Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies

Jan Fernback and Zizi Papacharissi

New Media Society 2007; 9; 715
DOI: 10.1177/1461444807080336

new media & society

Los Angeles, London, New Delhi and Singapore
Vol9(5):715–734 [DOI: 10.1177/1461444807080336]

ARTICLE

Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies

JAN FERNBACK
Temple University, USA

ZIZI PAPACHARISSI
Temple University, USA

Abstract

Several surveys attest to growing public concerns regarding privacy, aggravated by the diffusion of information technologies. A policy of self-regulation that allows individual companies to implement self-designed privacy statements is prevalent in the United States. These statements rarely provide specific privacy guarantees that personal information will be kept confidential. This study provides a discourse analysis of such privacy statements to determine their overall efficacy as a policy measure. The in-depth analysis of privacy statements revealed that they offer little protection to the consumer, instead serving to authorize business practices which allow companies to profit from consumer data. Using public good theory as a foundation, policy implications are discussed.

Key words

internet • privacy • regulation

Public discussion on the cultural impact of technology frequently addresses online misuses of private information. The Pew Internet & American Life Project revealed that 70 percent of internet users support new laws to

protect consumer privacy online (Fox and Lewis, 2001), in response to advanced data-mining technologies which transform personal data into a tradable commodity in capitalist societies (Hamelink, 2000). Although several European Union (EU) Member States have responded to such concerns by devising distinct regulations that protect consumer privacy, the USA has encouraged a privacy policy of self-regulation; thus, individual companies develop formulas for ensuring customer privacy online. Framed as self-devised protective measures, these online privacy statements seldom provide explicit reassurance that consumer information will be kept confidential and will not be exploited. This study examines online privacy and investigates how consumer information is protected or exposed by online portal sites. Building on a content analysis (Papacharissi and Fernback, 2002), which found that privacy statements are more often legal safeguards for companies rather than protectors of customer interests, this textual analysis supplements these findings. Whether or not consumers read these statements, they provide evidence of the internet industry's self-protective efforts at the expense of consumer privacy. This study uses public good theory to connect online privacy with specific policy recommendations following the analysis.

Voluntarily posted privacy statements often outline how companies intend to use customer information so that, in the event of consumer complaints, the companies are absolved of responsibility, thus offering compromised protection to the individual consumer (Kandra, 2001). Web users often have little faith in privacy policies as instruments of protection (Reagle and Cranor, 1999). Companies such as Microsoft Passport Services have exploited consumer information, and were pressured into revising their privacy policies and statements following a series of articles originating from Salon.com (www.salon.com). Both Yahoo and Microsoft email services reportedly divulged customer information in opposition to their stated privacy policies not to share personally identifiable information (Gillis, 2002). On a global level, a loosely-defined regulatory approach to privacy protection contradicts the policies of other countries occupying commercial online space and could lead to potential conflict. Hence, this discourse analysis of privacy statements provides in-depth analysis of privacy statement content and examines how portals use statements to guarantee personal information privacy and/or legally protect themselves. Because this is ultimately a policy question, discourse analysis allows the detailed examination of language, both legal and technical, in these statements.

THE PUBLIC AND ONLINE PRIVACY

Western nations value privacy as a basic human right – the 'right to be let alone', as noted by Warren and Brandeis' (1890) *Harvard Law Review* article. Since then, US and European courts have expanded privacy rights to include citizens' entitlements to control information about themselves. While these rights do not rise to the level of recognized legal privilege (such as doctor–patient), they are

recognized in common and statutory law in the USA. For example, Title 47 of the Code of Federal Regulations, section 64.2005 requires telephone companies to get customer permission to use or disclose personal information collected while providing services. Illegally intercepted electronic communications may not be disclosed according to Title 18, section 2511 of the US code. The US Electronic Communications Privacy Act of 1986, which prohibits unauthorized access to user files online, was enacted to protect data privacy in light of computer technology advancements. These laws demonstrate that going online does not constitute a waiver to individual privacy. Thus, judicial as well as legislative developments express an expectation of privacy when personal information is shared through a communication device.

These guarantees recognize that the release of private information can lead to discriminatory practices which, for example, preclude citizens from obtaining insurance or a mortgage loan in a form of redlining. The mishandling of private information can lead to identity theft or a misrepresentation of consumers' financial, credit, medical or criminal information. However, from a legal perspective, private information gathered by online businesses (e.g. portals) is unprotected by privacy legislation in the USA. This information is as valuable in the marketplace as, for example, long-distance telephone records, but those records cannot be collected and sold by long distance companies under penalty of Law. Therefore, consumers are not granted sufficient right to control information about their online activities under the current regulatory structure. The lack of privacy protections for personal data gathered online demonstrates an inconsistency with other legal protections offered to individuals in cyberspace; for example, 'cyberthreats' are the legal equivalent of physical threats (*Planned Parenthood* v. *ACLA*, 1999, 41 F.Supp 2d 1130, D. Or. (1999)); and federal anti-spam laws protect consumers from junk email.

Given the profitable trade in personal data, the lack of codified legal protections for this information is anachronistic and provides opportunity for misuse. The Pew Internet & American Life Project (Fox, 2000; Fox and Lewis, 2001) reveals that consumer trust is a vital issue for web users who, although concerned about online privacy violations, still disclose personally identifiable and non-identifiable information online. Of online users, 86 percent prefer 'opt-in' policies, which require websites to ask for permission before collecting or using personal data. However, many users do not possess the technological proficiency required to employ privacy protective methods. For example, only ten percent of internet users modify browser settings to reject cookies; five percent employ anonymizing software to conceal their computer identity; and 24 percent provide false personal data to avoid revealing true information. As a result, individuals have become cautious of disclosing personal information online (Fox, 2000; Fox and Lewis, 2001). Courts have acknowledged that privacy protections must be revisited with growing use of intrusive technologies, such as

heat seeking surveillance (*Kyllo* v. *United States*, 533 U.S. 27 (2000)). Individuals may inspect their own medical and governmental records, and susceptible personal information is safeguarded from unauthorized release (under the Video Privacy Protection Act of 1988). Even discarded garbage is afforded privacy protection (*California* v. *Greenwood*, 486 U.S. 35 (1988)). Thus the legal protections granted to personally identifiable information are well established. But a potential exists for the misuse of personal data obtained online which is virtually unpunishable. A right without a legal remedy is an illusory right.

Since the burden for securing privacy online is placed on the public, individuals frequently regard the presence of a privacy statement as an indicator of online vendor integrity. Miyazaki and Fernandez (2000) found that consumers are more likely to purchase items from web retailers whose privacy and security statements are present, but only 23.1 percent of retail websites reported customer identification practices. In a survey of online consumers about attitudes toward Federal Trade Commission principles for online privacy, Sheehan and Hoy (2000) found that consumer value of privacy is contextual – that certain types of information are submitted more readily to online retailers – while more valued information can be obtained by websites that are willing to provide something in exchange (e.g. contest entries). Princeton Research Survey Associates (2002) found that more than 75 percent of web users want definitive, accurate privacy policy information on e-commerce sites. Despite this climate of demonstrated willingness to engage in online transactions, Miyazaki and Fernandez (2001) argued that the continued acquisition of consumer data would hurt online retail sales eventually, due to perceived privacy infringements.

Reilly (1999) suggested that policymakers can address both consumer and e-tailer needs by restricting data collection techniques minimally to assert the empowering potential of online technologies to gather and protect information. Nevertheless, blocking or refusing personal information to a retailer frequently renders a website useless to the consumer. Indeed, Elgesem (1996) emphasized the growing assumption of risk undertaken by consumers: users must reveal information in exchange for convenience and access, even though fair practice entails that the costs of relinquishing individual privacy balance the service received in return. In response, McKenna (2001) recommended complete user control enabled with an opt-in device, permitting consumers to choose to visit or abandon sites with suspect data-collection policies (McKenna, 2001). Were this scenario to be implemented, e-tailers might find increased operation costs, since the loss of profiled consumer information would curtail web businesses' abilities to exploit it for marketing purposes (Farah and Higby, 2001). E-commerce sites would be forced to contend with rising marketing expenses in exchange for less streamlined marketing practices. Several businesses are concerned that restrictive privacy mechanisms will eliminate free and high-quality service for web customers (Farah and Higby, 2001).

Research highlights the contradictions present in maintaining a legal regime of self-regulation while maintaining profitability for online businesses and protecting consumer privacy. While previous research studied the legal complexities of providing such protection, this article focuses on the text of the privacy statement itself, examining the language through which online portals seek to guarantee privacy protection. Consumers expect legal protection of sensitive medical or financial information, but they do not necessarily extend those expectations of privacy to information collected about them by portal websites. Privacy statements, crafted by staff attorneys, are written to coincide with business models so that firms may maximize the ability to profit from information that they capture. Therefore, this study examines the substance of privacy statements as marketing tools, not as risk-management tools. It finds that, although the term, 'privacy statement' primes the user for a guarantee of privacy protection (since they are not 'disclosure statements'), the vocabulary of the statement itself rarely offers explicit privacy protection. Indeed, these statements are marketed to consumers using the rhetoric of protection in the form of assurances from the approved TRUSTe privacy stamp and in language that the online entity is 'committed to protecting your privacy' (e.g. http://privacy.msn.com). Privacy statements generally serve two major purposes: to mollify consumers wary of conducting transactions online for fear of privacy violations; and to convince regulators that further legislative initiatives to guarantee consumer privacy are unnecessary, since the industry self-policing efforts sufficiently protect citizen rights. If these statements were offered solely as legal protective devices, the statements would be brief and direct (e.g. 'we accept no liability'). But since the statements assure the reader that they are 'committed to protecting privacy', they are clearly written to go beyond mere legal protection. In the following section, we discuss the legal issues surrounding such privacy pledges.

PRIVACY REGULATION AND THE LEGAL LIMITATIONS OF PRIVACY STATEMENTS

The privacy statement formula follows in the tradition of self-regulation prevalent in the USA, which is founded on a lack of government involvement in regulating consumer privacy (with the exception of the Children's Online Privacy Protection Act of 1998 (COPPA)). The adequacy of privacy statements as protective measures is arguable; attorneys frequently draft online privacy statements to include catch-all stipulations that permit flexibility regarding uses of consumer information (Fausett, 2001). Although numerous consumer privacy bills (including the Online Personal Privacy Act and the Consumer Privacy Protection Act) are now before Congress, the USA remains the only major trading nation which has not adopted comprehensive privacy protection legislation.

In contrast, European Union member countries follow strict regulations that protect consumer privacy, specified by the Directive on Data Protection of 1998. This privacy directive safeguards individual control over consumer data and requires that foreign trading partners adhere to the same level of equal protection (Lee, 2000). The transmission of personal information from EU member countries to outside countries without adequate privacy protection is prohibited, but the EU has nonetheless established contractual agreements with US companies to conduct business despite the disparity in privacy approaches (Lee, 2000). Such business agreements prioritize legal protection over fair information practices, leaving the consumer exposed to personal information misuses.

In the USA, cyberlaw efforts are undertaken primarily by educational institutions and non-profit organizations, including the Stanford Center for Internet and Society. Lessig (1999) contends that in the present data-mining and monitoring environment, the responsibility to establish innocence and/or independence lies with the monitored individual. The problem is aggravated with the accumulation of data, which transform a consumer's life into an ever-expanding record that can be accessed at any time. A US Federal Trade Commission report (1998) confirmed scholarly, activist and public privacy concerns in findings that few websites meet the Federal Trade Commission-suggested privacy criteria of notice, access, security and third-party disclosure. A Federal Trade Commission (2000) follow-up study revealed that only 20 percent of randomly selected websites had implemented its suggested four fair information practices – principles of notice (of information collection practices); choice (regarding how personal data is used); access (to one's own collected information); and security (of collected information) – further cementing charges that industry self-regulatory efforts have not protected consumers adequately.

Additional studies document dominant trends in the privacy policies of companies. Graber et al. (2002) examined privacy statements posted on health websites, and found that one-third of the sample surveyed did not feature a privacy statement. They noted that featured privacy statements required an education level of two years of college to comprehend, while most websites had a policy that was not comprehensible by most English-language speakers in the USA. Another content analysis of Fortune E-50 companies examined the extent to which privacy statements were posted and were compliant with fair information practice standards as recognized by US government agencies (Ryker et al., 2002). The researchers found that only three out of the 15 business-to-business companies posted privacy statements, all of which failed to comply with fair information practices. The remaining business-to-consumer companies featured privacy statements, one-third of which failed to comply with one or more fair information practices. A comparative panel

analysis of privacy protection trends over time revealed that commercial websites are collecting less personal information than before and becoming more fair information practice compliant, while the penetration rate of privacy seal programs grows at a slower rate (Adkinson et al., 2002).

Cumulative evidence has thus forced the Federal Trade Commission to request that Congress enact legislation designed to protect consumer privacy online. The Financial Modernization Act (Gramm-Leach-Bliley Act) of 1999 specifies that financial institutions must inform customers about their privacy practices, even though the law provides limited control to consumers regarding the use and distribution of personal data (see Privacy Rights Clearinghouse; http://www.privacyrights.org). According to this Act, consumers are granted minimal privacy protection and are still required to take the initiative in ensuring that their personal information is not made available to third parties, in direct contrast to the virtual absence of any legal restraints on corporations regarding the collection and selling of private information. Still, COPPA presents one attempt at limiting corporate information-mining practices with some success. The Act lays out specific regulations for online businesses targeting children or with knowledge of collection of information from children under 13 (Cannon, 2001). The principles defined by this Act, in conjunction with the guidelines outlined by the EU Directive on Data Protection 1998 (which safeguards individual control over consumer data) could serve as the template from which privacy protection is sketched out legally in the USA.

Aside from COPPA, regulatory policy in the USA acknowledges that web operators should be responsible for the disclosure of information-gathering, use and protection practices. TRUSTe is a non-profit, privacy-stamp program, spun from federal efforts to help the internet industry to institute its own privacy guidelines. Websites displaying TRUSTe approval signals to users that data-gathering and dissemination practices will be divulged and are guaranteed by a third party (Benassi, 1999). This endorsement typically certifies that privacy policies are presented in plain language and are prominently displayed on a website. The TRUSTe logo may confuse unsophisticated users, who may see the stamp as a guarantee of their privacy rather than a fair disclosure of that site's information retrieval and use policies. Indeed, a content analysis of privacy statements revealed that even TRUSTe-certified websites do not abstain from collecting personally identifiable and/or non-identifiable data; they simply disclose this practice in their privacy statements (Papacharissi and Fernback, 2002). Fulfillment of TRUSTe requirements is voluntary, and sites that break policy have no specific retribution to fear, other than harmful publicity.

Additional industry coalitions have formed in response to consumer concerns. For example, the Online Privacy Alliance, a group of 50 online companies devoted to advancing consumer data security, provides its own seal of approval to companies that follow its recommended privacy policies

(Lee, 2000). The Association of Accredited Advertising Agencies also cultivates consumer privacy rights in its recommendations for marketers, and several analysts find that a few online businesses are restricting the sale of consumer lists, limiting monitoring and discontinuing spam email in response to such independently led advocacy efforts (Lee, 2000). However, it is apparent that these efforts shift the focus of this debate from organizational responsibility to individual technological know-how and assert, inadvertently, the legal capability to collect and use personally identifiable and non-identifiable data. In response to public concern and confusion over the efficacy of privacy statements, this article undertakes a discourse analysis to investigate the legal inadequacies of privacy statements and make recommendations for revision.

METHOD

This research examines online privacy statements to ascertain how much data protection they offer. A discourse analysis of privacy statements provides in-depth analysis of privacy statement content and examines how portals use statements to guarantee personal information privacy and/or legally protect themselves. Because this is ultimately a policy question, discourse analysis allows the detailed examination of language in these statements to determine how the themes of consumer privacy protection and legal protection for the company are presented, integrated or separated to reassure consumers. Qualitative textual analysis techniques (following Fairclough, 1995, 2000; van Dijk, 1997) seek a deep explanation of meaning through the observation and interpretation of patterns displayed in a mediated text (web privacy statements in this study). Textual discourse analysis lends an empirical grounding to the abstract observations about the social character of language and its cultural functions offered by social theory (Fairclough, 2000). In this particular analysis, the privacy statement is examined as a rhetorical device designed to inform the consumer about privacy practices and simultaneously safeguard the legal integrity of the company. We consider how these themes are articulated through information protection pledges throughout the text, and the extent to which they contradict or complement each other.

A sample of web portals was chosen from a content analysis of privacy statements conducted by Papacharissi and Fernback (2002), with privacy statements as the units of analysis. Portal sites were selected for analysis because they are frequently trafficked and attract users with differing levels of technological ability and diverse interests. For the purpose of this study, portals were defined as 'directories of general information' and using the aforementioned criteria of popularity and representativeness of audience, the following portals were focused on: MSN (www.msn.com); Google (www.google.com); Real.com (www.real.com); and Kazaa (www.kazaa.com). These sites were selected because they function as

portals of information while at the same time offer a wide array of services, thus attracting a demographically diverse population. MSN is news-oriented, Google is search-oriented, Real is entertainment-oriented and Kazaa focuses on information exchange. As such, they represent the various information transactions that transpire online and provide a comprehensive reflection of the legal and fiscal concerns of online businesses. Moreover, they provide an inclusive overview of typical user surfing behavior. The purpose of the discourse analysis is to provide in-depth understanding of a phenomenon; therefore, this sample does not purport to be statistically representative. Nevertheless, it includes sites which not only offer popular services online, but also require personal information and customization to function effectively for the user. Analysis of this sample helps to illuminate the mode by which actual users might interact with and interpret the text of these privacy statements. Qualitative analysis tackles smaller samples to understand communication processes in detail. This analysis does not seek to generalize findings to the general population.

It takes on privacy statements, a tool constructed to explain privacy protection practices to consumers, and analyzes whether and how this goal is fulfilled in this text. The privacy statement is seen as a rhetorical device, which maps out the basis of the business – consumer relationship.

This work examines discourse (as defined by Fairclough, 1995 and Wood and Kroger, 2000) as a text. Wood and Kroger define discourse as 'all spoken and written forms of language use (talk and text) as social practice' (2000: 19). Thus, the aim of discourse analysis is to clarify the 'systematic links between texts, discourse practices, and sociocultural practices' (Fairclough, 1995: 17). For the purposes of this research, discourse encompassed written language in the text of the privacy sections in the sample of websites. Words, syntactical characteristics and text structures that illuminate the commonly understood meaning of the privacy statements were analyzed. The focus was the relation between two themes within the online text: consumer protection and legal safeguards for the web company. The following questions were asked: first, how does the web company assure the consumer of privacy protection practices? Second, how is the consumer positioned toward the privacy statement, portal use and the web company? In response to these questions, the study examines how personal data are purported to be used and protected by the company, analyzes the comprehensibility of language to ordinary internet users, and draws attention to inaccuracies or conflicting statements as indicators of overall statement trustworthiness. The privacy statement is systematically analyzed and thematically coded as a rhetorical device designed to establish the terms of the consumer – company relationship. Focusing on the use of language helps to understand the process through which private information is compromised under the guise of offering personalized and improved services. For the purposes of clarity, the analysis is presented by portal, with each theme addressed accordingly.

ANALYSIS OF PORTAL PRIVACY STATEMENTS

Microsoft networks (MSN)

The Microsoft Networks privacy statement (http://privacy.msn.com) begins by pledging that 'MSN is committed to protecting your privacy', reassuring the consumer of privacy protection by providing explanations of how personal information will be used and by using language that positions the reader as a consumer who can trust MSN with privacy issues. In doing so, the MSN statement draws upon computer and legal discourses which assume that the reader is computer-literate and legally astute. Therefore, explanations of data-collection practices frequently are not detailed or clear enough for the average user.

For example, the statement 'When we transmit highly confidential information (such as a credit card number) over the internet, we protect it through the use of encryption, such as the Secure Socket Layer (SSL) protocol', neglects to define encryption and provides an example of an encryption program as a rhetorical dismissal of potential reader ignorance. This device may be used, in conjunction with early reassurances, to play upon the reader's established sense of security that first, MSN can be trusted to protect privacy, and second, that readers, based upon their position as an informed and protected consumer, will not question any language that is incomprehensible. For example, the following excerpt fails to define clearly the relationship between cookies and privacy:

> MSN uses 'cookies' to help you personalize your online experience. A cookie is a text file that is placed on your hard disk by a Web page server. Cookies cannot be used to run programs or deliver viruses to your computer . . . One of the primary purposes of cookies is to provide a convenience feature to save you time . . . This simplifies the process of recording your personal information . . . If you choose to decline cookies, you may not be able to fully experience the interactive features of the MSN services.

Users must link to the MSN Personal Information Center at http://privacy.msn.com/profilemgmt/ and then to the Cookie FAQ site at http://privacy.msn.com/profilemgmt/cookiesFAQ.asp for a more detailed explanation of cookies, how they may be deleted and the consequences of deleting them. The discourse about cookies is framed in terms of convenience to the user; deleting them will result in a less streamlined, less personal and less productive MSN web experience. This statement also serves, rhetorically, to comfort the user that cookies are not dangerous (i.e. they do not deliver viruses), although they are used to monitor consumer online activity (Lipschultz, 2001). Whatever privacy concerns might be raised by the notion that monitoring devices are placed on the user's computer are mollified discursively by the emphasis on convenience. Thus the consumer is positioned to make a choice between privacy and convenience.

The text of the MSN privacy statement contains a section entitled 'Control Your Personal Information', which speaks to that facet of privacy law addressing the right to control information about oneself. Users are informed of 'choices for the collection, use and sharing of personal information', but they must link to another site to see these policies and obtain a MSN Passport account before viewing, editing or deleting any personal information. This rhetoric functions to empower the consumer, but the intricate procedures to control personal data may deter consumers from pursuing this option. As MSN describes its data collection and use policies:

> MSN collects personal information, such as your email address, name, home or work address or telephone number. MSN may also collect demographic information, such as your ZIP code, age, gender, preferences, interests and favorites. Information collected by MSN may be combined with information obtained from other Microsoft services and other companies . . . MSN does not sell, rent or lease its customer lists to third parties . . . We will only provide those companies with the personal information they need to deliver the service. They are required to maintain the confidentiality of your information and are prohibited from using that information for any other purpose.

This language is straightforward in describing the information that MSN collects, but the discourse describing information use is broad. Information about individual consumers is collected and 'may be combined' with information obtained elsewhere, and thus MSN may construct profiles of individual users. MSN does not 'sell customer lists' to third parties, but does business with third parties in common, numerous ways. Readers are neither told how many third parties MSN transacts with, nor what the nature of those third parties may be. MSN provides only necessary information, but the consumer is not informed of what constitutes that essential information. Those third parties are 'required to maintain confidentiality', but the consumer is not told how this is done. The reader is placated by earlier assurances that MSN will guarantee privacy rights, but these vague statements about information use beg further interrogation by skeptical readers.

Thus, readers are positioned as consumers not unduly concerned with maintaining privacy online – otherwise data use policies and legal and computer terms would be explained in detail, and users would be informed of the full ramifications of MSN privacy practices. Linguistically, the MSN privacy statement constructs 'privacy' in benign terms. Learning about online privacy is the responsibility of the online consumer; the MSN statement may raise more questions than it answers. The exclusion of important data collection or use practices indicates that MSN is maximizing its own protection against the possibility of federal privacy regulation. This exclusion, combined with rhetorical devices which

construct the consumer as willing to relinquish privacy for convenience and the free flow of information, serves to position MSN as an untrustworthy advocate of consumer privacy.

Real networks

The Real Networks privacy statement (http://www.realnetworks.com/company/privacy) begins with assurances that 'Real Networks highly values our customer relationships and we want to make sure that you understand the details of how our products and services utilize the information you provide to us'. The text contains admissions that Real Networks collects specific personal information, assurances that Real 'does not create individual user profiles based on specific content accessed via our products', and an explanation of how Real uses personal information to provide better services for the consumer.

The statement avoids complex legal terms, never making a distinction between personally identifiable and non-identifiable information using this specific wording, despite the centrality of this distinction in the privacy debate. Computer monitoring utilities are introduced and explained with seeming clarity. However, these explanations highlight how information is collected to personalize services to the user more effectively, neglecting to inform the reader how the same information also might be useful to the company. For example, the explanation of cookies assures the reader that 'cookies store these small pieces of data on your machine so we may tailor your experience using our products and visiting our websites'. The text implies that it is acceptable to collect such information, because it is used only to better the services offered to the user; it emphasizes the benefits of information-collection to the user over potential value to the company. The reports on information collected serve to reinforce the reader's established sense of security, inviting the reader to trust that a company so open about its collection practices could not engage in privacy-violating behavior. These explanations avoid the term 'privacy'.

Additional explanations of information practices further sustain this veneer of sincerity by presenting these utilities as incapable of privacy violations. The company assures the user that information collected is only used in an aggregate manner. The text positions the reader as aware of the multilayered meanings of aggregate use. Furthermore, discussing aggregate use would involve visiting the distinction between personally identifiable and non-identifiable data, which the text does not engage. However, the admittance to collecting internet protocol (IP) addresses challenges the consistent claims of aggregate use, because an IP address is the equivalent of an online name tag. It also provides a way of tracing online behaviors to a specific computer depending on its internet access mode, thus contradicting the definition of aggregate use. This violation is explained by the admission that IP collection

is necessary in the event that 'RealOne services [detect] an international IP address and . . . are prohibited from selling that specific service outside of the United States'. The fact that collecting such information in other countries is restricted or prohibited is overlooked. Thus collection of information is framed as an altruistic process, motivated by selfless commitment to protecting the interests of the user and abiding by the law.

The relationship of Real to third parties and information exchange with other parties are tackled with earnestness and ambiguity. Following several pledges to not disclose personal information of an aggregate nature to third parties, Real concludes:

> We will never sell, rent or disclose to third parties our customers' personally identifiable information . . . gathered on a RealNetworks Website unless we are required to do so by law or receive your advance informed consent.

This sentence does not define the term 'personally identifiable', it leaves non-identifiable information exposed, and contradicts previous assurances that all information uses adopted by Real are aggregate. These promises are overturned by a section titled 'Change of Control', at the end of the document, which reads:

> Your personally identifiable information may be transferred in connection with a sale, merger, transfer, exchange or other disposition (whether of assets, stock or otherwise) of all or a portion of a business of RealNetworks, Inc. and/or its subsidiaries.

This admission nullifies previous privacy pledges but is surprising only to the reader who has read the policy in its entirety and was knowledgeable enough about privacy practices to discern the inadequacy of explanations offered. 'Change of Control' clauses have been used to attempt to sell customer information as a means of staving off the financial burden of bankruptcy proceedings (Toysmart) or to profit from the sale of consumer information gathered under false pretenses (GeoCities and Liberty Financial) (Szendro, 2001).

This progression from initially complete privacy pledge to reversed privacy protection exposes the inadequacies of the privacy statement as a policy instrument. The text is founded on principles of marketing and a vague understanding of the law, rather than a universal appreciation for individual privacy. The text summons the reader as a respected customer, but violates that trust through contradictory and vague claims about information protection. Primarily, the statement is conceptualized as a promotional tool, designed to supplement online press releases and statements on charitable work as a testament to the presumed integrity of the company. This superficial approach attempts to establish credibility by employing language and image, while failing to offer practical pledges of privacy protection.

Google

The Google privacy statement (http://www.google.com/privacy.html) reassures consumers that Google 'respects and protects the privacy' of its users and will not disclose 'individually identifiable information'. The statement's language addresses the reader as an average, somewhat educated consumer. There is no legal jargon and little use of complicated computer terms. However, when addressing connections with third parties, the policy is set up to protect Google rather than the user.

> The sites displayed as search results or linked to by Google Search Services are developed by people over whom Google exercises no control. Other links . . . are also on sites not controlled by Google. These other sites may send their own cookies to users, collect data or solicit personal information.

The discourse here is straightforward; the responsibility of Google ends once the user exits the site. However, the remainder of this section would be less discernible to a beginning or moderate computer user:

> Google may choose to exhibit its search results in the form of a 'URL redirector', if you click on a URL from a search result site, information about the click is sent to Google, and Google in turn sends you to the site you clicked on.

Google does not define a 'URL redirector', again assuming the level of the user's computer and internet knowledge. This strategy of vague honesty utilizes frank language to construct a sense of trust while failing to provide substantial privacy assurances.

The Google policy promises that any information collected is done so in the aggregate and is not personally identifiable. Therefore, the statement 'Google may share information about you with advertisers, business partners, sponsors, and other third parties', is qualified to seem less invasive. However, Google collects IP addresses, allowing for the monitoring of user surfing patterns, in the short and possibly the long term. The policy does not reveal that this type of information can be used for marketing purposes. The policy avoids mentioning any purpose of collecting information, even aggregate, except to improve user service. For Google, online privacy is positioned as a low-level concern eclipsed by concerns regarding service quality (of which privacy should be one). If Google regarded privacy in this manner, the privacy policy would be given a more prominent position on the site, all necessary terms would be explicitly outlined for the user in detail, and updates and alterations to policies would be announced. By failing to fulfill these obligations, Google underestimates the consumer's entitlement to online privacy.

Kazaa media desktop

The Kazaa privacy statement (http://www.kazaa.com/us/privacy/privacy.htm) assumes a straightforward tone but refrains from providing extensive

reassurances that privacy will be protected. Instead, this statement admits that privacy policies are limited to personal information, without clarifying the term further. Moreover, Kazaa Media Desktop reiterates throughout the statement that personal information is not collected at all, so it is unclear why the privacy statement is limited to explaining uses of personal information. The further implication is that the site is not responsible for disclosing how it uses non-personally identifiable or aggregately used information, however, the reader is excluded from participating in that decision. The language reveals an effort to explain a complex process in simple terms. Nevertheless, the simplicity in language is accompanied by lack of substance, especially pronounced in the explanations for cookie use and third-party advertising. The text describes procedures rendered, rather than explaining their use or consequence. The discussion of log file use is limited to a paragraph and characterized by a descriptive and informal tone:

> Like most website servers we use log files. This includes internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, platform type, date/time stamp, and number of clicks to analyze trends, administer the site, track users' movement in the aggregate, and gather broad demographic information for aggregate use. We do not collect personal information from log files. We use a tracking utility called URCHIN that uses log files to analyze user movement.

Aside from failing to explain log files clearly, the text claims use of such information is aggregate, neglecting to explain how a utility that tracks a specific behavior back to a certain computer and connects it to demographic information is aggregate. In contrast to Real Networks, Google or MSN statements, this text does not engage in the initial pretense of establishing trust with the reader, but rather provides a scant, descriptive disclosure of information collection practices.

This statement is based on the assumption that collection and exchange of non-personally identifiable information is widely permitted, while personally identifiable information should be protected. While in fact this distinction may be meaningful, there is no legal document that establishes it for online entities. Moreover, these terms are neither defined nor conceptually separated, frequently confusing information that potentially may contain personal data. For example, the Kazaa privacy statement sometimes includes email addresses as personal information and other times places them in the aggregate information category. While Kazaa assures users that no personally identifiable information is shared with others, it admits to sharing aggregate information with third parties. These disclosures appear at first to be straightforward, but the absence of proper and consistent definitions of personal versus aggregate data challenges their integrity.

This pattern of assurances without substance situates the user within a business transaction which empowers the user to provide personal and aggregate information in exchange for a service. The statement reinforces the

assumption that this bargaining game is executed on equal terms, and the words 'choice' and 'opt-out' are used to assert that the user is positioned to make an informed, independent decision. Were this exchange to take place on equal terms, the user would be empowered to negotiate all information provided and the purposes for its use. Instead, the consumer is merely offered the choice of accepting the retailer's terms or not. The option of this compromised choice serves to sustain the false impression of control, while allowing the online entity to determine, enforce and modify the rules of the game without providing equal rights to the user. This pattern is employed frequently in privacy statements and suggests that a revision of privacy protection terms that grants equal power to all parties should be adopted.

POLICY IMPLICATIONS

This sample of portal privacy statements is representative of the services offered; each statement has a different approach, and each exposes inadequacies of privacy statements. The MSN use of language articulates a concern for Microsoft's legal standing rather than for consumer protection. The Google privacy statement offers consumers little protection. The Kazaa statement is dismissive of consumer concerns, and the Real statement is a contradictory promotional apparatus. These statements are insufficient policy devices. The spirit of privacy law is lost in the obfuscatory language, unclear or undefined policies and market orientation of these statements. What is ostensibly a concern for consumer safety is shrouded in rhetoric that protects the portals themselves. Each privacy statement initially assures consumers of a commitment to privacy and subsequently dismantles any true protection of consumer data. These portals are businesses and must be free to operate as such; they must be able to profit responsibly, without undue restriction. However, these privacy statements pose virtually no restriction on businesses to profit excessively from the collection and use of consumer information. Unless consumers read privacy statements, they are unaware that these statements offer little protection. The statements are marketed as protective devices; the language reinforces this belief. Analogously, car leases or loan agreements do not inform customers that the lender is 'committed to helping' them complete payments.

When examined carefully, the rhetoric of these privacy statements reveals business practices that favor profit initiatives over consumer protection. Attempts at a *laissez faire* approach to online business have failed to respect the tenets of privacy law in the USA. While businesses are not obligated to protect consumer privacy, nearly every online business acquiesces to consumer privacy concerns by offering a privacy statement. Insincere privacy guarantees, such as those examined herein, show that company privacy policies are often invasive rather than protective; they describe how consumer privacy is systematically undermined. Consumer cognizance of privacy rights and control over personal data must become policy priorities.

Privacy law is about being let alone, but it is also about the ability to control information about oneself. The law also recognizes an individual's right to profit from one's personal information. Because privacy encompasses both social and economic dimensions, the concept of privacy itself can be regarded as a public good. Public goods such as parks, postal services or universal education contribute to the well-being of a society without any determinable material price, value, ownership or structure for compensation. They are not diminished as they are used; they are available to all, and their value cannot be established through issues of supply and demand. They are essential for both markets and societies to function. Individuals may gain market value for personal information, but the sum of its economic and social value is indeterminable. Moreover, a monetary value cannot be assigned to the basic human dignity of being let alone to enjoy one's solitude, free from undue intrusions. While the philosophical foundation of privacy is predicated on individual dignity, it recognizes the value of privacy in contributing to the common good. In this way, the concept of privacy contributes to the public good in ways that enrich the social environment. Therefore, conceiving of privacy as a public good is a useful foundation for providing recommendations for a democratic internet privacy policy.

Currently, the privacy bills before Congress have stalled due to challenges by businesses claiming that legislative privacy actions interfere with commercial First Amendment rights (*US West* v. *FCC*, 182 F.3d 1224 (10 Cir. 1999)). These challenges may not pass constitutional muster, and Congress is granted the authority to regulate commerce under Article I, Section 8 of the US Constitution. Specifically, this study makes three overarching recommendations informed by public good theory. First, national privacy legislation must be enacted, beyond what is contained in pending bills, based on the Organization for Economic Cooperation and Development (OECD) principles of fair information practices (notice, choice/consent, access, security, enforcement). Consumers will be given opportunities for affirmative consent – opting to divulge information rather than choosing to remove or alter already collected information. This provides consumers with individual agency in their own privacy protection through a plain language format (similar to the Truth in Lending Act of 1968).

Conceptualizing privacy protection as a business transaction can provide a meaningful solution to this policy question, so long as consumers and the private sector participate on equal terms. Inequality in bargaining rights places the consumer in a disadvantaged position, which the privacy statement serves to reinstate. A fair solution either would place controls on the types of private information use to be effected by retailers, or would grant consumers rights to negotiate private information with greater precision, specifying what information is to be traded and for what purpose. Nevertheless, conceptualizing this as a business problem instead of an ethical dilemma forces abstract concepts

such as privacy and information to be treated like commodities. Since these concepts differ from traditional goods or services, their abstract nature prevents us from unitizing them and exchanging them within a capitalist system in a manner that makes sense to all (Bates, 1988).

If private information is to exist as a commodity or currency in the information age, defining it and exchanging it should involve all interested parties in ways that contribute to the public good as well as to corporate profit. Although individuals are protective of material property, internet users, while vaguely protective of their private information online, possess a cavalier attitude about its potential worth, often underestimating the actual value of private information. Second, therefore, the next recommendation from this study is mandated consumer education about privacy rights, stemming from government and industry collaboration, to increase public appreciation of online privacy. Because privacy statements bewilder consumers, this education campaign could encourage consumer support of opt-in privacy measures. The Federal Trade Commission could be mandated to conduct annual audits of online privacy policies to ensure that companies are meeting the expectations outlined in their privacy policies. The TRUSTe privacy stamp program could contract with the Federal Trade Commission to administer the audits, thus fulfilling the TRUSTe guarantee to protect consumer control over personal information. Moreover, the Federal Trade Commission could be authorized to fine offenders, guaranteeing an enforcement mechanism. The self-regulatory mentality prevalent in the USA does not foster a climate in favor of these policy solutions; similar policies adopted by the EU and other US business partners mandate privacy protection.

Third, while several legislative solutions could offer greater protection for consumers, a long-term solution would involve defining private information as a type of private (intellectual) property (as considered by Lessig, 1999), which the individual can disclose at his or her discretion. Consumers could administer their personal data using an information management tool that tracks the compilation, use, disclosure and retention of private data. This would grant consumers with copyright, allowing them to license their personal information. Thus, while portals would be legally obligated to release information in response to court orders or other legal mandates, their use of cookies or tracking devices would be curtailed such that the consumer dictates their use. This solution allows businesses limited access to consumer information yet demands accountability for the collection and use of that information. Further, responding to privacy concerns as intellectual property reflects an economic (or capitalistic) rather than a social ethical solution to a human concern, and opens avenues for the use of other common laws, such as trespass, to address privacy concerns. For example, trespass laws prohibit the unauthorized use of property, and courts are now considering the application of trespass rights to online databases (see *eBay* v. *Bidder's Edge*, 100 F.Supp 2d 1058 (N.D. Cal 2000). Ultimately, this recommendation might

encourage online businesses to contract with users on equal terms, empowering the consumer and reducing the need for misleading 'privacy' statements. It strikes a constructive balance between freedom of information, individual privacy and the public good in ways that enhance the values of democracy.

Acknowledgement

Thanks to Melissa Retano, doctoral student at Temple University, for her assistance in an earlier version of this manuscript.

References

Adkinson, W.F., J.A. Eisenach and T.M. Lenard (2002) *Privacy Online: A Report on the Information Practices and Policies of Commercial Websites*. Washington, DC: Progress and Freedom Foundation.

Bates, B.J. (1988) 'Information as an Economic Good: Sources of Individual and Social Value', in V. Mosco and J. Wasko (eds) *The Political Economy of Information*, pp. 76–94. Madison, WI: University of Wisconsin Press.

Benassi, P. (1999) 'TRUSTe: An Online Privacy Seal Program', *Communications of the ACM* 42(2): 56–9.

Cannon, R. (2001) 'Coping with COPPA: Children's Privacy in an Online Jungle', *Web Techniques* 6(8): 34–8.

Elgesem, D. (1996) 'Privacy, Respect for Persons, and Risk', in C. Ess (ed.) *Philosophical Perspectives on Computer-Mediated Communication*, pp. 45–66. Albany, NY: State University of New York Press.

Fairclough, N. (1995) *Media Discourse*. London: Edward Arnold.

Fairclough, N. (2000) 'Critical Analysis of Media Discourse', in P. Marris and S. Thornham (eds) *Media Studies: A Reader*, pp. 308–25. New York: New York University Press.

Farah, B.N. and M.A. Higby (2001) 'e-Commerce and Privacy: Conflict and Opportunity', *Journal of Education for Business* 76(6): 303–7.

Fausett, B.A. (2001) 'Privacy Certified', *Web Techniques* 6(8): 14–17.

Federal Trade Commission (1998) 'Privacy Online: a Report to Congress', June, URL (consulted March 2004): http://www.federal trade commission.org

Federal Trade Commission (2000) 'Privacy Online: Fair Information Practices in the Electronic Marketplace', May, URL (consulted 30 March 2004): http://www.federal trade commission.org

Fox, S. (2000) 'Trust and Privacy Online: Why Americans Want to Rewrite the Rules', Pew Internet & American Life Project, 20 August, URL (consulted 30 March 2004): http://www.pewinternet.org

Fox, S. and O. Lewis (2001) 'Fear of Online Crime: Americans Support FBI Interception of Criminal Suspects' Email and New Laws to Protect Online Privacy', Pew Internet & American Life Project, 2 April, URL (consulted 30 March 2004): http://www.pewinternet.org

Gillis, C. (2002) 'Soft Talk: Hotmail Pushes for Revenue', *Eastside Journal*, 16 May, URL (consulted 30 March 2004): http://www.eastsidejournal.com/92560.html

Graber, M.A., D.M. D'Alessandro and J. Johnson-West (2002) 'Reading Level of Privacy Policies on Internet Health Websites', *Journal of Family Practice* 31(7): 642–5.

Hamelink, C.J. (2000) *The Ethics of Cyberspace*. London: Sage.

Kandra, A. (2001) 'The Myth of Secure e-Shopping', *PC World* 19(7): 29–32.

Lee, L.T. (2000) 'Privacy, Security, and Intellectual Property', in A.B. Albarran and D.H. Goff (eds) *Understanding the Web: Social, Political, and Economic Dimensions of the Internet*, pp. 135–64. Ames, IA: Iowa State University Press.

Lessig, L. (1999) *Code: and Other Laws of Cyberspace*. New York: Basic Books.

Lipschultz, J.H. (2001) *Free Expression in the Age of the Internet: Social and Legal Boundaries*. Boulder, CO: Westview Press.

McKenna, A. (2001) 'Playing Fair with Consumer Privacy in the Global On-line Environment', *Information and Communications Technology Law* 10(3): 339–54.

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.

Miyazaki, A.D. and A. Fernandez (2001) 'Consumer Perceptions of Privacy and Security Risks for Online Shopping', *Journal of Consumer Affairs* 35(1): 27–44.

Papacharissi, Z. and J. Fernback (2002) 'Online Privacy and Consumer Protection: An Analysis of Portal Privacy Statements', paper presented at the Annual Conference of the Association of Internet Researchers 2002, Maastricht, October.

Princeton Survey Research Associates (2002) 'A Matter of Trust: What Users Want from Websites: a Report on Consumer Concerns about Credibility of Websites', *Consumer WebWatch*, URL (consulted 11 November 2005): http://www.consumerwebwatch.org/news/1.abstract.com

Reagle, J. and L.F. Cranor (1999) 'The Platform for Privacy Preferences', *Communications of the ACM* 42(2): 48–55.

Reilly, R.A. (1999) 'Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward', *Richmond Journal of Law and Technology* 6(2): URL (consulted 30 March 2004): http://www.richmond.edu/jolt/v6i2/article1.html

Ryker, R.E., E.C. Lafleur, C. Cox and B. McManis (2002) 'Online Privacy Policies: an Assessment of the Fortune e-50', *Journal of Computer Information Systems* (42)4: 15–20.

Sheehan, K.B. and M.G. Hoy (2000) 'Dimensions of Privacy Concern among Online Consumers', *Journal of Public Policy and Marketing* 19(1): 62–73.

Szendro, P. (2001) 'Internet Privacy', *Converium*, 12 October, URL (consulted 30 March 2004): http://www.converium.com/web/converium/converium.nsf/0/2AE1F775B3862C0D85256AE30068DF1E?OpenDocument

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

Warren, S.D. and L.D. Brandeis (1890) 'The Right to Privacy', *Harvard Law Review* 4: 193–221.

Wood, L.A. and R.O. Kroger (2000) *Doing Discourse Analysis: Methods for Studying Action in Talk and Text*. Thousand Oaks, CA: Sage.

JAN FERNBACK is an associate professor at the Department of Broadcasting, Telecommunications and Mass Media, Temple University.
Address: Department of Broadcasting, Telecommunications and Mass Media, Temple University, 2020 N. 13th Street, Philadelphia, PA 19122–6080, USA. [email: fernback@temple.edu]

ZIZI PAPACHARISSI is an associate professor at the Department of Broadcasting, Telecommunications and Mass Media, Temple University.