Online Privacy: A Global Perspective

An analysis of the current state of global privacy practices, perceptions, laws and how if affects your organization

Zach Evans

August 5, 2003

Why is online privacy important? This complex question is one that has been haunting businesses and individuals alike since the dawn of the Internet. The World Wide Web—and the technologies that drive it—has broken down cultural, ideological, and geographical barriers, but this 'closeness' has come at a cost. The commercial enterprises that have shouldered a large portion of the development costs of the Internet are looking for a reward for their efforts: information.

The Internet allows for the collection, enhancement, and aggregation of data almost instantaneously. All the parties involved with the online world bring certain expectations to the table and have specific responsibilities they must fulfill. Customers and 'browsers' expect to be able to find what they are looking for in a relatively easy fashion. The attention span of the average online consumer is getting shorter and shorter. Businesses expect browsers to be willing to exchange *something* for the production and distribution of what is largely free content and services. This is where the waters begin to become a little murky. Depending on whom you ask, the responsibilities of each party may vary greatly.

Businesses have taken on substantial risk when they developed their online presence but they must remember one very key fact: online, their competitors are only a click away. To obtain and retain a loyal customer they must accept that privacy and permission are the foundations on which customer trust is built. Businesses that want to survive have to learn to walk the fine line between customer *wants* and business *needs*.

Factors in Deciding to Visit a Web Site

In a recent survey performed by Consumer WebWatch[i], respondents identified nine key factors that influenced their decision to visit a web site.

	Very Important	Somewhat Important	Not Too Important	Not At All Important
The site is easy to navigate and to find what you want	80	16	2	1
Being able to trust the information	80	14	3	1
Being able to easily identify the sources of information	68	25	4	2
Knowing the site is updated frequently with new information	65	28	4	2
Being able to find out important facts about a web site	50	36	8	4
Knowing who owns a web site	32	33	22	12
What organizations financially support the site	24	37	27	11
The site displays seals of approval from other groups	19	41	26	12
The site displays awards and certificates from other groups	9	30	36	23

Source: Consumer WebWatch

Four out of every five users surveyed say that being able to trust the information disseminated through a web site is very important to them and an additional 14 percent say it is somewhat important. A total of only four percent rated trust of a site's information as not too important or worse. This survey finds that users rate the issue of trust and credibility at the very top of their concerns, second only to a site's ease of use.

Additional analysis found that there was little to no variation in the responses when segmented by age or race. In the 18 to 42 year old segment, 82 percent of respondents said that trusting information was very important compared with 75 percent of those age 50 or older. 81 percent of whites, the same percentage of African-Americans, and 77 percent of Hispanics say that trusting information is very important.

The same survey asked respondents to rank six factors that directly apply to their choice of an e-commerce site.

	Very Important	Somewhat Important	Not Too Important	Not At All Important
A statement of fees that you will be charged for using the site	95	3	0	1
A statement of how the site will use the personal information you provide	93	4	1	1
An explanation of when you can expect delivery	89	9	1	1
A statement of the site's policies for returning unwanted items	85	8	1	2
The email address, street address or phone number where you can reach the site's staff	81	14	2	2
The site's privacy policy	76	18	4	2

Source: Consumer WebWatch

A statement of how a site will be using personal information supplied during an e-commerce transaction was rated very important by 93 percent of respondents and an additional four percent rated it as somewhat important. The only item ranked higher (by a total of one percent!) was disclosure of fees that will be assessed during the transaction, such as shipping, transaction, and handling fees.

Again, in the same survey, respondents were asked to rank the importance of various policies and pages on a site as well as being asked about how often they viewed those policies. The results were that 76 percent of the users surveyed felt that a web site having a privacy policy was very important, second only to the credit card protection policy, which 93 percent of users felt was very important.

So what is the bottom line of all of these surveys? Forrester Research estimates that businesses lose **$15 billion** a year in potential revenue due to consumer concerns over privacy protection online.[ii]

Privacy Laws in the United States

Privacy is recognized as a "fundamental human right" in the Universal Declaration of Human rights, which was adopted by the United Nations in 1948.[iii] Some citizens are shocked when they learn that there is no 'right to privacy' guaranteed in the Constitution of the United States. This, however, is the case. In spite of this fact, the Constitution does restrict how the government, at all levels, can collect and use personal information about citizens (see the First and Fourth Amendments and the Equal Protection clause). The court system has, through common (or case) law, limited the intrusive collection of personal information. Congress has even gotten into the mix. In 1977 they initiated a Privacy Protection Study Commission that reported back to them three objectives they should strive for: to minimize the intrusiveness in the lives of individuals by the government; to maximize the fairness in institutional decisions made about individuals with the information that is collected; and to provide individuals with legitimate, enforceable expectations of confidentiality.[iv]

The Better Business Bureau summarizes current privacy laws in the United States on their web site, BBBOnline.org.[iii] A representative sample of these laws can be found below.

Law	Summary
Cable Communications Policy Act	Requires providers to annually inform subscribers as to the nature of personal data collected, data disclosure practices, and subscriber rights to inspect and correct errors in such data.
Census Confidentiality Statute	Prohibits any use of census data for other than the original statistical purpose. Also prohibits any disclosure of census data that would allow an individual to be identified, except to sworn officers and employees of the Census Bureau.
Children's Online Privacy Protection Act of 1998 (COPPA)	Requires web sites directed at children under the age of 13 to obtain 'verifiable parental consent' before collecting personal information online. Also

	requires these web sites to disclose in a notice its online information collection and use practices with respect to children, and provide parents with the opportunity to review the personal information collected online from their children.
Customer Proprietary Network Information	Restricts private sector access and use of customer data. Also imposes restrictions on the use of such data in aggregate form.
Driver's Privacy Protection Act	Prohibits State Department of Motor Vehicles from releasing 'personal information' from drivers' licenses and motor vehicle registration records.
Electronic Communications Privacy Act	Prohibits the tampering with computers or accessing certain computerized records without authorization. Also prohibits providers of electronic communication services from disclosing the contents of stored communications. Usually requires that the customer be notified and given the opportunity to contest in court a government entity's request for access to electronic mail or other stored communications.
Freedom of Information Act (FOIA)	Provides individuals with access to many types of records that are exempt from access under the Privacy Act, including many categories of personal information. FOIA procedures are not available to non-resident foreign nationals.
Gramm-Leach-Bliley Act	Regulates the privacy of personally identifiable, nonpublic financial information disclosed to non-affiliated third parties by financial institutions.
Privacy Act	Mandates that personal data be collected as directly as possible from the record subject. Prohibits collection of information about an individual's exercise of First Amendment rights.
Telephone Consumer Protection Act	Requires entities that use the telephone to solicit individuals, to provide such individuals with the ability to prevent future telephone solicitations. Also prohibits the sending of unsolicited advertisements to facsimile machines.

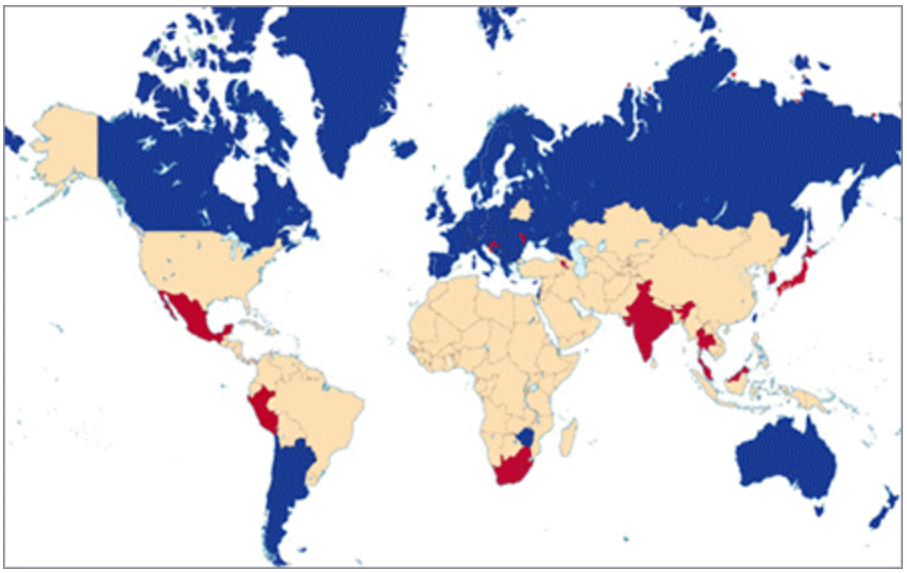
Source: BBBOnline.org

In spite of the laws mentioned above, only one—the Children's Online Privacy Protection Act of 1998—directly regulates the collection of personally identifiable information online. Many of the other laws regulate and restrict the means in which the

collected information may be used or disclosed, but American consumers over the age of 13 must rely only on the trustfulness of the company collecting the information online when it comes to what is collected and how they uses that information internally. This lack of control drastically pales in comparison to the privacy protection laws enacted in other countries throughout the world.

Privacy Laws in Other Countries

Below is a map depicting online data protection laws around the world.[v] Countries shaded in blue have enacted data protection laws while countries depicted in red have not.



Source: PrivacyInternational.org

Most of the developed countries in the world, with the exception of the United States (see above) and China (if they can be classified as 'developed') have already passed into law regulations regarding the protection of data online.

In 2000 the Australian parliament passed into law the Privacy Amendment Act[vi] (the "Act"). The Act provided that personal information could not be collected without

the consent of the person giving it. It further protected consumer privacy by mandating that, once collected, the information must be kept confidential. Furthermore, the information in question could not be transferred to another country that does not offer similar privacy protection. Due to the very nature of the Internet and the fact that it allows even small companies to compete on a global basis, the Act puts serious constraints on US companies wanting to do business in Australia. US companies that do business in Australia, whether through an Australian subsidiary or not, cannot transfer information between countries because the US does not (currently) have adequate privacy protection laws.

American companies that wish to do business in the European Union face an even stricter level of regulation.[vii] Adopted in 1998 and becoming applicable to US companies in 2001, European Union Directive 95/46/EC (the "Directive") states that users must 'unambiguously' give consent for personal data to be collected *after* being informed about the purposes of the collection. The Directive also expressly forbids the collection of 'sensitive data' such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, and sexual preference. Finally, the Directive forbids the transfer of personal data to a country that does not provide a level of protection similar to its own.

In response to the Directive, the US Chamber of Commerce negotiated a set of 'Safe Harbor' provisions with the European Union. These provisions stated that US companies must voluntarily inform customers of the identity of the entity collecting the data, the purposes for any processing of the data, the recipients of the data collected, and any rights that the customer may have in regards to this data. As of mid-2001,

fewer than 75 US companies had signed on to participate in the Safe Harbor program. Of these companies Microsoft, Intel, Hewlett Packard, and Proctor & Gamble have pledged to provide European-grade privacy protection to their customers around the globe, even though no law requires them to do so.

In Canada, the Privacy Commissioner of Canada oversees consumer privacy protection. The Commissioner primarily enforces two laws: The Privacy Act and the Personal Information Protection and Electronic Documents Act ("PIPEDA"). The Privacy Act is, essentially, a code of ethics for the government's collection and handling of personal information. The Privacy Act also ensures that Canadian citizens have the right to access information collected about them, and that they can challenge the accuracy of the information.[viii]

PIPEDA's main focus is the regulation of privacy practices in the private sector. Under the guidelines of the law, organizations can only collect information about you if it is: gathered with the knowledge and consent of the consumer, collected for a reasonable purpose, used only for the reasons for which it was gathered, accurate and up to date, open for inspection and correction by the consumer, and stored securely. All organizations that operate within Canada are regulated by this law and are also required to designate an individual to handle privacy issues and any complaints lodged against it.

Making Privacy a Top-Level Issue

Many companies are already taking issues of privacy very seriously in light of the Internet. At the very least they are posting detailed privacy policies on their web sites and making printed copies of these policies available to customers that request them.

Larger organizations have even gone as far as creating a new C-level position: the Chief Privacy Officer (the "CPO"). They have also developed programs designed to increase employee awareness and training about the issue of customer privacy while also establishing self-regulatory initiatives.

The CPO position serves as a liaison between the organization and the consumers. These high-powered offices often have veto power over: new product launches, marketing campaigns, and strategic partnerships. Any and all customer-facing programs or internal practices that deal with sensitive information come under the direct supervision and regulation of the CPO.[ix]

Guidelines for Online Privacy Policies

Strong corporate privacy initiatives start with the adoption and implementation of an organization-wide privacy policy. The organization has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information. The organization should also take steps to foster the adoption of effective privacy policies by the other organizations that they interact with.

Once the privacy policy has been adopted the organization must implement a policy of notice and disclosure. The corporate privacy policy must be easy to find, read, and understand. It must also be available prior to or at the time that the individually identifiable information is collected or requested. The policy should clearly state several things: what information is being collected; the use of the information being collected; the choices available regarding collection, use, and distribution of the information collected; a statement of an organizations commitment to data security; and the steps the organization takes to ensure data quality and access. Finally, the policy should also

disclose the consequences, if any, of an individual's refusal to provide information to the organization.

After notifying and disclosing the privacy policy to its customers, the company must also allow their customers the right to choose. Individuals must be given the opportunity to exercise their right to choose regarding how the information collected may be used when such use is unrelated to the purpose for which it was collected. At the very minimum, individuals must be given the option to opt-out of receiving any future information from the company or any of the company's partners.

Finally, the company has three distinct responsibilities for the data that they have collected: security, quality, and access. The company should take all appropriate steps and measures to assure data reliability and should take reasonable precautions to protect it from loss, misuse or alteration. The company should also take all reasonable steps to ensure the data is accurate, complete, and timely for the purposes for which they are to be used. Appropriate processes or mechanisms need to be implemented so that inaccuracies in the data may be corrected. Reasonable consumer access to, and correction of, the data need to be planned for as well.

Online Privacy Resources and Certifying Organizations

Out of the ashes from the Internet boom of the mid- to late-1990s, one new and one old non-profit organization emerged whose sole purpose was the promotion, monitoring, and certification of online privacy practices and policies. TRUSTe[x] (a.k.a. the new entrant) and the BBBOnline[xi] (part of the Better Business Bureau, a.k.a. the old entrant) are attempting to standardize privacy practices to allow businesses to practice

their trade better while also giving customers a recognizable 'seal of approval' they can trust in.

TRUSTe is an independent privacy initiative dedicated to building users' trust and confidence on the Internet and accelerating the growth of the Internet industry. They've developed a third-party oversight 'seal' program designed to alleviate users' concerns about online privacy, while meeting the specific business needs of each of the licensed web sites. TRUSTe has four separate privacy programs available to its licensees: the Privacy Statement Trust Mark, the Kids Privacy Statement Trust Mark, the eHealth Privacy Statement Trust Mark, and the European Union (EU) Privacy Statement Trust Mark.

TRUSTe only awards the Privacy Statement Trust Mark to sites that adhere to established privacy principles of disclosure, choice, access, and security. Along with this, the sites that display the privacy seal must agree to comply with ongoing oversight and alternative dispute resolution processes if a complaint is ever lodged against them.

The Children's Privacy Seal program offers companies a solution for addressing children's privacy issues. The Children's Privacy Seal program is completely compliant with the Children's Online Privacy Protection Act of 1998 (COPPA) and has been approved by the Federal Trade Commission as an authorized 'safe harbor' for companies subscribing to the service.

The eHealth Privacy Statement Trust Mark was developed through a team effort with the American Accreditation Health Care Commission to provide a certification program for companies that provide health services and information on the Internet.

This program assures users that the web site they are using is following all of the necessary HIPPA regulations in regards to their medical information.

Finally, the EU Privacy Statement Trust Mark allows companies that do business with members of the EU, to comply with the Safe Harbor Privacy Framework set forth by the U.S. Department of Commerce after negotiations with EU authorities.

The BBBOnline, a wholly owned subsidiary of the Better Business Bureau, has as its mission to promote the trust and confidence of the Internet through the BBBOnline Reliability and Privacy Seal programs. BBBOnline's web site seal programs allow companies with web sites to display seals once they have been evaluated and confirmed to meet the program's requirements.

The BBBOnline has two programs to offer: on that is for traditional Better Business Bureau members and one that is available to anyone willing to abide by its premises. The first program, the BBB Reliability Seal, confirms that a company is a member of their local Better Business Bureau, has been reviewed to meet truth in advertisement guidelines, and follows good customer service practices. The second program, the BBB Privacy Seal, confirms to users that the licensing company stands behind its online privacy policies and has met the program requirements regarding the handling of personal information that is provided through its web site.

A third, more technical, option is beginning to gain momentum as a means to standardize privacy policies across web sites in order to give consumers a single view of their privacy rights. The Platform for Privacy Preferences Project[xii] ("P3P") has been developed by the World Wide Web Consortium ("W3C") as a "standardized set of

multiple-choice question[s] covering all the major aspects of a web site's privacy policies."[xiii]

According to the W3C, the goal of P3P has two parts: First, P3P is designed to allow web sites to present their privacy policies in a machine-readable format that P3P-enabled web browsers can read and then compare to the users' own set of privacy preferences. Secondly, it better allows users to understand what data is being collected about them, how it will be used, and what their 'opt-in' and 'opt-out' options are.

One major drawback of the P3P system is that it does not provide a mechanism for the enforcement of its guidelines. The W3C is not a regulatory body; its goal is to promote the standardization of the Internet so that it can be more easily developed and used. At best, P3P should be viewed as complementary to current, and future, laws and other self-regulatory programs that do provide enforcement protocols.[x]

Recent Changes in Information Collection

More and more, companies are beginning to better define the line between their customer's personal need for privacy and their business needs to have access to information about their customers. A study sponsored by The Progress and Freedom Foundation[xiv] ("PFF") looked at 85 of the Internet's most popular web sites—such as Amazon.com, CNN.com, and Yahoo.com—as well as a random sample of sites receiving more than 39,000 visitors a month in order to better understand the use of privacy policies and whether or not companies are taking privacy seriously or not.

The study found that web sites are collecting 'significantly less' information about browsers then they were as reported in a 2000 study and the use of 'cookies' (small text files a site stores on a user's computer) by web sites to track browser behavior has

fallen by 30 percent. Furthermore, sites are more likely to "offer visitors choices in how personal information might be used or shared outside the company." The survey cluster that included the Internet's most popular sites showed that 93 percent of them offered visitors 'opt-in' choices, up from 77 percent in the previous study. While the PFF admits that these changes are largely evolutionary, not revolutionary, it is widely held that they signal a move in the right direction for consumer privacy advocates.

Final Thoughts

Any organization that exists online today must face the reality that consumer privacy protection concerns are important, not only to the consumers they effect, but to their own survival as well. Organizations that provide high-quality privacy protection and offer their consumers something valuable in return for the information they provide will be able to truly reap the benefits of communication and community the Internet allows. Before any organization can make that leap however, they must first do a better job of educating their consumers about their data access needs and the methods and means they are using to collect that data.

A study[xv] by the Annenberg Public Policy Center of the University of Pennsylvania ("APPC") recently found that 57 percent of the adults that used the Internet at home believed "incorrectly that when a web site has a privacy policy, it will not share their personal information with other web sites or companies." More than half of the adults they surveyed—without knowing the contents of the policies—felt that simply having a privacy policy posted meant the web site would guard their personal information and would not give it to anyone else. Any one that has ever signed up for an email newsletter and then started getting inundated with SPAM knows that this is not the

case: most of the web sites that have such unsavory practices have privacy policies posted on their web sites.

Percentage of adults who 'Agreed' or 'Strongly Agreed' with these statements:	
I should have a legal right to know everything that a web site knows about me.	94
I am nervous about web sites having information about me.	70
I look to see if a web site has a privacy policy before answering any questions.	71
I trust web sites not to share information with other companies or advertisers when they say they won't.	49
Web site privacy policies are easy to understand.	47

Source: Annenberg Public Policy Center of the University of Pennsylvania

Organizations must take a much more proactive role in educating their users on online privacy truths, practices, and principles.

APPC also found that users are fairly positive and upbeat when it comes to the possible effectiveness of privacy policies.

Responses of adults to policies' probable effectiveness (percentage)	Very or Somewhat	Neither Effective nor Ineffective	Not Very or Not at All
A law that requires web site policies to have easy to understand rules and the same format.	86	0.5	12
A law that gives you the right to control how web sites use and share the information they collect about you.	84	0.5	15
A law that requires companies that collective personal information online to help pay for courses that teach Internet users how to protect their privacy online.	74	0.5	25

Source: Annenberg Public Policy Center of the University of Pennsylvania

Since no organization likes to be legislated into compliance if they can help it, they should take advantage of the opportunity to reduce consumer's concerns, educate them, and become compliant with both domestic and global privacy laws.

[i] A Matter of Trust: What Users Want from Web Sites : A survey performed by Princeton Survey Research Associates for Consumer WebWatch : Published in January 2003 : Available online at www.consumerwebwatch.com.

[ii] PRIVACY: What Every Manager Should Know : Published in the May/June 2002 issue of *The Information Management Journal*

[iii] Privacy@net: An international comparative study of consumer privacy on the internet : A study performed by Consumers International Office for Developed and Transition Economies : Published in January 2001 : Available online at www.consumersinternational.org.

[iv] A Review of Federal and State Privacy Laws : A report by the Better Business Bureau : Available online at www.bbbonline.org/understandingprivacy/

[v] www.privacyinternational.org/survey/dpmap.jpg

[vi] www.privacy.gov.au

[vii] Global Privacy and the Privacy Clash : Published in the January/February 2002 issue of *The Information Management Journal*

[viii] www.media-awareness.ca

[ix] The Ethics of Database Marketing : Published in the May/June 2002 issue of *The Information Management Journal*

[x] www.truste.org

[xi] www.bbbonline.org

[xii] www.w3.org/P3P/

[xiii] www.cmor.org/govt_affairs_opr1.htm

[xiv] www.upi.com/print.cfm?StoryID=270032002-011257-9793r

[xv] Americans & Online Privacy: The System is Broken : A report from the Annenberg Public Policy Center of the University of Pennsylvania : Published in June 2003 : Available online at www.appcpenn.org.