• HUAIQING WANG, MATTHEW K.O. LEE, AND CHEN WANG •

Consumer PRIVACY CONCERNS about Internet Marketing

The Internet is quickly becoming the world's largest public electronic marketplace. It is estimated to reach 50 million people worldwide, with growth estimates averaging approximately 10% per month. Innovative business professionals have discovered that the Internet can

A BUYER'S-EYE VIEW OF ONLINE PURCHASING WORRIES.

A major impediment against full-scale integration of the Internet marketplace with modern business is the lack of confidence Internet consumers have in the newly developed marketing machinery.

be exploited to offer a number of services both for their customers and for their strategic partners. The Internet has also revolutionized retail and direct marketing. Consumers are able to shop from their homes for a wide variety of products from manufacturers and retailers all over the world. They are able to view these products on their computers or televisions, access information about the products, visualize the way the products may fit together, and then order and pay for their choices. The Internet has changed modern business and presented a new paradigm of business relationships and transactions.

Despite the much-heralded recent successes in utilizing the Internet marketplace, one of the major impediments against full-scale integration of the Internet marketplace with modern business is the lack of confidence Internet consumers have in the newly developed marketing machinery [1, 2]. The most crucial issue that Internet consumers have identified is fear and distrust regarding loss of personal privacy associated with the emerging electronic commerce marketplace. One recent survey undertaken by Equifax and Harris Associates determined that over two-thirds of Internet consumers considered the privacy concern to be very important [3, 7].

Despite its importance, the available literature on Internet marketing and privacy is often ad hoc, sketchy, and at times contradictory. There is a clear need for systematic research to synthesize ideas from various sources in order to arrive at a comprehensive picture of the relevant issues. This article presents such a comprehensive picture from the consumer's privacy perspective. For companies engaging in Internet marketing, this article enables them to become better aware of consumer privacy issues and better equipped for the implementation of privacy codes for fair information practices. For consumers, this article provides a comprehensive picture of the issues involved and knowledge of the relevant privacy enhancing technologies and tools that they can use to protect themselves.

What is Consumer Privacy?

The term *privacy* is usually described as "the right to be let alone," and is related to solitude, secrecy, and autonomy. However, when associated with consumer activities that take place in the arena of the electronic marketplace, privacy usually refers to personal information and the invasion of privacy is usually interpreted as the unauthorized collection, disclosure, or other use of personal information as a direct result of electronic commerce transactions. When it comes to the invasion of personal information privacy, the types of personal information that are involved can be classified into two major categories based on their nature.

On the one hand, personal information that is not expected to change dramatically over time can be referred to as *static private information*, such as referential information, historical financial information, health information, personal affiliations and beliefs, and personal documents.

Other private information includes information that changes dramatically over time, but nevertheless can be collected and analyzed in such a way that a well-informed individual profile may be generated. This information is referred to as *dynamic personal information*, such as *activity history* and *activity content.*

A Taxonomy for Privacy Concerns

There exists a wide range of Internet marketing activities that have negative effects on the Internet consumer's individual privacy [5, 9]. The privacy concerns are not limited to the more well-known cases of junk mailing [6, 8], or illicit Web cookie distribution, but have expanded to certain practices that have become cornerstones of Internet merchants' revenue streams, for example, the selling of consumer databases for direct marketing purposes. Over the past few years, we have seen evidence of an increasing number of privacy-related cases, as related to the growth of Internet marketing activities:

- Privacy concerns related to the activities of junk email marketing organizations, such as CyberPromotions and net.net.
- The activities of Web-based advertisements that track the user's usage history and preferences through cookies, such as those from DoubleClick.net, Preferences.com, and many others.

- Privacy concerns over malicious programs that can be constructed through security holes in many Internet tools, such as Java, ActiveX, JavaScript, and many others. Well-known malicious techniques include ActiveX controls that can obtain a person's credit information and JavaScript that accesses personal files.
- Privacy concerns regarding the use and transfer of private information, illustrated by the cases involving: MSN (Microsoft Network) and their practice of tracking all activities of their subscribers; Microsoft SideWalk viewers and their viewing activity patterns to be used for Microsoft marketing purposes. Choices to opt out of such practices are often non-existent or extremely difficult to exercise.

	Improper acquisition			Improper use		Privacy invasion	Improper storage
	Improper access	Improper collection	Improper monitoring	Improper analysis	Improper transfer	Unwanted solicitation	
Direct mailing				P		E	
Preference tracking	E	E	E				
Unwanted eavesdrop	P	E	E				
No opting-out				E			P
Third-party distribution				E	E		P

E: Explicit *P: Probable*

Table 1. A taxonomy of privacy concerns

- Concerns over distribution, often for financial gains, of private information, often for purposes other than the purpose for which it was collected: a noted case is the recent example of America Online selling its subscriber contact information, financial information, and Internet activities.

Table 1 shows a taxonomy of consumer privacy concerns in the Internet marketing area. This table also describes the relationships between the Internet marketing activities (rows) and the privacy concerns (columns). For instance, the first row shows that direct mailing usually causes unwanted solicitation and probably causes improper use of private information.

The column headings appearing in Table 1 are defined in greater detail as follows:

Improper Access: To infiltrate an Internet consumer's private computer without notice to or acknowledgment from the consumer. This type of privacy infringement results in the exposure of private information to unauthorized viewers, often resulting in the collection of such information for marketing purposes.

Improper Collection: To collect a consumer's private information from the Internet without notice to or acknowledgment from the consumer. Such private information includes a consumer's email address, types of software the consumer uses, the consumer's Web access history, private files or databases, etc. Usually, improper collection will lead to improper analysis and improper transfer.

Improper Monitoring: To monitor (conduct surveillance on) a consumer's Internet activities without notice to or acknowledgment from the consumer. By using cookies, Internet marketing businesses are able to watch where and when the consumer visits Web sites, how long the consumer stays, and what type of transactions the consumer conducts. In most cases, improper monitoring will result in improper analysis.

Improper Analysis: To analyze a consumer's private information without proper notice, and to derive conclusions from such an analysis. Such conclusions may include a consumer's shopping and spending patterns, shopping behaviors and preferences. The collection of private information by an Internet merchant initially for one particular purpose, but its subsequent use for other purposes without consent from the consumer, not only could be described as improper analysis but also could result in improper transfer.

Improper Transfer: To transfer a consumer's private information to other businesses without notice to or acknowledgment from the consumer. For instance, various Internet companies sell, publish, distribute, and share their customer databases, which contain cus-

The balancing of beneficial uses of data sources with the privacy rights of individuals is truly one of the most challenging public policy issues of the information age.

tomer private information such as postal and email addresses.

Unwanted Solicitation: To transmit information to potential Internet consumers without their acknowledgment or permission. Such privacy invasions include junk mail, mass direct email, and junk Internet push channels.

Improper Storage: To keep private information in a non-secure manner resulting in a lack of trustworthiness of the stored information, or lack of authentication control for information access. For instance, enabling individual account holders to view private information concerning other accounts, changing information without proper authorization would constitute such privacy concerns. Improper storage is commonly related to the concerns of information confidentiality and data integrity.

Principles for Protecting Privacy

The key issue of privacy in the Internet marketplace is that the privacy rights of individuals should be balanced with the benefits associated with the free flow of information. Protecting privacy must be undertaken in combination with a number of other efforts. There are three main parties involved, each playing different roles:

- *Government*: promoting strong privacy laws for both the public and private sectors; establishing independent privacy commissions to oversee the implementation of these laws; educating the public about privacy issues; encouraging business self-regulation.
- *Businesses*: promoting self-regulation for fair information practices.
- *Individuals*: adopting privacy enhancing technologies, such as network and information security tools.

The U.S. government has recently recommended a set of principles (the "Privacy Principles") governing the collection, processing, storage, and reuse of personal data:

I. General Principles: To guide all the participants and identify the fundamental requirements necessary for the proper use of personal information, and in turn the successful implementation of privacy. Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy. Such information should not be improperly altered or destroyed and should be accurate, timely, complete, and relevant for the purpose for which it is provided and used.

II. Principles for Users of Personal Information: Businesses should assess the impact on privacy in deciding whether to acquire, disclose, or use personal information, and use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information. Businesses should not use personal information in ways that are incompatible with the individual's understanding of how it will be used, and should educate themselves and the public about how information privacy can be maintained.

III. Principles for Individuals Who Provide Personal Information: Individuals should obtain adequate, relevant information about why information is collected, what it is to be used for, how to protect it, how to provide and withhold it and rights of redress, and they should be able to safeguard their own privacy by having a means to obtain information, a means to correct errors, a means of redress if harmed by an improper disclosure or use of personal information, and the ability to use appropriate technical controls to protect personal information, and to remain anonymous.

Regulatory Protection for Privacy

Privacy is a complex concept. An acceptable use of private information in one setting may be an unacceptable invasion of privacy in another. In this section, only those regulations related to consumer privacy in Internet marketing are discussed. A large number of governments have introduced privacy protection laws. In the U.S., the Privacy Act was passed in 1974. This Act restricts the collection, use, and dissemination of personal information by federal agencies. This Act generally applies only to federal records, but not to foreign visitors, private corporations, or other organizations. In 1988, the Computer Matching and Privacy Act was introduced, regulat-

ing federal agencies' use and exchange of information contained in existing agency databases. The U.S. government has also introduced a number of laws to protect all real-time communications and stored transmissions. For instance, the Telecommunications Act of 1996 imposes limits on the use of customer proprietary network information by common carriers. In Europe, the Council of Europe passed Convention 108 (Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data) in 1981. It protects personal data held by both the private and public sectors. It also protects individual freedom by placing limits on the collection, storage, and transmission of personal information. In Asia, for example, Hong Kong has instituted privacy legislation in relation to personal data [4], which is not dissimilar to the provisions of Convention 108.

However, many privacy issues are in the so-called "gray" area. Many industries in the private sector are now introducing meaningful, consumer-friendly, self-regulatory privacy regimes in their operations. These include mechanisms for facilitating awareness and the exercise of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution. The Direct Market Association (DMA) has, for example, established a number of codes and guidelines for self-regulatory actions for its members. For instance, the Mail Preference Service (MPS) and the Telephone Preference Service (TPS) handle unsolicited junk mail and telemarketing. Businesses in the Internet markets are paying more attention to the need for consumer privacy. A growing number of voluntary businesses, from banking and insurance to direct Internet marketing and telecommunications, have written their own privacy codes in an effort to fend off legislation and nurture a much-needed degree of confidence among their consumers.

Privacy Enhancing Technologies

While regulatory approaches aimed at addressing privacy issues in Internet marketing have received considerable attention, the successful integration and widespread acceptance of privacy regulations are still not a reality. On the other hand, a self-initiated private industry aimed at providing technological solutions to practical Internet marketing privacy concerns has been growing at a dramatic rate. Emerging standards as well as the myriad of products embodying privacy enhancing technologies are providing a wealth of individualistic technological choices that one can make to enhance the protection of one's privacy in the context of Internet commerce (see Table 2).

Table 2. Relationships between privacy enhancing technologies and privacy concerns

	Awareness principle		Empowerment principle				Redress principle
	Merchant profiling	**Trust framework**	**Access control**	**User pref. profiling**	**Anonymity**	**Encryption**	**Content filtering**
Improper access		E	E	P			
Improper collection	P	P		P		E	
Improper monitoring	P	P		P	E	P	
Improper use	P	P					
Improper transfer	P	P		P			
Unwanted solicitation				P	P		E
Improper storage	P	P		P		E	

E: Effective *P: Partially effective*

P3 and OPS. One of the leading efforts by the technology industry aimed at standardizing privacy preference expression has been undertaken by the World-Wide Web Consortium (W3C), a non-profit group specializing in proposing and enforcing standards on the Web. The Platform for Privacy Preference (P3) standard will enable Internet consumers to be informed and to make choices about the collection,

use and disclosure of their private information on the Web. Under P3 each Internet merchant will profile and register his or her own privacy practice. In an event in which an Internet consumer's privacy preference matches with the privacy practice profile of the Internet merchant, then no action will be taken. Otherwise, the Internet consumer will be informed of the discrepancies, and he or she will be able to make choices regarding whether to accept or reject each discrepancy. The P3 standard is based largely on the OPS (Open Profiling Standard) submitted by Internet technology vendors: Netscape (which has already announced plans to support P3 in browser and server environments), Firefly (using a proprietary technology in which consumers can submit preference profiles), and VeriSign (which will issue the trusted identity for all the parties involved in the Internet market). Microsoft has also indicated that it intends to support the P3 standard in its future products.

The Internet consumer community has largely supported the standardization efforts such as P3 and OPS, but nevertheless is concerned with the lack of audit and enforcement processes dealing with discrepancies between the privacy profile and actual privacy practices. Profiling techniques can only partially deal with the concern of lack of consumer privacy in the Internet marketplace.

Trust Framework. A number of firms offer technological services to tackle the central issue of universal trust infrastructure. Such a service provides non-repudiation of identity, practices, and privilege for both Internet consumers and Internet merchants.

The service offered by VeriSign (www.verisign.com) deals exclusively with the problem of establishing a trusted identity through the accreditation of the public key, producing what is commonly known as a digital certificate. Verification of identity as established by VeriSign is done through a process called Digital Signature, in which the certificate is checked for VeriSign's authentication signa-

Table 3. Internet software tools and privacy enhancing technologies

	MP	T.F.		Ac.Con.			UPP	Anony.		Encry.		CF	Web URL
		Ce	Ra	IP	GP	TP		Re	Ag	Co	St		
Netscape Browser	+	**	+	**		**	+			**			www.netscape.com
IE Browser	+	**	+	**		**	+			**			www.microsoft.com
Netscape Server	+	**		*	**					**	*	**	www.netscape.com
IE Server	+	**		*	**					**	*		www.microsoft.com
VeriSign	+	**				*	+						www.verisign.com
Nortel Entrust		**		**	*						*		www.centrust.com
GTE CyberTrust		**		*	*								www.cybertrust.gte.com
TRUSTe			**										www.truste.org
NetNanny			*									*	www.netnanny.com
CyberSitter			*									*	www.cybersitter.com
UNIX, WinNT				**	*								various
TIS Gauntlet		*		*	**	*						*	www.tis.com
Remailer								**		*			soda.csua.berkeley.edu
Anonymizer.com								**					www.anonymizer.com
CyberCash				*				*					www.cybercash.com
Jango				*					**				www.marimba.com
PGP		*		**				*		*	*		www.pgp.com
PGP CookieCutter				*								**	www.pgp.com
DiskCrypt				**							**		www.diskcrypt.com
RSA SecurePC		*		**							**		www.rsa.com
Intermute				*								**	www.intermute.com

*: support; **: strong support; +: future support

MP: Merchant Profiling
T.F.: Trust Framework
Ce: Digital Certificate
Ra: Review and Audit
Ac.Con.: Access Control
IP: Individual Permit
GP: Group Permit
TP: Tool Permit (e.g., switch off Java)
UPP: User Pref. Profiling
Anony.: Anonymity
Re: Anonymous Redirection
Ag: Anonymous Agents
Encry.: Encryption
Co: Encryption for Communication
St: Encryption for Storage
CF: Content Filtering

ture. From a privacy perspective, both the Internet consumer and Internet merchant will have to be verified to be trusted in order for an electronic transaction to occur. By dealing with an Internet merchant that is considered trusted, Internet consumers will not have to be concerned about improper access to their private data. Furthermore, issues of improper information collection, improper monitoring and confidentiality can also be dealt with in a similar manner through trusted identities.

On other hand, the services offered by TRUSTe (www.truste.org) are aimed at providing Internet consumers with a trusted brand of privacy practices. TRUSTe can review and audit sites to ensure they correctly disclose their information practices. This approach resembles a regulatory approach in their efforts to deal with improper collection, use, and transfer in a fashion that is limited by the extent of the universality of TRUSTe's service.

Anonymity and Encryption. At present, the most successful and widely used technology that has had a significant impact on the privacy concerns of Internet consumers has been cryptography. Confidentiality of communication between the two communicating parties is dealt with, as any observing third party can not view the contents of a message. Furthermore, encryption can also be utilized for the purpose of protecting one's own data, since undesirable parties cannot collect useful information regarding the Internet consumer. Encryption privacy enhancing technology is often bundled with digital signature technology as the technology underlying an international secure infrastructure, providing effective authenticated, confidential and verifiable means of Internet commerce between Internet merchants and consumers.

Another means of protecting the Internet consumer's privacy is to enable Internet consumers to carry out their activities in an anonymous manner. Numerous current efforts are aimed at enabling Internet consumers to carry out anonymous activities, such efforts include CyberCash (www.cybercash.com), which enables anonymous cash usage in Internet commerce; various anonymous remailers that enable anonymous email communications; Anonymiser.com, which permits consumers to browse the Web anonymously; and intelligent Web agents such as Jango (www.marimba.com).

Local Control and Filtering. In terms of protecting one's own privacy, a wide variety of privacy enhancing technologies have been developed, permitting an individual Internet consumer to choose the level and scope of personal information to be made available to Internet merchants. The first category of personal privacy enhancing technology deals with the issue of access control, in the sense that information is given to Internet merchants only when the required permission is granted. Such a technology has been widely used in the area of controlling access of Internet merchant applications, such as Java, ActiveX, JavaScript, and many others. Individual Internet consumers can enable or disable accesses (such as file system accesses, or communicating with the Internet merchant) based on the marketing purpose of the merchant application. Recently, Internet merchant applications have adopted the certificate and trust framework to provide the consumer with a better sense of understanding with regard to the origin of such applications, resulting in trusted Java and ActiveX technologies. Corporations have long applied various access control technologies, such as firewalls, and proxy servers, not only to protect the privacy of individual corporate users, but also to protect the confidentiality of the organization as a whole.

An individual Internet consumer also may decide to utilize the various privacy enhancing technologies that perform the function of filtering individual Internet marketing messages based on their contents. In the area of electronic message filtering, products such as Intermute and Junk Mail filter have enabled the consumer to resist direct Internet mail marketing efforts and therefore address the privacy concern of unwanted solicitation. Furthermore, parents have long been protecting the privacy of their children by using popular Internet filtering software such as Net Nanny, and Cyber Sitter, which filter out the inappropriate content that may be present (see Table 3).

Conclusion

Internet marketing holds a tremendous potential for businesses and consumers, but it may also cause privacy violations. The balancing of beneficial uses of these data sources with the privacy rights of individuals is truly one of the most challenging public policy issues of the information age. Consumers in the Internet marketplace want to control what personal information is disclosed about them, to whom, and how that information will be used and further distributed. In this article, we have outlined a taxonomy that helps describe, categorize, and analyze consumer privacy concerns. We have also reviewed the current state-of-the-art technology, and pointed out the imminent integration of business self-regulation, regulated law enforcement, and the consumer's ability to enhance individual privacy protection through the use of technology. However, the future is not all rosy. There remains much that needs to be done in order to make the Internet a widely acceptable marketplace for the exchange of goods and ser-

Major Privacy-related Organizations

Electronic Privacy Information Center: www.epic.org
American Civil Liberties Union: www.aclu.org
Consumer Project on Technology: www.essential.org/cpt/cpt.html
Internet Privacy Coalition: www.privacy.org/ipc
Privacy International: www.privacy.org/pi
Privacy Rights Clearinghouse: www.privacyrights.org

vices between merchants and consumers. The nature of the remaining problems are as follows:

- The ability to conduct law enforcement against the violators of individual privacy is very limited. Even though many countries have enacted similar privacy protection legislation, the enforcement of such local legislation is difficult without the aid of international treaties and collaboration since the Internet has no national boundaries. This difficulty is reflected by the inability of some nations in trying to impose selective censorship on the information content available on the Internet.
- Self-regulation might not provide the best solution to privacy concerns. The inability to enforce such regulation in the absence of a widely recognized accreditation system would be disastrous to the consumer's ability to choose creditable Internet merchants, and it would lead to an environment of chaos not dissimilar to the Web market of today.
- Today's privacy enhancing technologies are not only primitive in nature, but also lacking the integrated environment under which most of the Internet consumers' privacy concerns can be dealt with. Such technologies are often cumbersome to use, unfriendly and require a degree of knowledge exceeding that of the common Internet consumer. The lack of technical standards that deal specifically with the privacy concerns of Internet consumers has resulted in many incompatible products providing similar function.

Furthermore, it is vital that privacy enhancing technologies, industry self-regulations, legislation, and legal enforcement regimes be coordinated in order to provide an overall privacy framework that will be used a basis for answering important pragmatic questions such as: When does an individual's responsibility begin and when does it end? Can legal enforcement be conducted in a transparent and unobtrusive manner? While we have made tremendous improvements on the privacy issues related to online marketing, there still remains much to be done before we can achieve the vision of the perfect marketplace that will change the face of commerce as we know it today. C

References

1. Campbell, A.J. Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *J. Direct Marketing 11*, 3 (Summer 1997), 44–56.
2. Determining how and when privacy matters. *J. Direct Marketing 9*, 3 (Summer 1995), 46–60.
3. Kakalik, J.S. and Wright, M.A. Responding to privacy: Concerns of consumers. *Review of Business,* (Fall 1996), 15–18.
4. Lee, M.K.O. Information privacy legislation: The case of Hong Kong. *Hong Kong Computer J. 9*, 11 (Nov. 1993), 23–26.
5. Milberg, S.J., Burke S.J., Smith H.J., and Kallman, E.A. Values, personal information, privacy and regulatory approaches. *Commun. ACM 38,* 12 (Dec. 1995), 65–74.
6. Sipior, J.C. and Ward, B.T. The ethical and legal quandary of email privacy. *Commun. ACM 38*, 12 (Dec. 1995), 48–54.
7. Wang, P. and Petrison L.A. Direct marketing activities and personal privacy: A consumer survey. *J. Direct Marketing* 7, 1 (Winter 1993), 7–19.
8. Weisband, S.P. and Reinig, B. Managing user perceptions of email privacy. *Commun. ACM 38,* 12 (Dec. 1995), 40–47.
9. Wilinsky, C. and Sylvester, J. Privacy in the telecommunications age. *Commun. ACM 35*, 2 (Feb. 1992), 23–25.

Huaiqing Wang (iswang@is.cityu.edu.hk) is an associate professor in the Department of Information Systems at the City University of Hong Kong.
Matthew K.O. Lee (ismatlee@is.cityu.edu.hk) is an associate professor and the head of the Department of Information Systems at the City University of Hong Kong.
Chen Wang (cwang@netdox.com) is a principal technologist with NetDox, a secure messaging start-up company located in Deerfield, IL.