practices voluntarily, despite the fact that they care about user privacy.

Privacy may be on its way to mature from the ethics/compliance focus to a more responsive, proactive focus, but at the moment, it plays a minor role as a CSR. This point is also reflected in the finding that companies address primarily consumer concerns and step up employee training, while all other stakeholder groups in privacy play a subordinate role. Companies may not have recognized the benefits to be gained from engaging with secondary stakeholder groups, e.g. from cooperating with industry partners. At the same time, companies may have been too occupied with implementing privacy standards internally, so that their privacy efforts do not involve secondary stakeholders as yet. These internal compliance measures are clearly the *sine qua non* for a company's external privacy activities, such as participation in industry initiatives.

This study is not without limitations. One clear limitation is that the data stem from corporate self-reports, which are problematic (cf. Podsakoff & Organ 1986) in that they are based on what the company reveals rather than what is actually true. This could mean that companies overstate their activities. At the same time, companies may not have mentioned the particular measures they have taken, because they did not consider them important enough. Also, the sample size could have been larger, but the small sample size also serves to illustrate that privacy is just about to begin to play a role in CSR programs of technology-oriented companies.

Appendix A: Companies in the sample

Adobe
Agilent
ATT
Belgacom
British Telecom
Cisco
Computer Associates
Dell
Deutsche Telekom
Electronic Data Systems
France Telecom
HP
IBM
Microsoft
Motorola
Nokia
Oracle

Portugal Telekom
Royal KPN
Sabre
Sprint
Sun
Symantec
Telefonica
Telekom Austria
Telia Sonera
Verizon
Virgin
Vodafone
Xerox

References

Aguilera, R.V., Rupp, D., Williams, C.A. and Ganapathi, J. 2007. 'Putting the S back in CSR: a multilevel theory of social change in organizations'. *Academy of Management Review*, 32:3, 836–863.

Ansoff, I. 1965. *Corporate Strategy*. New York, NY: McGraw-Hill.

Awazu, Y. and Desouza, K.C. 2004. 'The knowledge chiefs: CKOs, CLOs and CPOs'. *European Management Journal*, 22:3, 339–344.

Basu, K. and Palazzo, G. 2008. 'Corporate social responsibility: a process model of sensemaking'. *Academy of Management Review*, 33:1, 122–136.

Baumer, D.L., Earp, J.B. and Poindexter, J.C. 2004. 'Internet privacy law: a comparison between the United States and the European Union'. *Computers and Security*, 23:5, 400–412.

Bowie, N. and Jamal, K. 2006. 'Privacy rights on the internet: self-regulation or government regulation?'. *Business Ethics Quarterly*, 16:3, 323–342.

Brown, P. and Levinson, S.C. 1987. *Politeness*. Cambridge: Cambridge University Press.

Burke, L. and Logsdon, J.M. 1996. 'How corporate social responsibility pays off'. *Long Range Planning*, 29:4, 495–502.

Carroll, A.B. 1979. 'A three-dimensional conceptual model of corporate performance'. *Academy of Management Review*, 4:4, 497–505.

Carroll, A.B. 1991. 'The pyramid of corporate social responsibility: toward the moral management of organizational stakeholders'. *Business Horizons*, 34:4, 39–48.

Carroll, A.B. 1998. 'The four faces of corporate citizenship'. *Business and Society Review*, 100:1, 1–7.

Caudill, E.M. and Murphy, P.E. 2000. 'Consumer online privacy: legal and ethical issues'. *Journal of Public Policy and Marketing*, 19:1, 7–19.

Chaudhri, V.A. 2006. 'Organising global CSR: a case study of Hewlett-Packard's e-inclusion initiative'. *Journal of Corporate Citizenship*, 23, 39–51.

Ciocchetti, C.A. 2007. 'E-commerce and information privacy: privacy policies as personal information protectors'. *American Business Law Journal*, 44:1, 55–126.

Culnan, M.J. and Armstrong, P.K. 1999. 'Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation'. *Organization Science*, 10:1, 104–115.

De George, R.T. 2000. 'Business ethics and the challenge of the information age'. *Business Ethics Quarterly*, 10:1, 63–72.

DiMaggio, P.J. and Powell, W.W. 1983. 'The iron cage revisited: the institutional isomorphism and collective rationality in organizational fields'. *American Sociological Review*, 48:2, 147–160.

Fairclough, N. 2005. 'Critical discourse analysis, organizational discourse, and organizational change'. *Organization Studies*, 26:6, 915–939.

Fernback, J. and 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.

Foxman, E.R. and Kilcoyne, P. 1993. 'Information technology, marketing practice, and consumer privacy: ethical issues'. *Journal of Public Policy and Marketing*, 12:1, 106–119.

Fukukawa, K. and Moon, J. 2004. 'A Japanese model of corporate social responsibility? A study of website reporting'. *Journal of Corporate Citizenship*, 16, 45–59.

Han, P. and Maclaurin, A. 2002. 'Do consumers really care about online privacy?'. *Marketing Management*, 11:1, 35–38.

Herring, S.C. 2004. 'Computer-mediated discourse analysis: an approach to researching online behavior'. In Barab, S.A., Kling, R. and Gray, J.H. (Eds.), *Designing For Virtual Communities in the Service of Learning*: 338–376. New York, NY: Cambridge University Press.

Introna, L.D. and Pouloudi, A. 1999. 'Privacy in the information age: stakeholders, interests and values'. *Journal of Business Ethics*, 22:1, 27–38.

Jick, T.D. 1979. 'Mixing qualitative and quantitative methods: triangulation in action'. *Administrative Science Quarterly*, 24, 602–611.

Johnson, D. 2006. 'Corporate excellence, ethics, and the role of IT'. *Business and Society Review*, 111:4, 457–475.

Jones, T.M. 1995. 'Instrumental stakeholder theory: a synthesis of ethics and economics'. *Academy of Management Review*, 20:2, 404–437.

Kayworth, T., Brocato, L. and Whitten, D. 2005. 'What is a chief privacy officer?'. *Communications of AIS*, 16, 110–126.

Kelle, U. and Laurie, H. 1995. 'Computer use in qualitative research and issues of validity'. In Kelle, U. (Ed.), *Computer-Aided Qualitative Data Analysis. Theory, Methods and Practice*: 19–28. London: Sage.

Kelly, E.P. and Rowland, H.C. 2000. 'Ethical and online privacy issues in electronic commerce'. *Business Horizons*, 43:3, 3–12.

Kolbe, R.H. and Burnett, M.S. 1991. 'Content-analysis research: an examination of applications with directives for improving research reliability and objectivity'. *Journal of Consumer Research*, 18:2, 243–250.

Krippendorff, K. 1980. *Content Analysis: An Introduction to its Methodology*. Beverly Hills, CA: Sage.

Lieberman, M.B. and Montgomery, D.B. 1998. 'First-mover (dis)advantages: retrospective and link with the resource-based view'. *Strategic Management Journal*, 19:12, 1111–1125.

Markoff, J., Shapiro, G. and Weitman, S.R. 1974. 'Toward the integration of content analysis and general methodology'. In D. Heise (Ed.), *Sociological Methodology*: 1–58. San Francisco, CA: Jossey-Bass.

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.

Mintzberg, H. 1983. 'The case for corporate social responsibility'. *Journal of Business Strategy*, 4:2, 3–15.

Neate, R. 2009. 'Deutsche Bank admits possible privacy breaches.' *The Telegraph*, July 23.

Neuendorf, K.A. 2002. *The Content Analysis Guidebook*. Thousand Oaks, CA: Sage.

Norberg, P.A. and Horne, D.R. 2007. 'Privacy attitudes and privacy-related behavior'. *Psychology and Marketing*, 24:10, 829–847.

Norberg, P.A., Horne, D.R. and Horne, D.A. 2007. 'The privacy paradox: personal information disclosure intentions versus behaviors'. *Journal of Consumer Affairs*, 41:1, 100–126.

O'Brien, K.J. 2008. 'Privacy laws trip up Google's expansion in parts of Europe.' *New York Times*, November 18.

Payne, D. and Trumbach, C.C. 2009. 'Data mining: proprietary rights, people and proposals'. *Business Ethics: A European Review*, 18:3, 241–252.

Phelps, J., Nowak, G. and Ferrell, E. 2000. 'Privacy concerns and consumer willingness to provide personal information'. *Journal of Public Policy and Marketing*, 19:1, 27–41.

Podsakoff, P.M. and Organ, D.W. 1986. 'Self-reports in organizational research: problems and prospects'. *Journal of Management*, 12:4, 531–544.

Pollach, I. 2003. *Communicating Corporate Ethics on the World Wide Web: A Discourse Analysis of Selected Company Websites*. Frankfurt: Peter Lang.

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.

Post, J.E. 2000. 'Moving from geographic to virtual communities: global corporate citizenship in a dot.com world'. *Business and Society Review*, 105:1, 27–46.

Rifon, N.J., LaRose, R. and Choi, S.M. 2005. 'Your privacy is sealed: effects of web privacy seals on trust and personal disclosures'. *Journal of Consumer Affairs*, 39:2, 339–362.

Sama, L.M. and Shoaf, V. 2002. 'Ethics on the web: applying moral decision making to the web'. *Journal of Business Ethics*, 36:1–2, 93–103.

Shapiro, B. and Baker, C.R. 2001. 'Information technology and the social construction of information privacy'. *Journal of Accounting and Public Policy*, 20:4, 295–322.

Sharfman, M.P., Pinkston, T.S. and Sigerstad, T.D. 2000. 'The effects of managerial values on social issues evaluation: an empirical examination'. *Business and Society*, 39:2, 144–182.

Sheehan, K.B. 2002. 'Toward a typology of internet users and online privacy concerns'. *The Information Society*, 18:1, 21–32.

Smith, A.D. and Rupp, W.T. 2004. 'Online privacy policies and diffusion theory perspectives: security or chaos?'. *Services Marketing Quarterly*, 25:3, 53–75.

Snider, J., Hill, R.P. and Martin, D. 2003. 'Corporate social responsibility in the 21st century: a view from the world's most successful firms'. *Journal of Business Ethics*, 48:2, 175–187.

Spinello, R.A. 1998. 'Privacy rights in the information economy'. *Business Ethics Quarterly*, 8:4, 723–742.

Strauss, A.L. and Corbin, J. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park, CA: Sage.

Tetrault Sirsly, C.A. and Lamertz, K. 2008. 'When does a corporate social responsibility initiative provide a first-mover advantage?'. *Business and Society*, 47:3, 343–369.

Trauth, E.M. and Jessup, L.M. 2000. 'Understanding computer-mediated discussions: positivist and interpretive analyses of group support system use'. *MIS Quarterly*, 24:1, 43–79.

van Dijk, T.A. 1985. 'Levels and dimensions of discourse analysis'. In van Dijk, T.A. *Handbook of Discourse Analysis*, Vol. 2: 1–12. London: Academic Press.

van Dijk, T.A. 1997a. 'Discourse as interaction in society'. In van Dijk, T.A. *Discourse as Social Interaction*: 1–37. London: Sage.

van Dijk, T.A. 1997b. 'The study of discourse'. In van Dijk, T.A. *Discourse as Structure and Process*, Vol. 1: 1–34. London: Sage.

Weber, R.P. 1985. *Basic Content Analysis*. Beverly Hills, CA: Sage.

Westin, A.F. 1967. *Privacy and Freedom*. New York, NT: Atheneum.

Wray, R. 2009. 'T-Mobile confirms biggest phone customer data breach.' *The Guardian*, November 17.

Zonghao, B. 2001. 'An ethical discussion on the network economy'. *Business Ethics: A European Review*, 10:1, 108–112.