Journal of Business Ethics (2005) 62: 221–235
DOI 10.1007/s10551-005-7898-3

A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent

ABSTRACT. The opaque use of data collection methods on the WWW has given rise to privacy concerns among Internet users. Privacy policies on websites may ease these concerns, if they communicate clearly and unequivocally when, how and for what purpose data are collected, used or shared. This paper examines privacy policies from a linguistic angle to determine whether the language of these documents is adequate for communicating data-handling practices in a manner that enables informed consent on the part of the user. The findings highlight that corporate privacy policies obfuscate, enhance and mitigate unethical data handling practices and use persuasive appeals to increase companies' trustworthiness. The communicative strategies identified provide starting points for redesigning existing privacy statements with a view to communicating data handling practices in a more transparent and responsible manner, laying the groundwork for informed consent.

KEY WORDS: cookies, critical linguistics, data handling practices, electronic commerce, information privacy, language, privacy policies, trust, websites

Introduction

The growth of information technology has continuously produced new and enhanced possibilities for companies to collect, disseminate and combine data, which the advent of the Internet has extended even further. Internet commerce has brought with it not only increased speed and enhanced convenience for consumers, but has also fundamentally changed the relationship between companies and consumers by empowering online marketers with data collection methods at the expense of consumers' privacy interests (Kelly and Rowland, 2000). With the emergence of electronic commerce more data than ever before are being collected, while people have less control than ever before over their personal data (Stahl, 2004). The reason for this is that e-commerce is less anonymous than traditional commerce, since online merchants need to collect personal information such as names, shipping addresses and credit card numbers (Rennhard et al., 2004).

With consumer information being a key element of the exchange process between consumers and online merchants, the question of information ownership has become a central issue (De George, 2000). Neither consumers nor businesses have absolute proprietary rights to the information that is exchanged in commercial transactions. When people interact with others, their control over information about themselves is only relative and "limited by the rights of others" (Fried, 1968, p. 486), which means that Internet users give up some of their proprietary information rights when they complete transactions. Although businesses legitimately obtain consumer information during transactions or may even buy it from information brokers, it can hardly be argued that they have the right to use this information for any purpose without the consumer's consent (Foxman and Kilcoyne, 1993). Rather, consumers and businesses can be considered to have joint ownership privileges of consumer information (Mascarenhas et al., 2003).

Irene Pollach is an assistant professor in the Department of English Business Communication at the Vienna University of Economics and Business Administration in Austria. Her research interests include corporate communication, WWW-mediated stakeholder relations, and ethical aspects of the Internet. She is also the author of Communicating Corporate Ethics on the World Wide Web.

However, these joint ownership rights may not always be respected, given that electronic commerce puts web merchants in a better position to advance their interests than consumers (Introna and Pouloudi, 1999). These power asymmetries are, for example, evident from the fact that Internet users implicitly consent to a website's privacy policy when they enter the site and the first pieces of data may already have been collected before they have had a chance to read the website's privacy policy. Recent studies have also highlighted that web merchants post ambiguously worded privacy policies that deter users from reading them (Antón et al., 2004; Milne and Culnan, 2004). Even if privacy policies do not contain outright lies, the use of obfuscating language can lead to ethical problems when readers misinterpret texts (cf. Riley, 1993). According to the Theory of Informed Consent, people can only consent to something if they have received sufficient information, have understood it and have explicitly expressed agreement (Faden and Beauchamp, 1986). Since web merchants do not seem to communicate their data handling practices in such a manner, people are unable to provide informed consent to their data handling practices.

This paper first explores the notion of information privacy and looks at privacy policies in more detail. It then discusses the interests of key stakeholder groups in online privacy, examining data handling and informed consent in the light of normative ethical theories before going on to present the findings of a linguistic analysis of online privacy policies. The analysis draws on critical linguistics, a method useful for uncovering hidden meanings in texts. More precisely, critical linguistics examines how authors use grammar and vocabulary to construct their own versions of reality, thereby abusing their power as information providers (Fowler and Kress, 1979a). The linguistic analysis seeks to determine why the language of privacy policies is inadequate for communicating data-handling practices. The results of this analysis are intended to provide starting points for enhancing the readability and usefulness of online privacy policies in order to lay the groundwork for informed consent.

Privacy and privacy policies in e-commerce

Although there is no consensus on how to define privacy, there is agreement that privacy is an element of human dignity. One of the earliest definitions of privacy is offered by Warren and Brandeis (1890) who view privacy as the "the right to be let alone". Prosser (1960) identified four distinct but related torts associated with privacy interests, which have provided the basis for subsequent definitions of information privacy. These torts include (1) intrusion of a person's seclusion or solitude, (2) public disclosure of embarrassing private facts, (3) appropriation of a person's identity or image, and (4) publicity which places a person in a false light in the public eye. Although these torts do not explicitly relate to information privacy, they represent potential threats in electronic commerce, e.g. when Internet marketers use intrusive data collection methods or intrude a person's privacy by sending unsolicited commercial e-mails, when financial information is stolen or made available to third parties, or when marketers do not give users control over the data that have been collected about them.

Westin (1967) provided one of the first definitions of information privacy, which he defines as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). Fried (1968) holds that "privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves" (p. 482). Later definitions also stress control as a core element of information privacy. Hoffman (1980), for example, sees information privacy as a set of rights, including "the right of individuals to know what information about themselves is collected, to determine what information is made available to third parties, to access personal data". Similarly, consumer privacy has been defined as consumers' control over information disclosure and over the environment in which a transaction occurs (Goodwin, 1991). Foxman and Kilcoyne (1993) argued that privacy is a two-dimensional concept, embracing control over and knowledge of data collection.

Fried (1968) also recognized that control over personal information is essential to one's development as an individual and to the formation of respect and trust in relationships. He argued that being able to control who knows what about us allows us to maintain personal relationships of varying degrees of intimacy. Rachels (1975) has extended this proposition to all kinds of social relationships, arguing that there is a close connection between the ability to control who has access to one's information and one's ability to maintain different kinds of relationships with different parties. This line of reasoning seems to hold true in electronic commerce as well. Users have been found to divulge personal information only after a certain level of trust has been negotiated between users and Internet marketers (Chen and Rea, 2004). Furthermore, users' privacy concerns and the manner in which a company deals with user privacy have been found to determine the level of user trust in a website, which in turn influences users' behavioral intentions, i.e. whether or not they revisit the site, recommend it to others, or make purchases (Liu et al., 2004; Metzger, 2004).

In order to solicit more information from Internet users and encourage them to purchase online, Internet companies have begun to seek third party certification and post privacy statements on their websites (Palmer et al., 2000). Essentially, such privacy policies are legal documents, designed not only to inform readers how data are collected, what purposes they are used for and with whom they are shared but also to protect the company against privacy lawsuits (Metzger and Docter, 2003). Previous research on privacy policies has been quantitative in nature. For example, Antón et al. (2004) have assessed the readability of privacy policies of financial institutions by means of statistical text-readability metrics. They found that understanding 80% of these documents requires more than college education and concluded that almost one third of the U.S. adult population is unlikely to be able to understand the content of these documents since they contain complex words and sentence structures. These results suggest that the language of privacy policies is inadequate, which is in line with the findings from a user survey indicating that Internet users tend not to read privacy policies because they perceive them as too long, too legalistic and difficult to comprehend (Milne and Culnan, 2004). Other research on privacy policies has focused on the practices they address (Miyazaki and Fernandez, 2000), the practices companies actually admit to (Pollach, 2004), and their compliance with the Federal Trade Commission's Fair Information Practices (Liu and Arnett, 2002; Nyshadham, 2000; Ryker et al., 2002). The qualitative study presented in this paper adds well to the body of quantitative research on privacy policies by examining how they represent corporate data handling practices and suggesting ways to improve the quality of privacy disclosures.

Stakeholders in online privacy

Stakeholders in electronic commerce have been classified into participating stakeholders (e.g. companies, consumers), enabling stakeholders (e.g. trust-service providers), and supervisory stakeholders (e.g. policy makers) (Jones et al., 2000). Privacy policies not only regulate the relationship between participating stakeholders, but may also incorporate guidelines issued by enabling or supervisory stakeholders. In order to provide a deeper understanding of what roles are played by the key stakeholders in online privacy, this section examines how they can influence the level of privacy afforded to providers of data.

Online merchants

Web merchants collect personally identifying information when users register with a website, engage in transactions, or participate in sweepstakes (Oz, 2004). They also gather non-identifying information by placing invisible graphic files (''web bugs'') on their websites or by sending cookies to users' PCs to track how they move through the site (Bennett, 2001). They are even able to tie such non-identifying information to personally identifying information when users submit personal information via forms (Van Wel and Royakkers, 2004). These practices clearly give rise to a conflict between commercial interests and people's right to be left alone (Cannon, 2002), in particular when they use the personally identifying information they have collected to send unsolicited commercial e-mails to customers (Samoriski, 1999). Companies argue that they need to collect data in order to meet consumers' needs more effectively (Foxman and Kilcoyne, 1993) and personalize offerings (Stead and Gilbert, 2001).

Internet users

Users' privacy concerns in WWW-mediated environments have been the subject of numerous academic studies (e.g. Han and Maclaurin, 2002; Olivero and Lunt, 2004; Phelps et al., 2000; Saban et al., 2002; Shapiro and Baker, 2001). Although their concerns vary in terms of scope and intensity across situations and individuals, commonly voiced privacy concerns include data collection, data sharing, unsolicited marketing communications (Miyazaki and Fernandez, 2000), and the use of data for purposes other than those that they were collected for (Beltramini, 2003). To protect their privacy, individuals have been found to enter false data when asked to provide personal information (Hoffman et al., 1999), disable cookies, install anonymizers (Schwartz, 2001), block unsolicited commercial e-mails with filters (Sakkis et al., 2003), and subscribe to pseudonymity networks, which enable people to purchase digital goods anonymously (Rennhard et al., 2004).

Trust-service providers

Privacy advocacy groups have introduced programs that provide third-party certification of corporate privacy practices. Examples of such programs include TRUSTe and BBBOnline. Companies which voluntarily comply with the privacy standards prescribed by these groups may display the group's seal of approval on their websites to signal to users that they handle user data responsibly (Smith and Rupp, 2004). These third-party certification schemes can make a website more trustworthy in the eyes of the consumer, provided that the certifying party is credible (Koehn, 2003). However, seal programs have been accused of being more interested in adding new members than revoking seals (Boutin, 2002) and of accepting donations from corporate members (McCullagh, 1999).

Policy makers

Government initiatives regulating electronic privacy have taken different forms in different countries. In the European Union, they consist of comprehensive national legislation, as mandated by the E.U.'s Directive on Data Protection of 1998. Further, when E.U. citizens do business with companies in the U.S., their privacy is protected by the Safe Harbor Principles, which were laid down in an agreement between the E.U. and the U.S. in 2000. The U.S., by contrast, has not passed any laws governing specifically data privacy on the Internet, apart from the Children's Online Privacy Protection Act (COPPA). The U.S. Federal Trade Commission has, however, identified five Principles of Fair Information Practices, which companies are encouraged to adopt to address online privacy issues (Metzger and Docter, 2003). These principles include *Notice* (informing users how information is collected and used), *Access* (granting users access to their personal information), *Choice* (enabling users to opt in or out of data collection), *Data Security* (preventing unauthorized access to data), and *Enforcement/Redress* (imposing sanctions for non-compliance) (Federal Trade Commission, 2000).

Ethics and data handling

The unequal distribution of power between the two participating stakeholder groups in electronic commerce, viz. web merchants and Internet users, coupled with their conflicting interests gives rise to ethical issues. Normative theories are helpful in resolving such issues. In normative analyses, ethical situations can be examined from four different angles, including the agent, the act, its consequences, and the stakeholders affected. These four factors also constitute the foci of four different ethical realms, viz. virtue ethics, deontology, teleology and justice (Mason, 1995). One appropriate approach was chosen from each realm to discuss ethical aspects of data handling practices on the WWW. Table I shows the four foci, their corresponding realms, the ethical approaches chosen within these realms, and the criteria they employ to distinguish right from wrong.

Virtue ethics

Aristotle's virtue ethics focuses on the person that performs an act. It is based on a set of virtues, four of which he considered core virtues – courage, prudence, temperance, and justice. All virtues he

TABLE I

Ethical foci and their corresponding theories

Focus	Realm	Approach	Criterion
Agent	Virtue ethics	Aristotelian ethics	Golden mean
Act	Deontology	Categorical imperative	Universalizability
Consequences	Teleology	Utilitarianism	Maximum utility
Stakeholders	Justice	Rawls	Equality

identified are "the golden mean" on a continuum stretching between the extremes of deficiency and excess. According to Aristotle, justice is the highest of these virtues, as a just person is able to achieve a balance among all other virtues as well. People who habitually display at least the four core virtues are considered ethical agents (Mason et al., 1995). Given that the virtue of justice subsumes other virtues such as integrity, fairness and honesty, current data handling practices would only be ethically justified from the perspective of virtue ethics, if web merchants communicated their data handling practices in a comprehensible manner and asked the information providers for their consent before engaging in these practices.

Deontology

Kant's Categorical Imperative falls under deontological theories, which are based on rights and duties. According to Kant's approach, people have the duty to treat others as free persons equal to everyone else. The action of an agent is morally right if the agent would want other people to do the same thing in a similar situation and provided that the agent's interior motivation is a sense of duty and not the advancement of personal interests. This goes hand in hand with the golden rule "Do unto others as you would have them do unto you". Further, the Categorical Imperative commands us to respect other people's freedom by always treating them as ends and never as means. That is to say, people should be treated as they have consented to be treated (Velasquez, 2002). Thus, according to Kant's Categorical Imperative, a web merchant may collect and disseminate user data only if users have freely consented to such practices beforehand and if both users and the merchant benefit from the company's use of these data.

Teleology

Teleological theories focus on the results, consequences and goals of actions. One approach within this realm is utilitarianism, according to which actions are evaluated on the basis of the costs and benefits they impose on society. The right course of action is that which produces more utility (i.e. net benefits) than any other possible action and which therefore ensures the greatest good for the greatest number (Buchholz, 1995). In the context of data handling practices in WWW-mediated environments, this means that a company collecting user data without notifying people and obtaining their consent beforehand produces social costs by invading users' privacy. These costs need to be weighed against the benefits the company derives from these data and the benefits users may derive from more personalized offerings. To determine whether this action is right, these costs and benefits need to be compared with alternative actions. The obvious alternative course of action would be to inform users adequately and obtain their consent to data collection. This course of action would probably mean that companies gather less information, which would result in lower benefits for both the company and Internet users, but it would not produce the social costs associated with privacy invasion. Since obtaining users' informed consent produces the greatest overall utility, it is considered to be justifiable.

Justice

Justice seeks to strike a fair balance among the claims of all stakeholder groups involved in a situation. The concept of justice considers stakeholder claims individually rather than on an aggregate basis, but – unlike utilitarianism – does not tolerate the violation of basic individual rights and privileges (Mason et al., 1995). Rawls's Theory of Justice is based on the principle that basic rights and duties should be equally assigned to all stakeholders and that social inequalities should be arranged in a manner that ensures they are advantageous to everyone (Buchholz, 1995). Mason et al. (1995, p. 143) argue that

> "In a Rawlsian information society ... every stakeholder's basic rights and liberties – such as one's right to know; right to privacy; right to accurate, reliable, unbiased information; right to one's own intellectual and tangible property, and right to fair access to information and information technology – are protected".

By establishing privacy as a basic individual right, its invasion is simply intolerable according to Rawls's Theory of Justice. Further, the right to know implies that people would need to be informed beforehand if data about them are collected or shared with other parties. The right to access entails that users are granted access to the information that has been collected about them in order for data handling to be ethical.

Although the four ethical theories focus on different aspects of ethical situations, their verdicts are unanimous: Data collection and dissemination on the WWW is unethical without obtaining people's informed consent beforehand. However, for this to happen, data handling practices need to be communicated in a comprehensible and user-friendly manner.

Research design

The sample used for this study includes 22 online retailers and 6 online travel agencies (see Appendix). The retail companies were selected from the top 35 websites among *Store* magazine's *Top Internet Retailers* (Reda, 2000), excluding websites of conglomerates, those that had gone out of business, and those not available at the time of data collection. The resulting list of 22 websites was combined with online travel sites that were considered commercially successful by the business press (Ebenkamp, 2002; "Forrester Research", 2002). The total corpus consisted of 60,272 words and the average number of words per document was 2153, ranging from 638 to 5956 words.

The analysis draws on critical linguistics, a school of discourse analysis, which is based on the works of Fowler and Kress (1979a, b), Fowler (1985), Kress (1985), and Hodge and Kress (1993). It follows Halliday's (1978) notion that the grammatical choices we make encode representations of the world and construe the world from our point of view. Critical linguistics views language and in particular grammatical forms as linguistic choices writers make to influence (Fowler and Kress, 1979a), inform, and deceive audiences (Hodge and Kress, 1993). A textual analysis guided by critical linguistics is able to uncover hidden meanings and realizations of ideologies (in the sense of worldviews) by looking at the lexical, semantic and syntactical choices a writer has made and their implications for the representation of events (Kress, 1985). These findings could provide starting points for improving documents as to clarity, accuracy and comprehensibility. For the present analysis, critical linguistics will determine whether the privacy policies examined enable informed consent on the part of the user, which is a prerequisite for ethical data handling practices on the web.

Fowler (1985) offers a checklist of parameters that may be worth examining when carrying out critical linguistic analyses. Those parameters relevant for the analysis of written texts include lexical processes, transitivity, syntactical transformations, modality, speech acts, implicature, and personal address.

- *Lexical processes* refer to the vocabulary used in a text. For example, the use of euphemisms and metaphors or the systematic use of certain words and the avoidance of others may give insights into what version of reality a text is intended to present to the reader (Fairclough, 1992; Galański, 2000; Schrøder, 2002).
- *Transitivity* includes the process types contained in verbs and the relations among the participants in these processes (Stubbs, 1996). Verbs carry the main responsibility for representing events and situations in texts and may thus serve to foreground certain aspects or background others (Fowler and Kress, 1979b). For example, verbal processes in passive voice often leave agency, causality and responsibility of an action unclear (e.g. *data are collected* vs. *we collect data*) and it may be a writer's conscious choice to do so (Fairclough, 1992).

- *Syntactical transformations* such as nominalizations or, again, the passive voice may also function to disguise agency. When a verb is transformed into a noun, not only its tense disappears but also the participants are deleted (e.g. *the collection of data* vs. *we collect data*). Similarly, in a passive construction the object becomes the subject position, while the agent of the process is omitted or at least backgrounded (Fowler and Kress, 1979b).
- *Modality* is a means to express the author's evaluations of and attitudes towards people or events. For example, the modal verb "may" expresses possibility and probability (Kreidler, 1998). Negation also deserves attention in linguistic analyses of modality, given that a positive proposition and its negation are two terminal points between which all propositions using modality fall (Fairclough, 1992). Essentially, a negation reverses the truth value of a proposition, just like the mathematical negative (Jordan, 1998). The writer's motivation to do so is to deny expectations in the mind of the reader that stem from contextual circumstances (Wason, 1965). For example, if writers of online privacy policies negate practices their readers might have concerns about – stemming from their knowledge of prior experience – they might ease their readers' presupposition that their privacy is violated.
- *Speech acts* are the communicative functions which utterances are intended to perform. The analysis of speech acts focuses on the roles they assign to readers and writers and the relationships writers seek to establish with their audience (Fowler and Kress, 1979b). For example, rhetorical questions in the first person are mere devices to draw the reader into the discourse by simulating an inner monologue rather than questions that need to be answered (Fowler and Kress, 1979b), e.g. *Do you collect data about me?*
- *Implicature* refers to inferences readers draw from texts when they read between the lines (Fowler, 1985). Inferences are defined as "deductions or guesses based on evidence in the text or derived from a person's preexisting knowledge" (McCabe, 1998, p. 280). Readers typically make correct inferences, though texts may intentionally be misleading to mitigate negative information or deceive readers (Riley, 1993).
- *Personal addresses and references* used in a text may reveal how formal a text is and what kind of relationships it seeks to establish. In particular, the use of the pronouns *we* and *you* in a text may be indicative of such relationships (Fowler, 1985).

The corpus of privacy statements was examined in light of these seven parameters by closely reading all privacy statements multiple times. All words and phrases indicating ideology, hidden meanings or the enactment of power were then subjected to a computer-assisted corpus analysis using *WordSmith Tools* so as to ensure that all instances of these words were considered. To facilitate their interpretation concordances were created. These display search terms in their immediate contexts (cf. McEnery and Wilson, 2001) and help to identify semantic ambiguities such as polysemy (words with multiple meanings) and homography (multiple words sharing the same spelling) (Ide and Véronis, 1998). Further, *WordSmith Tools* was used to identify high-frequency words. These frequency counts were also used to verify *post hoc* whether the findings of the qualitative analysis were valid (cf. Popping, 2000).

Results

This section first presents general textual patterns that appear throughout the privacy statements but are not related to any particular data handling practice. The subsequent three sections focus on communicative strategies companies use to describe their data handling practices pertaining to user identification, unsolicited marketing communications and data sharing, all of which are major privacy concerns among Internet users.

General patterns

Previous research has criticized the complex sentence structure of privacy policies (Antón et al., 2004). This pattern was also found in the policies examined. An extreme example of such a sentence is a 103-word sentence that is next to incomprehensible due to its length and the overuse of the conjunction *or*:

> (1) "In addition to the circumstances described above, Travelocity.com may disclose member information if required to do so by law, court order, as requested by other government *or* law enforcement authority, *or* in the good faith belief that disclosure is otherwise necessary *or* advisable including, without limitation, to protect the rights *or* properties of Travelocity.com *or* Sabre, Inc. *or* when we have reason to believe that disclosing the information is necessary to identify, contact *or* bring legal action against someone who may be causing interference with our rights *or* properties, whether intentionally *or* otherwise, *or* when anyone else could be harmed by such activities." (Travelocity.com) [emphasis added]

Such complicated syntax gives evidence of the legalistic nature of privacy policies, as does the use of legal phrases. The examination of the privacy policies has surfaced a number of phrases in "legalese" that leave readers in the unknown as to whether a certain practice is carried out or will be carried out in the future. For example:

> (2) "This aggregated data will *not* specifically identify you. We *reserve the right* to do so in the future" (uBid.com)

> (3) "Where we believe it to be appropriate (*in our sole discretion*), we will ask our agents *not* to disclose or use your personal information." (Buy.com)

> (4) "we periodically make such information ... available to selected third parties *including but not limited to*, those who trade or rent information for direct marketing purposes." (1–800 flowers)

One cannot safely say whether these statements are just poorly constructed or intended to obscure unethical data handling practices, but they do not give users a straightforward answer as to whether or not a certain practice is carried out, thus preventing informed consent.

A similar pattern found was that of denial of certain practices without users' consent accompanied by clauses pointing to exceptions of when this practice may still occur, which also makes informed consent impossible. These syntactic patterns and hedging words are confusing and may deter readers from reading privacy policies altogether:

> (5) "*Except as otherwise stated* in this Policy, without your consent, buy.com does *not* disclose its customers' Personally Identifiable Information" (Buy.com)

> (6) "The cookies we use do *not* reveal any personal information about you, *except perhaps* your first name" (Apple)

> (7) "without your consent, we do *not* make your ... email addresses available to third parties (*except* for subsidiaries, subcontractors or agents acting on our behalf in compliance with this Privacy Policy)" (1800-flowers)

The corpus of privacy statements also contains a large number of modality markers. The most frequent are: *may* (*n* = 476), *occasional(ly)* (*n* = 29), *might* (*n* = 27), and *from time to time* (*n* = 24). *May* was examined in a concordance to examine the contexts in which it occurs. It turned out that *may* occurs most frequently in connection with the verbs *use* (*n* = 47), *share* (*n* = 32), *collect* (*n* = 24), and *disclose* (*n* = 16). The use of *may* in combination with these verbs makes it impossible for users to judge how often a company engages in these practices. All it tells readers is: "Sometimes we do, sometimes we don't". This suggests that companies use modality strategically to downplay the frequency and probability with which certain data handling practices occur, which at the same time reduces the information value of these propositions.

Nominalizations are another language pattern that was found throughout the corpus. The transformation of verbal processes into nouns makes these processes seem like self-caused actions that happen in unspecified ways (Kress, 1985). Companies use this pattern in connection with data collection, data use, and data sharing to distance themselves from these questionable practices, given that nominalizations make it difficult for readers to determine who collects, uses, and shares data:

(8) "this document only addresses *the use and disclosure* of information we collect from you" (eBay)

(9) "How can I limit *the use and sharing* of personally identifiable information about me?" (Staples)

(10) "What choices are available to users regarding *collection, use and distribution* of the information ..." (Hotels.com)

Another feature found in the privacy statements are headings and subheadings phrased as questions (sometimes labelled FAQs), which are asked from a neutral perspective, from the reader's perspective or from the writer's perspective:

(11) "Who will the information be shared with, if anyone?" (Travelocity.com)

(12) "What information do we gather?" (1800-flowers)

(13) "What Information Do You Gather About Me?" (eToys)

Those questions in the neutral passive voice (11) and those in the first person plural (12) are primarily rhetorical questions used to attract the reader's attention. Meanwhile, those asked from the reader's perspective (13) serve a second purpose. They anticipate users' concerns and ease them by providing rather obvious answers, namely those the reader would like to read. This speech function also assigns roles to the participants in the discourse in that the readers are presented as being concerned about data privacy, while the writer appears forthcoming with information, not abusing his/her power as information provider.

User identification

All 28 companies admit to placing cookies on users' computers to identify returning visitors and collect aggregate user data. Users might object to the idea of cookies when they are made aware of them, i.e. when they read a website's privacy policy. To mitigate the fact that they place cookies, 16 companies emphasize that the cookies they send are very small files. However, the fact that cookies are small does not make the practice of placing them on users' PCs more acceptable. By collocating *cookies* with the qualitative adjective *small*, companies mitigate their own questionable practice, suggesting that cookies are harmless and no cause for concern. Also, companies seek to shift the responsibility for the placement of cookies on to the browser software by stating that the browser stores cookies on computers rather than pointing out that their websites send these cookies to users' computers, as examples (14) to (16) illustrate.

(14) "Cookies are *small* pieces of information that are *stored by your browser* on your computer's hard drive" (Travelocity)

(15) "Cookies are *small* bits of text that *your Web browser software stores* on your computer" (LL Bean)

(16) "A 'cookie' is a *small* file *stored by your web browser* on your computer's hard drive" (JC Penney)

Another means of justifying cookies is appeal to common practice by pointing out that most websites place cookies on users' PCs, suggesting that this is therefore no reason for concern. For example:

(17) "*Like many* websites, the Apple website uses 'cookie' technology"

(18) "*Like most* websites, the Site uses cookies" (Ticket Master)

(19) "Cookies are *routinely used by most, if not all*, E-commerce merchants, including Oce Depot"

Companies use the fact that most websites place cookies as evidence to support this ethically questionable practice. However, the mere fact that placing cookies is a standard data collection method on the Internet does of course not make this practice more acceptable.

Unsolicited marketing communications

Sending promotional offers or e-mail newsletters to registered users is standard practice among all 28 companies. However, they seem to be aware that users dislike unsolicited e-mails and offer opt-out alternatives for at least some of these e-mails. They employ interpersonal language resources to mitigate and enhance the practice of sending unsolicited marketing communications in two ways. First, they convey their attitudes towards this practice by de-emphasizing its frequency with temporal adverbs (*occasionally*) or modals (*may*). Second, they highlight the quality and benefits of unsolicited e-mails to their recipients in order to present themselves as trustworthy partners who do not abuse their power but send their registered users only material they will appreciate. Examples of mitigation and enhancement with interpersonal language resources include:

(20) "Office Depot *occasionally* sends our customers and the users of the Site announcements and updates, which ... *we believe to be of value* to our customers and users."

(21) "Outpost.com sends *occasional* emails to let you know about changes to our site and product specials *we believe will be of interest* to you." (Cyberian Outpost)

(22) "We send the L.L. Bean Email Newsletter ... to subscribers and *occasionally* to other customers who *we think might be interested* in receiving this information."

These examples show that the information conveyed about the frequencies with which users can expect to receive "spam" messages is insufficient for users to consent to receiving such messages.

As mentioned earlier, choices made about verbal process types and participants in these processes can be ideologically significant. When referring to unsolicited e-mails in their privacy policies, companies use verbal process types that call attention to users rather than themselves and address users personally. They achieve this by replacing the process of sending e-mails with the process of receiving e-mails, thereby redirecting the focus to the users (*you*). In some cases the companies still make an appearance in the sentence, in other cases they are removed from the sentence altogether. For example:

(23) "*you will occasionally receive* e-mails notifying you of special promotions" (Expedia)

(24) "From time to time, *you may receive* mail, e-mail or telephone calls *from* QVC"

(25) "As a customer, *you may receive* the following communications *from* the Barnes & Noble.com"

Sharing and selling data

Only 8 of the sample companies admit to sharing user data with third parties while the others only share them if the user has opted in or not opted out. To justify this questionable data handling practice, companies emphasize that the party receiving these data is reliable, and they downplay the frequency and probability of data sharing. For example, in 11 instances the third parties are referred to as *carefully selected, trustworthy, reputable, responsible*, or *carefully screened* to ease users' fears of data misuse. Further, in 6 instances, the use of the modal *may* or temporal adverbs such as *occasionally* or *from time to time* are used to mitigate the fact that data are made available to third parties. Examples include:

(26) "We *may* share information with *carefully selected* vendors" (Amazon)

(27) "Apple *may occasionally* share your personal contact information with *carefully selected* technology companies"

(28) "*From time to time, on limited bases*, we share with *trustworthy* third parties contact information of our registered customers" (Barnes and Noble)

Again, the use of adverbs of frequency does not tell users exactly when and how their data are made available to third parties, which prevents informed consent and mitigates unethical data handling practices.

The use of the passive voice is another linguistic strategy found in privacy statements. It removes the agent from the subject position and foregrounds the object of the sentence instead. Also, the agent is sometimes removed altogether, which obscures responsibility for an action, as no one in particular appears to be responsible for it. This strategy was used in connection with data sharing, as the following examples illustrate:

(29) "who the information *will be shared* with" (Travelocity.com)

(30) "With whom *is* information *shared*?" (BMG Music)

(31) "Your information *may be shared* with agents or contractors" (Dell)

Interestingly, companies sometimes switch to the passive voice when they talk about data sharing, but use the first person in the surrounding text. This suggests that they are careful not to present themselves as the agents of this process in order to distance themselves from the practice of data sharing:

(32) "*We* need your e-mail address. It will never *be shared* with or sold to anyone" (Lands' End)

(33) "we want you to know about the personal information *we* collect, how *we* use that information and with whom it may *be shared*" (BMG)

(34) "Amazon.com knows that you care how information about you *is used and shared*, and *we* appreciate your trust"

The use of negation in connection with data sharing is also a noteworthy feature. When companies claim that they do not share user data they implicitly contest the charge that they do – a response to the ongoing public debate about data privacy on the Internet. The 28 sample companies not only deny sharing data but 17 of them also deny selling and renting data. Companies apparently feel they have to dispel users' fears about their data being sold or rented, otherwise they would not deny doing it. This makes companies that do not mention anything about data selling appear suspicious, given that users cannot be sure whether these companies do not mention data selling in their policies simply because they do not do it or whether they deliberately fail to mention it because they do not want to admit doing it.

Discussion

The four ethical theories explored earlier have deemed data collection without the data providers' informed consent unethical. Although privacy policies would ideally inform readers in a manner that enables them to make an informed decision as to whether or not they want to divulge personal information on a website, the linguistic patterns identified suggest the opposite. They can be categorized into four different strategies (see Table II).

First, companies mitigate the negative effects of certain practices and enhance the qualities of others. For example, they emphasize their positive intentions when they speak of *carefully selected* third parties in connection with data sharing or when they de-emphasize the dangers associated with cookies by collocating *cookies* with *small*. In addition to lexical processes, companies use modality to mitigate and

TABLE II

Communicative strategies in online privacy policies

Communicative strategy	Pattern	Parameter	Textual realization	Examples
Mitigation & enhancement	(De)emphasizing qualities	Lexical processes	Qualitative adjectives	*carefully selected*
	Downplaying frequency	Modality	Temporal adverbs	*occasionally*
Obfuscation of reality	Hedging propositions	Modality	Modal verbs, legalese	*may*
	Obscuring agency	Transformation	Nominalization, passive	*the sharing of*
		Transitivity	Agent-free processes	*you receive*
Relationship building	Switching perspectives	Speech acts	First-person pronouns	*I/my*
	Addressing audiences	Personal address	Second-person pronouns	*you/your*
Persuasive appeals	Appealing to common practice	Implicature	Comparisons	*like most*
	Appealing to fear	Modality	Negative propositions	*not sell*

enhance their data handling practices and to downplay the frequency, probability and intensity with which certain practices occur. For example, when companies use the temporal adverb *occasionally* in connection with a certain data handling practice, they merely express their attitude towards its frequency but convey little information about the frequency itself, as *occasionally* may cover a range of frequencies.

Second, companies seek to obfuscate reality in two ways. They use hedging techniques either in an attempt to use cautious language or to deceive and confuse their readers, for example when they use modal verbs or phrase sentences in "legalese". Such utterances not only indicate a lack of certainty but also reduce speaker commitment to the utterances (cf. Jucker et al., 2003). Moreover, the companies frequently obscure agency, causality and responsibility in connection with data misuse by switching to passive voice (e.g. *is shared*), using nominalizations (e.g. *the sharing of*), and selecting agent-free processes or processes that background the company (e.g. *you receive* rather than *we send*).

Further, since trust is built more easily if there is a certain level of intimacy (Weber and Carter, 1998), companies seek to establish relationships with their readers. They achieve this by addressing their audiences with second-person pronouns (*you/your*) or by switching to the first-person perspective in certain speech acts to draw readers into the discourse and involve them emotionally.

Ultimately, companies use rational and emotional persuasive appeals to construct more credible arguments and convince their audiences that they are trustworthy, reliable and responsible handlers of data. They appeal to common practice when claiming that placing cookies has become standard practice on the Internet, from which readers may infer that cookies are not dangerous. Moreover, companies use appeals to emotion by raising and at the same time dispelling concerns about data misuse when they claim that they do *not* share or sell user data. This fear appeal (cf. Sti, 1994) is intended to raise the companies' credibility and convince readers of the companies' trustworthiness.

Overall, the analysis of communicative strategies in privacy policies has revealed that they contain vague statements, which prevents informed consent on the part of Internet users and may lead to ethical problems if they misinterpret the claims made in these documents. In general, vagueness, which is defined "as an expression which has more than one possible interpretation" (Zhang, 1998, p. 16), occurs for two reasons – lack of information at the time of speaking/writing or a deliberate choice to background certain things and direct the reader's focus to other things instead (Jucker et al., 2003). In the latter case, the grammatical structure of a sentence is an ideologically motivated choice if not a conscious attempt at deception (Fairclough, 1992). Since writers are more powerful than readers in that they have "the power to disguise power" and "the power to constrain content" (Fairclough, 2001, p. 43), they may exercise this power illegitimately in order to serve their own interests (Van Dijk, 1997).

As for the privacy policies examined, companies seem to abuse their power as authors of these policies by using language to construct a biased version of reality. They benefit from obfuscating, mitigating and enhancing data handling practices in that this helps them to obtain data they would not have access to if users were fully informed about data handling practices. The opacity and vagueness contained in these policies precludes people from understanding them in their entirety or may even deter them from reading these documents altogether (cf. Milne and Culnan, 2004), thereby preventing informed consent. However, as this paper has shown earlier, collecting and using information without the owner's informed consent is unethical, irrespective of whether one seeks the "Golden Mean", looks at the universalizability of the act, calculates the maximum utility obtained, or applies the principle of equality.

Web merchants do not seem to abide by these common ethical principles when they communicate their privacy standards. It seems that they still need to learn how to use the power the Internet has bestowed on them in an ethical and respectful way, for example by posting clearly and unequivocally worded privacy policies. It is upon all stakeholders in online privacy to reverse the unequal distribution of power the Internet has brought with it and empower users with knowledge, tools, and legal protection. If Internet merchants are not willing to improve their data handling communication, privacy seal programs could respond by requiring more user-friendly privacy policies before they award privacy seals. Both privacy advocacy groups and policy makers could empower Internet users by educating them about the use of privacy enhancing technologies such as anonymizers, which could mean that less information would be divulged to web merchants. Another way for policy makers to reduce the power of web merchants in data handling would be to pass privacy legislation, as European Union member states have done.

Conclusion

Web merchants wishing to ease users' privacy concerns may use the four communicative strategies identified above as starting points for reconsidering the wording of their policies and enhancing their readability. Future research is needed, however, to explore how people respond to the language patterns identified above and which changes in these patterns would engender most trust. Companies need to be more aware of what effects their linguistic choices have. Clearly, one does not know whether the texts are deliberately designed to allow multiple interpretations or whether the large number of vague utterances simply stems from the legal nature of the texts, but those companies that wish to communicate their data handling practices more effectively need to disambiguate their privacy policies and transform them into more accurate and transparent representations of their data handling practices. Only then will privacy policies enable web merchants to obtain informed consent from Internet users.

Acknowledgements

The author would like to thank two anonymous reviewers for their helpful suggestions on previous versions of this article.

Appendix – Sample companies

1–800-flowers, Amazon, America Online, American Express, Apple Store, Barnes & Noble, BMG Music, Buy.com, Cyberian Outpost, Dell, eBay, eToys, Expedia, Gap, Gateway, Hotels.com, JC Penney, L.L. Bean, Lands' End, Office Depot, Orbitz, Priceline, QVC, Staples, Ticket Master, Travelocity, uBid, Yahoo.

References

Antón, A., et al.: 2004, 'The Lack of Clarity in Financial Privacy Policies and the Need for Standardization', *IEEE Security and Privacy* **2**(2), 36–45.

Beltramini, R. F.: 2003, 'Application of the Unfairness Doctrine to Marketing Communications on the Internet', *Journal of Business Ethics* **42**(4), 393–400.

Bennett, C. J.: 2001, 'Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web', *Ethics and Information Technology* **3**(3), 195–210.

Boutin, P.: 2002, 'Just How Trusty Is TRUSTe?', *Wired*, April 9, http://www.wired.com/news/exec/0,1370,51624,00.html.

Buchholz, R. A.: 1995, *Business Environment and Public Policy Implications for Management* 5(Prentice Hall, Englewood Cliffs).

Cannon, D. A.: 2002, 'The Ethics of Database Marketing', *Information Management Journal* **36**(3), 42–44.

Chen, K. and A. I. Rea: 2004, 'Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques', *The Journal of Computer Information Systems* **44**(4), 85–92.

De George, R. T.: 2000, 'Business Ethics and the Challenge of the Information Age', *Business Ethics Quarterly* **10**(1), 63–72.

Ebenkamp, B.: 2002, 'Brand Keys to Travel Sites: Straighten up and Fly Right', *Brandweek* **43**(25), 19.

Faden, R. R. and T.L. Beauchamp: 1986, *A History and Theory of Informed Consent* (Oxford University Press, New York).

Fairclough, N.: 1992, *Discourse and Social Change* (Polity Press, Cambridge).

Fairclough, N.: 2001, *Language and Power* 2nd edition (Longman, London).

Federal Trade Commission: 2000, *Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress*, http://www.ftc.gov/reports/privacy2000/privacy 2000.pdf.

Forrester Research: US eCommerce – The Next Five Years, *M2 Presswire*, 29 August 2002.

Fowler, R. and G. Kress: 1979a, 'Rules and Regulations', in R. Fowler et al. (eds), *Language and Control* (Routledge, London), pp. 26–45.

Fowler, R. and G. Kress: 1979b, 'Critical Linguistics', in R. Fowler et al. (ed.), *Language and Control* (Routledge, London), pp. 185–213.

Fowler, R.: 1985, 'Power', in T. Dijkvan (ed.), *Handbook of Discourse Analysis* 4 (Academic Press, London), pp. 61–82.

Foxman, E. R. and P. Kilcoyne: 1993, 'Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues', *Journal of Public Policy and Marketing* **12**(1), 106–119.

Fried, C.: 1968, 'Privacy', *Yale Law Journal* **77**, 475–493.

Galański, D.: 2000, *The Language of Deception A Discourse Analytical Study* (Sage, Thousand Oaks).

Goodwin, C.: 1991, 'Privacy: Recognition of a Consumer Right', *Journal of Public Policy and Marketing* **10**(1), 149–166.

Halliday, M. A. K.: 1978, *Language as Social Semiotic: The Social Interpretation of Language and Meaning* (Arnold, London).

Han, P. and A. Maclaurin: 2002, 'Do Consumers Really Care About Online Privacy?', *Marketing Management* **11**(1), 35–38.

Hodge, R. and G. Kress: 1993, *Language as Ideology,* 2nd edition (Routledge, London).

Hoffman, D. L., T. P. Novak and M. Peralta: 1999, 'Building Consumer Trust Online', *Communications of the ACM* **42**(4), 80–85.

Hoffman, L.: 1980, *Computers and Privacy in the Next Decade* (Academic Press, New York).

Ide, N. and J. Véronis: 1998, 'Word Sense Disambiguation: The State of the Art', *Computational Linguistics* **24**(1), 1–40.

Introna, L. D. and A. Pouloudi: 1999, 'Privacy in the Information Age: Stakeholders, Interests and Values', *Journal of Business Ethics* **22**(1), 27–38.

Jones, S., M. Wilikens, P. Morris and M. Masera: 2000, 'Trust Requirements in E-Business', *Communications of the ACM* **43**(12), 80–87.

Jordan, M. P.: 1998, 'The Power of Negation in English: Text, Context and Relevance', *Journal of Pragmatics* **29**(6), 705–752.

Jucker, A. H., S. W. Smith and T. Lüdge: 2003, 'Interactive Aspects of Vagueness in Conversation', *Journal of Pragmatics* **35**(12), 1737–1769.

Kelly, E. P. and H. C. Rowland: 2000, 'Ethical and Online Privacy Issues in Electronic Commerce', *Business Horizons* **43**(3), 3–12.

Koehn, D.: 2003, 'The Nature of and Conditions for Online Trust', *Journal of Business Ethics* **43**(1–2), 3 –19.

Kreidler, C. W.: 1998, *Introducing English Semantics* (Routledge, London).

Kress, G.: 1985, 'Ideological Structures in Discourse', in T. Dijk van (ed.), *Handbook of Discourse Analysis, vol* 4 (Academic Press, London), pp. 27–42.

Liu, C. and K. P. Arnett: 2002, 'Raising a Red Flag on Global WWW Privacy Policies', *The Journal of Computer Information Systems* **43**(1), 117–127.

Liu, C., J. T. Marchewka, J. Lu and C.-S. Yu: 2004, 'Beyond Concern: A Privacy-Trust-Behavioral Intention Model of Electronic Commerce', *Information and Management* **42**(1), 127–142.

Mascarenhas, O. A. J., R. Kesavan and M. D. Bernacchi: 2003, 'Co-Managing Online Privacy: A Call for Joint Ownership', *Journal of Consumer Marketing* **20**(7), 686–702.

Mason, R. O.: 1995, 'Applying Ethics to Information Technology Issues', *Communications of the ACM* **38**(12), 55–57.

Mason, R. O., F. M. Mason and M. J. Culnan: 1995, *Ethics of Information Management* (Sage, Thousand Oaks).

McCabe, A.: 1998, 'Sentences Combined: Text and Discourse', in J. B. Gleason and N. B. Ratner (ed.), *Psycholinguistics* 2nd edition, (Harcourt Brace, Fort Worth, TX), pp. 275–308.

McCullagh, D.: 1999, Is TRUSTe Trustworthy?, *Wired*, November 5, http://www.wired.com/news/politics/0,1283,32329,00.html.

McEnery, T. and A. Wilson: 2001, *Corpus Linguistics* 2nd edition (Edinburgh University Press, Edinburgh).

Metzger, M.: 2004, 'Privacy, Trust and Disclosure: Exploring Barriers to Electronic Commerce', *Journal of Computer-Mediated Communication* **9**(4), http://www.ascusc.org/jcmc/vol9/issue4/metzger.html.

Metzger, M. J. and S. Docter: 2003, 'Public Opinion and Policy Initiatives for Online Privacy Protection', *Journal of Broadcasting and Electronic Media* **47**(3), 350–374.

Milne, G. R. and M. J. Culnan: 2004, 'Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Dont Read) Online Privacy Notices', *Journal of Interactive Marketing* **18**(3), 15–29.

Miyazaki, A. D. and A. Fernandez: 2000, 'Internet Privacy and Security: An Examination of Online Retailer Disclosures', *Journal of Public Policy and Marketing* **19**(1), 54–61.

Nyshadham, E. A.: 2000, 'Privacy Policies of Air Travel Web Sites: A Survey and Analysis', *Journal of Air Transport Management* **6**(2), 143–152.

Olivero, N. and P. Lunt: 2004, 'Privacy versus Willingness to Disclose in E-Commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control', *Journal of Economic Psychology* **25**(2), 243–262.

Oz, E.: 2004, 'Ethical Issues', in J. F. George (ed.), *Computers in Society. Privacy, Ethics, and the Internet* (Pearson, Upper Saddle River), pp. 284–295.

Palmer, J. W., J. P. Bailey and S. Faraj: 2000, 'The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements', *Journal of Computer-Mediated Communication* **5**(3), http://www.ascusc.org/jcmc/vol5/issue3/palmer.html.

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

Pollach, I.: 2004, 'Online Privacy Statements – Are They Worth Reading?', in M. Khosrow-Pour (ed.), *Innovations Through Information Technology* (Idea Publishing, Hershey), pp. 217–220.

Popping, R.: 2000, *Computer-Assisted Text Analysis* (Sage, London).

Prosser, W.: 1960, 'Privacy', *California Law Review* **48**(3), 383–423.

Rachels, J.: 1975, 'Why Privacy is Important', *Philosophy and Public Affairs* **4**(4), 323–333.

Reda, S.: 2000, 'VeriFone and Russel Reynolds Associates Top 100 Internet Retailers', *Stores*, https://www.stores.org/archives/00top100int_1.asp.

Rennhard, M., et al.: 2004, 'Towards Pseudonymous E-Commerce', *Electronic Commerce Research* **4**(1–2), 83–111.

Riley, K.: 1993, 'Telling More than the Truth: Implicature, Speech Acts, and Ethics in Professional Communication', *Journal of Business Ethics* **12**(3), 179–196.

Ryker, R., et al.: 2002, 'Online Privacy Policies: An Assessment of the Fortune E-50', *The Journal of Computer Information Systems* **42**(4), 15–20.

Saban, K. A., E. McGivern and J. N. Saykiewicz: 2002, 'A Critical Look at the Impact of Cybercrime on Consumer Internet Behavior', *Journal of Marketing Theory and Practice* **10**(2), 29–37.

Sakkis, G., et al.: 2003, 'A Memory-Based Approach to Anti-Spam Filtering for Mailing Lists', *Information Retrieval* **6**(1), 49–73.

Samoriski, J. H.: 1999, 'Unsolicited Commercial E-Mail, the Internet and the First Amendment: Another Free Speech Showdown in Cyberspace?', *Journal of Broadcasting and Electronic Media* **43**(4), 670–689.

Schrøder, K. C.: 2002, 'Discourses of Fact', in K. B. Jensen (ed.), *A Handbook of Media and Communication Research* (Routledge, London), pp. 98–116.

Schwartz, J.: 2001, Seeking Privacy Online, Even as Security Tightens, *New York Times*, November 11, 3.10.

Shapiro, B. and C. R. Baker: 2001, 'Information Technology and the Social Construction of Information Privacy', *Journal of Accounting and Public Policy* **20**(4–5), 295–322.

Smith, A. D. and W. T. Rupp: 2004, 'Online Privacy Policies and Diffusion Theory Perspectives: Security or Chaos?', *Services Marketing Quarterly* **25**(3), 53–75.

Stahl, B. C.: 2004, 'Responsibility for Information Assurance and Privacy: A Problem of Individual Ethics?', *Journal of Organizational and End User Computing* **16**(3), 59–77.

Stead, B. A. and J. Gilbert: 2001, 'Ethical Issues in Electronic Commerce', *Journal of Business Ethics* **34**(2), 75–85.

Stiff, J. B.: 1994, *Persuasive Communication* (Guilford, New York).

Stubbs, M.: 1996, *Text and Corpus Analysis Computer-Assisted Studies of Language and Culture* (Blackwell, Oxford).

Van Dijk, T. A.: 1997, 'Discourse as Interaction in Society', in T. A. Dijk Van (ed.), *Discourse as Social Interaction, vol* 2 (Sage, London), pp. 1–37.

Van Wel, L. and L. Royakkers: 2004, 'Ethical Issues in Web Data Mining', *Ethics and Information Technology* **6**(2), 129–140.

Velasquez, M. G.: 2002, *Business Ethics Concepts and Cases* 5th editions (Prentice Hall, Upper Saddle River).

Warren, S. and L. Brandeis: 1890, 'The Right of Privacy', *Harvard Law Review* **4**(5), 193–220.

Wason, P. C.: 1965, 'The Contexts of Plausible Denial', *Journal of Verbal Learning and Verbal Behavior* **4**, 7–11.

Weber, L. R. and A. Carter: 1998, 'On Constructing Trust: Temporality, Self-Disclosure, and Perspective-Taking', *The International Journal of Sociology and Social Policy* **18**(1), 7–26.

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

Zhang, Q.: 1998, 'Fuzziness – Vagueness – Generality – Ambiguity', *Journal of Pragmatics* **29**(1), 13–31.

Irene Pollach,
Department of English Business Communication,
Vienna University of Economics and Business Administration,
Nordbergstrasse 15, A-1090, Vienna, Austria, EU.
E-mail: irene.pollach@wu-wien.ac.at