International Journal of Finance and Accounting 2012, 1(6): 148-161
DOI: 10.5923/j.ijfa.20120106.03

Online Privacy Protection:Privacy Seals and Government Regulations in Select Countries

Madan Lal Bhasin

Department of Accounting & Finance, Bang College of Business, KIMEP University, Almaty, Republic of Kazakhstan

Abstract The proliferation of the Internet as a business medium has exacerbated violation of individual privacy. New e-business technologies have increased the ability of online merchants to collect, monitor, target, profile, and even sell personal information about consumers to third parties. Governments, business houses and employers collect data and monitor people, but their practices often threaten an individual's privacy. Because vast amount of data can be collected on the Internet and due to global ramifications, citizens worldwide have expressed concerns over increasing cases of privacy violations. Several privacy groups, all around the world, have joined hands to give a boost to privacy movement. Consumer privacy, therefore, has attracted the widespread attention of regulators across the globe. With the European Directive already in force, "trust seals" and "government regulations" are the two leading forces pushing for more privacy disclosures. Of course, privacy laws vary throughout the globe but, unfortunately, it has turned out to be the subject of legal contention between the European Union and the United States. The EU has adopted very strict laws to protect its citizens' privacy, in sharp contrast, to 'lax-attitude' and 'self-regulated' law of the US. For corporations that collect and use personal information, now ignoring privacy legislative and regulatory warning signs can prove to be a costly mistake. An attempt has been made in this paper to summarize the privacy legislation prevalent in Australia, Canada, the US, the EU, India and Japan. It is expected that a growing number of countries will adopt privacy laws to foster e-commerce. As a discussion-oriented paper, the main purpose is to share the information with the reader's.

Keywords Online Privacy, Security, Trust Seals, Government Regulation, Australia, USA, EU, Canada, Japan, India, Technology-Based Solutions

1. Introduction

For any organization to thrive in today's business environment, it must deal effectively with global competition and the rapid pace of technological change. The Internet has played a vital role in transforming business in the new millennium. With the opening of the Internet for commercial activities in 1991, thousands of businesses all over the world have hooked up and started doing business online, from establishing a mere presence to using their sites for transactions[1]. Still, the Internet is a public network and doing business online continues to be a double-edged sword. Everyday, companies are opening their information systems to other businesses and to the public to increase sales, and to make shopping, purchasing, and service more convenient for their clients. Unfortunately, the more businesses allow access to their services and systems through the Internet, the more they are vulnerable to security breaches[2]. Along with growing concerns about security, consumers are also concerned about their privacy. The potential for violation of privacy in e-commerce has been an issue of significant controversy ever since business on the Web began. Personal information is readily available because of the widespread usage of the Internet and of cloud computing, the availability of inexpensive computer storage, and increased disclosures of personal information by Internet users in participatory Web 2.0 technologies. The increased availability of online personal information has fuelled the creation of a new tracking industry. Behavioural advertising, a form of online advertising, is delivered based on consumer preferences or interest as inferred from data about online activities. In 2010, over $22 billion was spent on online advertising. This revenue allows websites to offer content and services for free. "What They Know," an in-depth investigative series by the Wall Street Journal, found that one of the fastest growing Internet business models is of data-gatherers engaged in "intensive surveillance of people[visiting web sites] to sell data about, and predictions of, their interests and activities, in real time"[3]. Web sites such as Spokeo, an online data aggregator and broker, give site visitors vast quantities of personal information. Consumers and public interest groups are filing complaints to challenge the collection and use of

* Corresponding author:
madan.bhasin@rediffmail.com (Madan Lal Bhasin)
Published online at http://journal.sapub.org/ijfa

consumer data without consumer consent or knowledge. Online privacy concerns are widespread.

The proliferation of the Internet as an educational and business medium has exacerbated violation of individual privacy. Today, computers make the collection, maintenanc e, and manipulation of personal data more possible, faster, less expensive, and more effective than manual methods[4]. A serious concern for individual privacy is growing right alongside the growth of e-commerce. In this context, privacy is the ability of individuals to control information about themselves—what and how much is collected, how it may be used, and so on. Three parties may violate the privacy of individuals—*government, businesses*, and *employers*[2]. Governments need individuals' information for planning of infrastructure, education and other services, as well as to facilitate law enforcement. Businesses collect consumer information to better target their marketing and service efforts. Employers monitor employees to ensure productivity and enforce corporate policies. Undoubtedly, all three parties have a legitimate need to collect data on individuals and to monitor people, but unfortunately their practices threaten privacy. On the other hand, individuals often feel that too many organizations know too much about their private lives. Therefore, many people try as hard as they can to minimize the amount of information collected about them, or at the least, they demand that their consent to use their personal information be obtained[5].

Collection of data by businesses about individuals has always invoked issues of privacy. However, online technology increases the concerns, as it allows for faster and easier storage of more data. It also allows for easier manipulation of that data and cross-referencing at unbelievable speeds[6]. In addition, in the online world, data collection can occur even without the knowledge of the individual, through the use of 'cookies'. "Privacy is also threatened by the tracking of consumer usage by Web sites and 'click- stream' data is the term given to data that tracks user surfing habits online."[2]. Finally, privacy is threatened when individuals' data is shared and/or sold by some companies with other companies, without the explicit approval of the individuals. Consumers are usually afraid that businesses, including those on Web sites, will sell personal information to other organizations without their knowledge or permission.

Well, in the past few years, several organizations have had significant lawsuits filed against them by customers claiming that their privacy was violated. Consumers, all over the world, are becoming increasingly angry when their personal information is used or released without their permission. As a result, new laws and regulations are being introduced in different countries that prohibit companies from releasing customer information to third parties without the consumer's express consent. Until privacy practices are made consistent and all organizations doing business online learn to properly respect individuals' right to privacy, we can expect these disputes to continue. As long as they do, some people will be reluctant to provide personal information online, and e-business will suffer[7].

However, online technology increases the concerns, as it allows for faster and easier storage of more data. It also allows for easier manipulation of that data and cross-referencing at unbelievable speeds[3]. In addition, in the online world, data collection can occur even without the knowledge of the individual, through the use of cookies. Information relating to individuals, called 'personal data,' is collected and used in many aspects of everyday life. An individual gives personal data when he/she, for example, registers for a library card, signs up for a membership of a gym, opens a bank account, etc. Personal data can be collected directly from the individual or from an existing database. The data may subsequently be used for other purposes and/or shared with other parties. Personal data can be any data that identifies an individual, such as a name, a telephone number, sex, or a photo. Internet technology has posed new challenges to the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination[8]. Each of these systems is capable of monitoring, capturing, and storing communicatio ns that pass through it.

In today's technological world, millions of individuals are subject to privacy threats. There emerged various cases on Internet privacy, such as, Google Earth map, right of being online anonymous, mobile-phone tracking, surveillance etc, which have close tie to safety and freedom of expression. Face book is the most popular 'social' networking site. Student life without Face book is almost unthinkable. Thus, social network sites deeply penetrate their users' everyday life and, as pervasive technology, tend to become invisible once they are widely adopted, ubiquitous, and taken for granted. When people, for instance, set up accounts for "Face book," they enter bank and credit card information to various websites. The analysis by a researcher[9] shows that "Face book's privacy strategy is a self-regulatory privacy policy mechanism that advances an individualistic privacy conception. It tries to manipulate the perception of privacy by Face book users and the public by complexifying the understanding of targeted advertising in its privacy policy, minimizing advertising control settings, implementing a complex usability for the few available advertising opt-outs, and reducing privacy to an individual and interpersonal issue".

Specific privacy concerns of online social networking include inadvertent disclosure of personal information, damaged reputation due to rumours and gossip, unwanted contact and harassment or stalking, surveillance-like structures due to backtracking functions, use of personal data by third-parties, and hacking and identity theft[10]. The rise of social networks and Cloud computing are increasingly defining norms of privacy, acting as gatekeepers for applications, and setting their own proprietary standards rather than universally compatible standards[4].

In cyberspace users' rights to privacy and freedom of expression, are not only be infringed by government monitoring and surveillance, but also impacted by Internet intermediaries, companies or simply by other users[11]. It is possible to record many online activities, including which online newsgroups or files a person has accessed, which Web sites and Web pages he/she has visited, and what items that person has inspected or purchased over the Web. Much of this monitoring and tracking of Web site visitors occurs in the background without the visitor's knowledge. Web sites can learn the identity of their visitors if the visitors voluntarily register at the site to purchase a product or to obtain a free service, such as information. Web sites can also capture information about visitors without their knowledge using "cookies" technology[12]. Cookies are tiny files deposited on a computer hard drive when a user visits certain Web sites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has deposited a cookie, the Web site software will search the visitor's computer, find the cookie, and "know" what that person has done in the past. It may also update the cookie, depending on the activity during the visit. Recently, Sweden passed legislation that restricts how Web sites can use cookies.

The Internet is inspiring even more subtle and surreptitious tools for surveillance. "Web bugs" (sometimes called invisible.GIFS or clear.GIFS) are tiny graphic files embedded in e-mail messages and Web pages that are designed to monitor who is reading the e-mail message or Web page[13]. They transmit information about the user and the page being viewed to a monitoring computer. Because Web bugs are very tiny, colourless, and virtually invisible, they can be difficult for unsophisticated Internet users to detect. Marketers use these Web bugs as another tool to monitor online behaviour and can develop detailed consumer profiles by combining Web bug data with data from other sources.

2. Privacy Versus Security

Privacy and security are said to be two of the biggest concerns regarding e-business/commerce. In reality, both are major concerns for any computerized environment, including businesses, governments, and individuals. Privacy of data can be thought of as the confidentiality of the data collected by businesses or governments about the individuals using their services. Simply stated, privacy is the ability to manage information about oneself. Since it is willingness of consumers to share information over the Internet that allows transactions to be made, the consumers' control over 'how much' and 'what' information is shared is the essence of privacy on the Internet[2].

A security threat is defined as a "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse."[14]. Security, then, is the protection against these threats. Under this definition, threats can be attacks on network and data transactions or unauthorized access by means of false or defective authentication. However, discussion about various forms of security threats, and security technologies and solutions is beyond the scope of the present paper. The primary focus will be on the issue of privacy protection on the Internet.

In other words, security relates to controlling one's environment for protection of data[15]. Consumers, in the context of security, could be concerned with sharing information online because they fear hackers stealing their information. Privacy refers to monitoring the secondary use of information. Consumers, in the context of privacy, could be concerned that once the information is freely submitted to a Web site, there is diminished or nonexistent control over whether and/or how there is further sharing of that information with third parties.

3. What is Privacy Concept?

As individuals and businesses continue to use e-business in increasing numbers, an equally increasing amount of information about these same individuals and businesses is collected and stored. If the parties involved are knowledgeable about the data being collected and how those data will be used, there is not a problem. The problem occurs when users either do not know what data are being collected, or do not know or consent to how the data should be used. The question of the degree to which the privacy rights of individuals should be protected is a leading barrier to global e-business. On the surface, it seems obvious that privacy rights should be protected, but the common standard applied differs from country to country. For example, privacy laws in the European Union are much stricter than those in the United States, which implies that U.S. companies who want to do business in the European Union must follow the E.U. standard[16]. However, the issue is not that simple.

One of the most important issues in managing information, which has both legal and ethical implications for managers, is "privacy". In the context of information, 'privacy' refers to an individual's rights as a customer, employee or citizen concerning what personal data are held about them by third-parties, such as companies, employers and government agencies and how they are used. Privacy is usually defined as the right of any citizen to control his or her own personal information and to decide about it (to keep or disclose information)[17]. Privacy is a fundamental human right recognized by Article 12 of UDHR, the International Covenant on Civil and Political Rights, and in many other international and regional human rights conventions[4]. Now-a-days, computers make the collection, maintenance, and manipulation of personal data more possible, faster, less expensive, and more effective than manual methods. Therefore, a serious concern for

individual privacy is growing right alongside the growth of e-commerce. Privacy is the "claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state."[1]. In this context, privacy is the ability of individuals to control information about themselves—what and how much is collected, how it may be used, and so on.

"Privacy is the right to be left alone, when you want to be, to have control over your own personal possessions, and not to be observed without your consent. It is the right to be free of unwanted intrusion into your private life."[18]. As mentioned earlier, privacy has several dimensions: individuals snooping on each other; employers' collection of information about employees; businesses' collection of information about consumers; government collection of personal information; and the issue of privacy in international trade. Claims to privacy are also involved at the workplace: millions of employees are subject to electronic and other forms of high-tech surveillance[19]. Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective. Collection of data by businesses about individuals has always invoked issues of privacy.

In July 2000, the U.S. Federal Trade Commission (FTC) identified five core principles of privacy protection that are widely accepted in the U.S., Canada, and Europe[20]. The FTC core principles are:

- **Notice—**Consumers should be made aware of an entity's information practices before any personal information is gathered.
- **Choice—**Consumers should be given the opportunity to consent or deny any secondary uses (uses other than the processing of a transaction) of information. Secondary uses include mailing notices or transfer of data to third parties.
- **Access—**Consumers should be able to access their personal data and review it without significant delays. Further, consumers should be able to easily correct inaccurate personal information in a timely manner.
- **Integrity and Security—**The data regarding consumers' personal information should be processed in a fashion so that the data is accurate. Further, the data needs to be kept confidential as it is transmitted, processed and stored by the entity.
- **Enforcement—**Consumers should have recourse to action, if any, of the above 'core' principles are violated.

Unless businesses fall into certain categories (such as medical or financial institutions), U.S. law does not require that they abide by any of these. Note that the fourth recommendation is actually making two recommendations ensuring accuracy and ensuring that only authorized people have the access to the data.

Unfortunately, U.S. companies are notorious for not following the very first recommendation. Some do have policies in place to ensure access only on a "need to know" basis. Industry groups, such as the On-Line Privacy Alliance[5] have vigorously lobbied against increased government regulation in this area, claiming that the current self-regulated environment is adequate. Critics, however, have questioned the ability of these groups to properly monitor the industry and suggest that the privacy seals may be no more than marketing ploys to lull consumers into a false sense of security.

To enforce privacy rules, some companies have established the position of "Chief Privacy Officer" (CPO). The appointment of such an officer may calm fears of privacy abuse[21]. Regarding the privacy rights of adults, the U.S. government is still willing to allow private industries the opportunity to device sufficient privacy rights policies, but thus far these efforts have fallen short of expectations. As opposed to the United States, all European Union nations have strict laws that ensure all the above rules are followed in letter and spirit. The U.S. government is facing pressure from privacy advocacy groups and the European Union's (EU) new privacy regulation. As a result, U.S. lawmakers are increasingly "threatening" the business sector that they may soon introduce privacy regulations if industry efforts are not satisfactory[8].

To reduce consumer privacy concern and subsequent negative responses, organizations need to pay close attention to their privacy policies through greater self-regulation, third-party accreditation, and to ensure the presence of compliance mechanisms that support and check the marketing and collection activities of their organization and related parties[7]. Regulators can reduce consumer concern by further defining and improving the legal framework for protecting consumer privacy on the internet. In addition, governments should consider overseeing third-party privacy accreditation as well as firm and industry self-regulation. Finally, to improve consumer perceptions of privacy protection, enhanced regulatory privacy protection should be communicated to the public along with a response outlet for privacy concerns so that consumers know that they should report privacy-related complaints to a regulatory agency.

4. Privacy Policy or Statement

Companies that are open and honest in their communications usually adopt privacy policies or statements, and are very clear about how they use collected data discreetly to further corporate growth, efficiency and performance will benefit from wider consumer acceptance in international markets. This is what leads to increased revenue, less litigation from the aggrieved, enhanced reputations for their brands, and more prospective partners willing to enter into lucrative cooperative ventures that require a deep well of trust. Among the companies given high marks by privacy advocates for making data protection a priority, to name a few, are Dell, IBM, Intel, Microsoft, Procter & Gamble, Time Warmer and Verizon. Some of these companies—such as Microsoft, which has in the past been plagued by security leaks in its operating system and e-commerce programs—have embraced hard-line privacy

stances only after experiencing first-hand the potential damage to their businesses that privacy breaches can inflict.

One way that consumers have to be knowledgeable about the possible consequences of dealing with a Web merchant is the privacy policy or statement. This statement should discuss the privacy policy of the Web merchant regarding the data collected and their subsequent use. It should be easily accessible through a link clearly visible on the first page (home page) of the merchant's Web site. Some companies show this link at the bottom of their home page (in small type) while others show it at the top of their home page. When a company wants to design its own privacy statement, the manager in-charge has to be careful to include all policies to which the company wishes to adhere, and to include them in clear, concise language. The manager must then write the actual statement, have it approved by the company's management (and probably the company's legal department or law firm), and finally, post it on the company Web site. The content of the statement, of course, will vary from company to company. To promote the use of privacy statements, several online tools have been developed to automatically generate or test privacy statements. For example, Microsoft Corporation has a privacy statement generator at www. Microsoft.com/privacy/wizard/, and similarly, the *IBM Corporation* had its own at www.alphaworks.ibm.com/tech/p3peditor[22]. However, many Web sites do not even have privacy policies.

Although online retailers detail their privacy practices in online privacy policies, this information often remains invisible to consumers, who seldom make the effort to read and understand those policies[5]. Businesses address these privacy concerns by posting privacy policies or displaying privacy seals to convey their information practices. However, 70% of people surveyed disagreed with the statement privacy policies are easy to understand, and few people make the effort to read them (Privacy Leadership Initiative 2001, Trustee 2006). Similarly, empirical evidence suggests that consumers do not fully understand the meaning of privacy seals[23]. Various studies have also indicated that most people are willing to put aside privacy concerns, providing personal information for even small rewards. In such cases, people readily accept trade-offs between privacy and monetary benefits or personalization. Studies show privacy policies are hard to read, read infrequently, and do not support rational decision making [11].

Privacy (or Trust) seals and government regulations are two leading forces pushing for more and better privacy disclosures on Web sites. Trust seals promote privacy in the form of self-regulation by industry, while government regulation takes the form of litigation, forcing companies into better privacy practices[24]. Both trust seals and government regulations are summarized below.

5. Privacy/Trust Seals

"Trust" is particularly important in online markets to facilitate the transfer of sensitive consumer information to online retailers. As privacy concerns have been identified as a primary barrier to consumer trust online, governments and third parties have proposed various approaches to privacy protection. We find that firms' ability to influence consumer beliefs about trust depends on whether firms can send unambiguous signals to consumers regarding their intention of protecting privacy[25]. At the heart of these approaches are "privacy or trust seals" that aim to empower consumers with more transparency and control over their information. Therefore, it is important to realize what privacy/trust seals are and the distinction between the major seal sources. Seal issuing authorities provide a set of guidelines and a voluntary enforcement mechanism to assure that the site abides by its own privacy policy. "Privacy seals symbolically communicate a third-party authority designed to engender trust in the Web site's information practices as stated in their privacy policy. By clicking on the privacy seal, the user can check back with the seal authority's Web page to verify authenticity." The seal authorities collect an annual fees ranging from a few hundred to several thousand dollars, prorated on revenues, for the seal's display[26].

In the United States, there are three not-for-profit organizations, whose purpose is to guarantee that Web sites maintain adequate privacy standards. These organizations respond to voluntary invitations of commercial Web sites to examine their standards. If a Web site passes the test, they allow the site to use their seal of approval. While such organizations provide e-commerce firms with a mechanism of self-regulation, most of them have not sought such seals of approval. These seals are supposed to instil consumer confidence in the Web site. Examples of these seals include the Better-Business-Bureau Online (BBBOnLine), AICPA WebTrust, and TRUSTe. A number of other seals also exist on the Internet. For example, there is the VeriSign program, which is mostly for security through encryption and authentication products, or the International Computer Security Association's (ICSA) seal. Table-1 compares some of the requirements for businesses that want to display three of the trust seals.

The AICPA WebTrust seal program was specifically started to address customer concerns about privacy and security on the Internet. It focuses on disclosure of not only what information is collected and how it will be used, but also on business practices of the company. It requires a thorough examination of the Web site by a certified public accountant or a chartered accountant. BBBOnLine, a subsidiary of the well-established Better Business Bureau, administers the BBBOnLine seal, which promotes ethical business standards and voluntary self-regulation. While it promotes the idea that companies using this seal are good citizens, the program does not specifically address privacy and security online. It does require, however, that the company be in business for at least one year before being eligible to receive the seal. TRUSTe is also administered by an organization that focuses on promoting online privacy.

The role of the seal on a company's Web site is to reassure consumers that the company follows the set of self-regulation rules established by TRUSTe for the collection and use of private and personal information.

Table 1. Comparison of Some Web Site Seals

	AICP Web Trust	BBBOnLine	TRUSTe
Fee?	Yes (High)	Yes (Low)	Yes (Low)
Policies	Web site must be examined Thoroughly before seal can be affixed.	Web site must follow BBB advertising ethics and policies.	Web site must agree to site compliance reviews.
Disclosure Required	Yes; Business Practices, transaction integrity, and information protection must be disclosed.	No	Yes; Easily understandable and easy to find privacy statement.
Consumer redress	Options for redress must be disclosed.	Promptly handle consumer complaints; agree to binding arbitration; mechanisms for complaints provided.	Promptly handle consumer complaints; mechanisms for complaints provided.

(Source: Slyke, Craig Van, and Belanger, France (2008), "E-Business Technologies: Supporting the Net-Enhanced Organization," John Wiley & Sons, Inc.)

All three seals attempt to embody fair information practices similar to those supported by the U.S. FTC, U.S. Department of Commerce, and other industry associations, such as the Online Privacy Alliance (www.privacyalliance.org). For instance, in order to be TRUSTe compliant, the Web site must agree to the program principles, and abide by the TRUSTe's oversight and resolution procedures. "The program principles state that a privacy policy must be displayed on their site that clearly states what personally identifiable information is collected. The principles also require that users consent to how the data is used and shared. The site must also have adequate security measures to safeguard customer information. The oversight procedures include "seeding" user information to see whether Web sites are complying with their stated policies"[27]. Complaints are dealt with under a resolution process that could potentially escalate from TRUSTe mediation, to onsite compliance reviews by official auditors such as PricewaterhouseCoopers, to referral to the appropriate government agency. The other two seals outline similar principles, although BBBOnline does not have an oversight procedure, and AICPA Web-Trust has no oversight or complaint procedure. In summary, it appears that TRUSTe and BBBOnLine offer a minimal baseline of assurance that consumers' personally identifiable information is handled appropriately. Likewise, their privacy seals can be obtained at a minimal cost. WebTrust, however, offers a much greater amount of assurance that consumers' personally identifiable information is handled appropriately, but at what is assumed to be a much greater cost[8]. How important consumers perceive the protection of their personally identifiable information to be will determine to what extent the privacy seal program market grows and which type of privacy seal program flourishes.

To encourage privacy on the Web, several organizations have set up Web site certifications and privacy seals, and many businesses have posted one or more of these seals on their Web sites. TRUSTe is by far the most popular Web privacy seal. By 2001, fewer than 3000 e-commerce sites had the seal of approval of any of these organizations. TRUSTe has awarded some 2000 licenses since its 1997 inception, while BBBOnLine has passed out 727 seals since launching last year. WebTrust is considered the most stringent of the three programs. However, due to its costly fees and strict standards, WebTrust had awarded only two seals by 2001. At year-end 2003, the websites of more than 3,500 organizations displayed the TRUSTe seal, including Netscape, IBM, Yahoo, Microsoft, AOL Time Warner, Adobe, and Disney. Another popular program is the Better Business Bureau's (BBB) "Online Privacy Program" (with seals on 706 company sites as of April 2003). The AICPA also has an Online Privacy Program (and Principle) as part of its Web Trust seal program. Several surveys revealed that the public is unimpressed with these seals of approval. Cost may explain why, as of October 2004, CPA Web Trust has only approximately 40 recipients, while TRUSTe has around 1300 and BBBOnline around 600. Notable seal recipients include America Online, AT&T, Bell Canada, IBM, Intel, Microsoft, and Hewlett-Packard.

Two of the three organizations' privacy seal programs (TRUSTe and BBBOnLine) are very similar including: (a) They are both non-profit organizations, (b) The process to obtain their privacy seals relies heavily on self-assessments; (c) Consumer complaints are handled within the organization and is free; (d) Their cost structures for obtaining a privacy seal are both based upon total revenue and total potential vendor costs are similar ($6,999 for TRUSTe versus $6,000 for BBBOnLine). WebTrust, on the other hand: (a) Is obtained through WebTrust providers which are for-profit entities (typically, CPA's); (b) Relies heavily on a thorough examination by the WebTrust provider; (c) Handles consumer complaints through an organization external to the WebTrust program; (d) Does not publish its cost structure since it varies from customer to customer depending on the specific arrangement between the WebTrust provider and the requesting company[26].

Critics have pointed out that organizations sponsoring these privacy seals are largely self-regulated. Another problem is confusion about privacy seals and what they mean. The BBB's "Online Reliability Program" sounds like it might be a privacy seal, but it has nothing to do with privacy protection. The BBB program that specifically addresses online privacy is called the "BBB Online Privacy

Program". In practice, the seal assurance programs have been less than perfect. The main criticism of these seals is the assurance organizations, such as TRUSTe, AICPA, and BBB, have no real power to deal with abuses, although TRUSTe for one has shown its willingness to challenge abuses, such as its pursuit of bankrupt e-tailer Toysmart.com that attempted to sell its customer database [28]. Since then, however, a number of Web sites have included a disclaimer in their privacy statement that allows the sale of customer data should all or part of the business be sold in the future. Such Web sites include Amazon and eBay. In order for privacy seals to be effective, B2B Web sites must display them more prominently so that online consumers can begin to recognize these graphic images and understand their function. Industry groups, such as, the On-Line Privacy Alliance have vigorously lobbied against increased government regulation in this area, claiming that the current self-regulated environment is adequate[17]. Critics have questioned the ability of these groups to properly monitor the industry and suggest that the privacy seals may be no more than marketing ploys to lull consumers into a false sense of security.

A cornerstone of the TRUSTe, BBBOnLine and WebTrust privacy programs is their branded online seal, or "Trustmark." The seals are displayed by websites that adhere to these organizations' established privacy requirements and agree to comply with oversight and consumer dispute resolution processes. A displayed trust mark signifies to online users that the website will openly share, at a minimum, what personal information is being gathered, how it will be used, with whom it will be shared and whether the user has an option to control its dissemination. Based on such disclosure, users can make informed decisions about whether or not to release their personally identifiable information to the website.

6. The Privacy Protection: Government Regulations (Legislation) Scenario

Globalization is a noteworthy factor behind the increased attention being paid to privacy. To do business around the world, companies have had to adapt to local cultures and regulations. On the surface, it seems obvious that privacy rights should be protected, but the common standard applied differs from country to country[29]. For example, privacy laws in the European Union are much stricter than those in the United States, which implies that U.S. companies who want to do business in the European Union must follow the E.U. standard. In Nordic countries, which are not all in the EU, similar laws exist which acknowledge the use of a personal identity code for each person in an ID card scheme.[1]. In Europe, individual countries develop on enact their own laws, based on the Directive, which hold to the principles, but may differ in detail. For example, German law does not permit any unsolicited direct mail communications, which are permitted in the UK, although consumers can request not to receive these. Similar laws exist in many countries and are documented by Privacy International (www.privacyinternational.org). However, the issue is not that simple.

The claim to privacy is protected in the U.S., Canadian, and German constitutions in a variety of different ways and in other countries through various statutes. Several other countries such as UK, Spain, Switzerland, Sweden, Australia, China (Taiwan), Thailand, Singapore, to name a few, have enacted laws to protect data and privacy rights [30]. Sweden passed legislation that restricts how Web sites can use cookies[Bayardo and srikant]. Privacy rules, therefore, vary widely throughout the globe, and navigating this thicket of laws is critical to international commerce.

Legislatures across the globe have taken notice and tried to minimize invasion of privacy. On the surface, it seems obvious that privacy rights should be protected, but the common standard (law) applied differs from country to country. Privacy rules vary widely throughout the globe, and navigating this thicket of laws is critical to international commerce. We are surveying below the privacy legislation scenario prevalent in Australia, the United States (U.S.), the European Union (E.U.), Canada, Japan and India. It is expected that a growing number of countries will adopt privacy laws to foster e-commerce.

6.1. Australia

Australia enacted a Privacy Act quite early on in 1988, which regulates the handling of personal information by federal government agencies and also provides some protection for the use of credit information and tax file numbers by the private sector as well as the public sector. Other commonwealth laws contain privacy provisions which regulate use of data-matching, criminal convictions, and Medicare information. Similar legislation was expected for the private sector. However, the government announced its preference for voluntary self-regulation as in the US to address private sector information handling issues "because of concerns about the costs of compliance with legislatively based scheme"[31].

6.2. The United States of America (USA)

In the United States, the claim to privacy is protected primarily by the First Amendment, which guarantees freedom of speech and association. Fourth Amendment provides protection against unreasonable search and seizure of one's personal documents or home, and the guarantee of due process of law. The Federal Trade Commission ("FTC") supports industry self-regulation for online privacy. While FIPs do not themselves carry the force of law, they provide a set of principles for legislation and government oversight[11]. In this way they are similar to the Universal Declaration of Human Rights, in which Article 12 states the principle that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone

has the right to the protection of the law against such interference or attacks," but leaves the specific legal implementations of those ideals in the hands of individual nations. The five FIPs the FTC adopted in 1973—notice/awareness, choice/consent,access/participation, integrity/security, and enforcement/redress—are a subset of the eight protections ensconced in the Organization for Economic Co-operation and Development ("OECD") Guidelines on the Protection of Privacy and Trans-border Data Flows of Personal Data[19]. The FIP of notice underlies the notion of privacy policies, which are mechanisms for companies to disclose their practices. The FTC was concerned that the FIP of notice/awareness was not faring well on the new Internet: consumers did not know where their data went or what it might be used for.

The claim that privacy is protected in the U.S. is based on a regime called "Fair Information Practices (FIP)". FIP is a set of principles governing the collection and use of information about individuals; they are based on the notion of "mutuality of interest" between the record-holder and the individual. The individual has an interest in engaging in a transaction, and the record-keeper—usually a business or government agency—requires information about the individual to support the transaction. Once gathered, the individual maintains an interest in the record, and the record may not be used to support other activities without the individual's consent. In 1998, The Federal Trade Commission (FTC) restated and extended the original FIP to provide guidelines for protecting online privacy. Table-2 describes the FTC's "Fair Information Practice Principles." In spite of these recent developments, many online businesses, especially in emerging markets, still collect information without consumers' knowledge and consent and do not satisfy the FTC's five principles of sound privacy policies[7].

There is no comprehensive federal privacy statute that protects personal information. Instead, a patchwork of federal laws and regulations govern the collection and disclosure of personal information and has been addressed by Congress on a sector-by-sector basis[8]. Federal laws and regulations extend protection to consumer credit reports, electronic communications, federal agency records, education records, bank records, cable subscriber information, video rental records, motor vehicle records, health information, telecommunications subscriber information, children's online information, and customer financial information. Some contend that "this patchwork of laws and regulations is insufficient to meet the demands of today's technology"[3].

The FTC's FIP are being used as guidelines to drive changes in privacy legislation. In July 1998, the U.S. Congress passed the Children's Online Privacy Protection Act (COPPA), requiring Web sites to obtain parental permission before collecting information on children under the age of 13. The FTC has recommended additional legislation to protect online consumer privacy in advertising networks, such as, DoubleClick, which collect records of consumer Web activity to develop detailed profiles that are then used by other companies to target online ads[32]. Other proposed e-commerce privacy legislation is focusing on protecting the online use of personal identification numbers, such as social security numbers, limiting e-mail, and prohibiting the use of "spyware" programs that trace online user activities without the users' permission or knowledge.

Table 2. Federal Trade Commission's Fair Information Practice (FIP) Principles

Notice/Awareness (core principle):	Web sites must disclose their information practices before collecting data. Includes identification of collector, uses of data, other recipients of data, nature of collection (active/inactive), voluntary or required, consequences of refusal, and steps taken to protect confidentiality, integrity, and quality of data.
Choice/Consent (core principle):	There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties.
Access/Participation:	Consumers should be able to review and control the accuracy and completeness of data collected about them in a timely, inexpensive process.
Security:	Data collection must take responsible steps to assure that consumer information is accurate and secure from unauthorized use.
Enforcement:	There must be in place a mechanism to enforce FIP principles. This can involve self-regulation, legislation giving consumers legal remedies for violation, or federal statutes and regulations.

Table-3 describes the major U.S. federal statutes that set forth the conditions for handling information about individuals in such areas as credit reporting, education, financial records, newspaper records, and electronic communications. Privacy protections have also been added to recent laws deregulating financial services and safeguarding the maintenance and transmission of health information about individuals. However, The Privacy Act of 1974 has been the most important of these laws, regulating the federal government's collection, use, and disclosure of information. At present, most U.S. federal privacy laws apply only to the federal government and regulate very few area of the private sector[8].

In the U.S., while there has been substantial interest in data privacy issues, efforts have been piecemeal. The Privacy Act, 1974 regulates federal government record keeping, and there are statutes, which regulate specific personal data, such as credit reports, bank records, and videotape rental records. In general, self-regulation by the information industry, along with technological privacy protection measures, has been favoured. However, a number of information industry groups have issued voluntary codes of conduct and guidelines for fair

information collection by their members. In some cases, mandatory codes of conduct have recently been adopted.

Table 3. Federal Privacy Laws in the United States

Central Federal Privacy Laws	Privacy Laws Affecting Private Institutions
Freedom of Information Act, 1966	Fair Credit Reporting Act of 1970 Family Educational Rights and Privacy Act, 1974
Privacy Act, 1974	Rights to Financial Privacy Act, 1978
Electronic Communications Privacy Act, 1986	Privacy Protection Act, 1980
Computer Matching and Privacy Protection Act, 1988	Electronic Communications Privacy Act, 1986; Cable Communications Policy Act of 1984
Computer Security Act, 1987	Video Privacy Protection Act, 1988
Federal Managers Financial Integrity Act, 1982 Driver's Privacy Protection Act of 1994 E-Government Act of 2002	Children's Online Privacy Act, 1998 Health Insurance Portability and Accountability Act of 1996 Financial Modernization Act (Gramm-Leach-Bliley Act) of 1999.

(Source: Laudon, K.C. and Laudon, J.P. "Management Information Systems: Managing the Digital Firm," Pearson, 12 edition, 2012)

For example, mandatory guidelines were issued by the Individual Reference Services Group (IRSG Group), which includes companies, such as Leis-Nexis, who sell personal data via their online services; the three credit reporting companies, Equifax, Experian, and Trans Union; and other companies that sell personal information[28]. The IRSG guidelines require that "annual compliance audits be conducted by independent third parties," and the guidelines prohibit members that are information suppliers from selling data to those found violating the guidelines.

Most recent privacy concerns have cantered on the Internet. Privacy laws in the U.S. are significantly more lax, especially with regard to non-government organizations. Further, governments are significantly more limited in the collection and dissemination of private data than are private businesses. Law does not limit businesses that are not financial institutions or medical organizations. The U.S. approach has been to expect businesses to impose self-regulation on data collection through the Internet. Whether or not this has happened to any significant degree is questionable. The U.S. government, however, has stepped in despite limitations, and Congress has adopted some laws to curb violation of privacy. To strengthen the foundation of commercial data privacy in the United States, we recommend "the consideration of the broad adoption of comprehensive Fair Information Practice Principles (FIPPs)." This step may help close gaps in current policy, provide greater transparency, and increase certainty for businesses. The principles that constitute comprehensive statements of FIPPs provide ample flexibility to encourage innovation[8].

6.3. The European Union

One of the first attempts to legislate on privacy matter came in the late 1960s from the Council of Europe, which sought to ensure that the European Convention on Human Rights conferred on individuals the right to protect personal information. Several Member states of the E.U. subsequently passed legislation protecting the fundamental rights of individuals, and in particular, their right to privacy from abuse resulting from data processing (i.e. the collection, use, the storage, etc.)

Historically, Europeans have been much more concerned about privacy issues than Americans, and most European countries have enacted very specific & strict laws designed to protect their citizens. Unlike the US, European countries do not allow businesses to use personally identifiable information without consumers' prior consent. The European Union (E.U.) adopted the "Directive on Data Protection (Directive 95)" in October 1998, which limits any collection and dissemination of personal data. In the E.U., a directive is framework of law; each member nation must legislate more restrictive law; but not a more relaxed one. The directive imposes the same rules in all 30 plus member countries of the E.U. These countries have passed laws that reflect Directive 95; some are even more restrictive. The directive provides that no one collect data about individuals ("subjects") without their permission; that the collecting party notify the subject of the purpose of the collection; that the maintainers of the data ask for the subject's permission to transfer the subject's data to another party; and that upon a proper request from the subject, data about the subject be corrected or deleted. The directive prohibits the transfer of personal data from E.U. countries to any country that does not impose rules at least as restrictive as those of the directive.

Companies operating from the E.U. countries are barred by law from trading with the U.S. companies that do not abide by the European privacy laws. To overcome the problem, the U.S. government offered to create a list of U.S. companies that voluntarily agree to obey these laws. This list is referred to as a "Safe Harbor"[33]. A safe harbor is a legal provision that provides protection against prosecution. Now, European businesses have a protection against prosecution if they deal with U.S. businesses that signed up as members of the arrangement. This arrangement is an official agreement between the United States and the European Union. A European company can look up a U.S. business on the list, which is published online, to see if that business participates. U.S. organizations must comply with the seven safe harbor principles, as spelled out by the U.S. Department of Commerce. However, months after the safe harbor was established very few U.S. companies had signed up.

The European Union Privacy Directive has important implications both for companies engaged in e-commerce and for multinational corporations with offices in E.U. countries. It is based on the idea that collecting and using

personal information infringes on the fundamental right to privacy. The directive covers a wide variety of data that might be transmitted during the normal course of business. Although the directive officially covers only personal data, it defines that to mean "any information relating to an identified or identifiable natural person". Organizations that want to trade in E.U. countries must guarantee that personal information is processed fairly and lawfully; that it is collected for specified, legitimate purposes; is accurate and up-to-date; and is kept only for the stated purpose and nothing more.

Substantial rights are given to individuals regarding the information that organizations possess about them. Individuals must have access to any personal information collected, and any mistakes must be corrected. More important, individuals may prohibit the use of their personal information for marketing purposes. One recent study suggested that E.U. Privacy Directive impacts numerous parts of an organization's records. A partial list of business includes human resources, call centres, customer service, payment systems, sale of financial services to individuals and business, personal and corporate credit reporting, as well as accounting and auditing. All forms of transmission are covered, including electronic and hard copy. In European Union's initial analysis, the U.S. was not listed among those countries seen as adequately protecting the privacy of personal data. Now, over 350 organizations are on the Department of Commerce's "Safe Harbor" List.

6.4. Canada

Canada has various regulations at the federal and provincial level regulating government information handling and has also some sector specific legislation. For example, Canada's Federal Bank Act was recently amended to require that financial institutions adopt privacy codes, and most of the provinces have statutes regulating credit-reporting practices. As in the U.S., industry groups have established model codes of conduct. For example, the "Canadian Direct Marketing Association" has compulsory guidelines that require members to ask permission before sending marketing e-mail, and to inform visitors to their websites as to what personal information is being collected, and how it will be used. Meanwhile, the Standards Association has voluntary codes of practice for use by businesses.

The Canada passed "The Personal Information Protection and Electronic Documents Act," in 2000. The act provides that Canadians have the right to know why a business or organization is collecting, using, or disclosing their personal information, such as name, age, medical records, income, spending habits, DNA code, marital status, etc[35]. They have the right to check their personal information and correct any inaccuracies. According to the act, businesses must obtain the individual's consent when they collect, use, or disclose personal information, except in some circumstances, such as information needed for an investigation or an emergency where lives or safety are at risk.

Like members of the European Union, Canada established a privacy commissioner[36]. The privacy commissioner is an officer of Parliament, reporting directly to Parliament. Under the act, individuals may complain to the privacy commissioner about how organizations handle their personal information. The commissioner functions as an ombudsman; initiates, receives, investigates, and resolves complaints; conducts audits; and educates the public about privacy issues. He or She has two sets of powers—the power of disclosure, which is the right to make information public; and the power to take matters to the Federal Court of Canada, which can in turn order organizations to stop a particular practice and award substantial damages for contravention of the law.

The act contains a set of fair information principles. These principles are based on the Canadian Standards Association's Model Privacy Code for the Protection of Personal Information. The code was developed with input from businesses, government, consumer associations, and other privacy stakeholders. The act applies to the collection, use, and disclosure of personal information by organizations during commercial activities both with brick-and-mortar and online businesses. Personal information is any information about an identifiable individual whether recorded or not. Organizations include associations, partnerships, persons, and trade unions. The term "commercial activity" includes the selling, or leasing of donor, memberships, or other fundraising lists.

6.5. Japan

Japan also has a privacy act, which regulates government data collection practices, but with regard to private sector information handling, the government has preferred voluntary guidelines issued by the government ministries rather than legislation. These include the Ministry of Finance, which issued guidelines in March 1986 on Information Handling relating to the Establishment or Use of Credit Information Agencies by Financial Institutions; the Ministry of International Trade and Industry, which issued guidelines in March 1986 on Consumer Credit Information Management; the Ministry of Posts and Telecommunications, which issued Guidelines on Personal Data Protection in Telecommunications in September 1991, and which issued Guidelines on the Protection of Subscriber Personal Data for the Audience of Broadcast Services in September 1996.

Japan also recently passed its first omnibus privacy law, which *Professor Alan F. Westin* at Privacy and American Business (P&AB) accurately describes as "a 'middle way' between the industry-sector-based privacy laws of the U.S. and the comprehensive data protection laws of the European Union." The P&AB offers the Guide to Consumer Privacy in Japan and the New Japanese Personal Information Protection Law to explain the data-protection climate in Japan and help companies navigate the legislation[37].

6.6. India

The fundamental rights, as engrained in the Constitution of India, come closest to protecting an individual's privacy and his freedom of expression. The right to freedom of speech and expression, and the right to privacy are two different sides of the same coin. One person's right to know and be informed, however, may violate another's right to be left alone. Just as the freedom of speech and expression is vital for the dissemination of information on matters of public interest, it is equally important to safeguard the private life of an individual to the extent that it is unrelated to public duties or matters of public interest. The law of privacy, therefore, endeavours to balance these two competing freedoms.

The freedom under Article 19(1)(a) means the right to express one's convictions and opinions freely, by word of mouth, writing, printing, picture, or electronic media. The freedom of expression includes the freedom of propagation of ideas, their publication and circulation and the right to answer the criticism levelled against such views, the right to acquire and import idea and information about matters of common interest. Moreover, a citizen is eligible to safeguard the privacy of his family, marriage, procreation, motherhood, child bearing, education, etc. A citizen's right to privacy is implicit in the right to life and liberty guaranteed under Article 21 of the Constitution, but is subject to the restrictions on the basis of compelling public interest[16, 27].

The right to privacy has been interpreted as an unarticulated fundamental right under the Constitution of India. The growing violation of this right by the State on grounds (that are not always bona fide) encouraged the Indian Judiciary to take a pro-active role in protecting this right.. The following case law outlines the principles of the law of privacy as prevalent in India. A landmark judgment with respect to this issue is *Kharak Singh v. State of U.P.5* The Supreme Court held that the right of privacy falls within the scope of Article 21 of the Constitution and therefore concluded that an unauthorized intrusion in to a persons home and disturbance caused to him is in violation of personal liberty of the individual[30]. Similarly, in R. Rajagopal v. State of Tamil Nadu, the Supreme Court was of the opinion that the right to privacy as an independent and distinct concept originated in the field of the court of law. This right has two aspects namely: (a) general law of privacy, and (b) constitutional recognition given to such right. The right of privacy, however, is not enumerated as a Fundamental Right but has been inferred from Article 21 of the Constitution. Any right to privacy must encompass and protect the personal intimacies of the home, the family, marriage, motherhood etc. In Mr. X v. Hospital Z, the Supreme Court was seized on an issue concerning an AIDS patient and the right to privacy and confidentiality regarding his medical condition, and the right of the lady to whom he was engaged to lead a healthy life. The Supreme Court was of the opinion that her marriage and consequent conjugal relations would endanger the life of the fiancée with the AIDS victim, and consequently, she was entitled to information regarding the medical condition of the man she was to marry. In the recent case of Sharda v. Dharampal, the Supreme Court was confronted with the issue whether subjecting a person to a medical test is in violation of Article 21 of the Constitution. The Court outlined the concept of the law of privacy in India and was of the opinion that the right to privacy in terms of Article 21 of the Constitution is not an absolute right. The Supreme Court quoted the previous decision of the same Court in Govind v. State of Madhya Pradesh, where it was held, "Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right, that fundamental right must be subject to restriction on the basis of compelling public interest." In conclusion, a citizen is eligible to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing, education, etc.

As regards the state-led initiatives in India, the Andhra Pradesh has proposed a "Data Processing (Special Contracts) Act" in line with the global standards. Accordingly, the Andhra Pradesh Data Protection law seeks to:

- Protect sensitive consumer related information being processed or stored by the BPO/ITES companies or their business associates.
- Provide a data protection and consumer privacy regime similar to the one in European Union, the UK, and the US.
- Enable the companies out locating to AP to enforce their agreements with regard to privacy/protection of sensitive information.
- Provide an avenue for re-dressal of grievances and resolution of disputes.
- Enable the foreign companies to proceed against their partners/associates in case of violation of privacy rules.

The Andhra Pradesh led initiative is the first of its kind in the country, and a move that will comfort overseas clients as to the privacy concerns over the processing of private data by third-party service players in the state. Most overseas clients protect the privacy of personal data being processed in India by their preferred providers through the traditional contract route.

Protection afforded to personal data in India may not be considered adequate, as compared to the global standards set by various governments and institutions across the globe. However, there are distinct differences in the concept of privacy that we understand in India vis-à-vis the approach of the Western countries. Generally, Indian society and culture is one of openness, and the concept of protecting one's identity from society is rather alien. However, this is not the position in Western nations, where personally identifiable data has been widely used to target minorities, fight wars, used for telemarketing purposes, committing financial frauds and scandals, and so on. However, some market players in India have already started misusing the general openness of Indian society to market credit cards, sell personal information, send Spam e-mails, conduct illegal background checks on persons, etc. In this context, it

would be necessary to balance the unique nature and needs of Indian society with the privacy and protection principles as expounded by the Indian Constitution. From an understanding of the Indian legal scenarios, it can be concluded that there exists no Indian legislation that covers the protection of rights of privacy, which can be interpreted in the realm of transactions between individuals and corporations or between two individuals over the Internet [16].

7. Conclusions

Companies are entering an era of information transparency of increasingly activist stakeholders, the growing influence of global markets, the spread of communications technology, and a new customer ethic demanding openness, honesty and integrity from companies. Consequently, risks to privacy are greater, and safeguarding sensitive information has become more significant, and more difficult to do. A serious concern for individual privacy is growing right alongside the growth of e-commerce/business[2]. Among the companies given high marks by privacy advocates for making data protection a priority are Dell, IBM, Intel, Microsoft, Procter & Gamble, Time Warmer and Verizon. Some of these companies, which had in the past been plagued by security leaks in its operating system and e-commerce programs, have now embraced hard-line privacy stances only after experiencing first-hand the potential damages to their businesses that privacy breaches can inflict. As stated earlier, many people feel that consumer profiling violates their privacy[24]. Hence, legislators all over the world have taken notice and tried to minimize invasion of privacy.

The online industry has preferred 'self-regulation' to privacy legislation for protecting consumers. In 1998 the online industry formed the "Online Privacy Alliance" to encourage self-regulation to develop a set of privacy guidelines for its members[35]. The alliance's guidelines call on companies to notify users when they are collecting data at Web-sites to gain consent for all uses of that data, to provide for the enforcement of privacy policies, and to have a clear process in place for receiving and addressing user complaints. The group is promoting the use of online "seals" such as that of TRUSTe, certifying Web sites adhering to certain privacy principles. Similarly, members of the advertising network industry have created an additional industry association called "Network Advertising Initiative (NAI)" to develop its own privacy policies to help consumers opt-out of advertising network programs and provide consumer redress from abuses[12]. In general, however, most Internet businesses do little to protect the privacy of their customers and consumers do not do as much as they should to protect themselves.

Privacy seals and government regulations are two leading forces pushing for more and better privacy disclosures on Web sites. Both trust seals and government regulations were highlighted in this paper. Trust seals promote privacy in the form of self-regulation by industry, while government regulation takes the form of litigation, forcing companies into better privacy practices. No doubt, privacy laws vary throughout the globe. In the US, Canada, and Germany, rights to privacy are explicitly granted in, or can be derived from, founding documents such as constitutions, as well as in specific statutes[35]. In fact, the E.U. has adopted very strict laws to protect its citizens' privacy, in sharp contrast, to 'lax-attitude' and 'self-regulated' law of the U.S. To avoid disruption of business with the E.U. and possible litigation, the U.S. businesses can sign on the "Safe harbor" arrangement. An attempt was made to summarize the privacy legislation scenario prevalent in the select countries, such as, Australia, Canada, the EU, the USA, Japan and India. However, protection afforded to personal data in India may not be considered adequate, as per Western countries standards. It is hoped that a growing number of countries will adopt privacy laws to foster e-commerce[34]. In nutshell, the privacy scenario in the United States and the European Union remains at best a gradual work-in-progress, and how soon it will attain perfection only future will tell us.

During the last several years, dozens of bills concerning the protection of privacy have been introduced at both the federal and state levels. Even without new federal regulation, the FTC is becoming more active regarding privacy protection on the Internet. Recently, Microsoft has launched a project called "Trustworthy Computing," under which Chairman Bill Gates has challenged the company "to be certain that availability, security, privacy and trustworthiness are the key components of every software and service products the company develops"[17].

Although many U.S. companies initially fought consumers' efforts to make companies pay attention to privacy, almost no major businesses today feel they can completely neglect data protection rules. Thus, all businesses must now take consumer privacy seriously. This will require investing resources to secure databases and Web sites. Organizations should also determine if their insurance covers lawsuits that may arise over privacy violation issues. At present, most of the organizations with an online presence have established online privacy statements or policy certifying that they comply with the legislated privacy standards.

There is no single solution to the erosion of privacy in cyberspace; no single law that can be proposed or single technology that can be invented to stop the profilers and survelliants in their tracks. Indeed, the battle of privacy must be fought on many fronts—legal, political, and technological—and each new assault must be vigilantly resisted as it occurs[38]. Technology alone cannot address all the concerns surrounding a complex issue like privacy. The total solution must combine laws, societal norms, markets, and technology. However, by advancing what is technically feasible, we can influence the ingredient mix and improve the overall quality of the solution.

REFERENCES

[1] Laudon, K.C. and Laudon, J.P. (2012), "Management Information Systems: Managing the digital firm," Pearson, 12 edition.

[2] Slyke, C.V., and Belanger, F. (2012), "E-Business Technologies: Supporting the Net-Enhanced Organization," John Wiley & Sons, Inc.

[3] Stevens, G. (2011) "Privacy protections for personal information online," April, Congressional Research Service Report 7-5700, available at www.crs.gov.

[4] UNESCO (2011) "Global Survey on Internet Privacy: Calls for proposals," June, 2011. Available electronically at www.unesco.org.

[5] Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, A. (2011) "The Effect of online privacy information on purchasing behavior: An experimental study," Information Systems Research, Volume 22, No. 2, June, pp. 254-268.

[6] Punch, L. (2000), "Big Brother Goes Online," Credit Card Management 13(3): 22-32.

[7] Wirtz, J., Lewin, M.O. and Williams, J.D. (2007), "Causes and Consequences of conumer online privacy concern," International Journal of Service Industry Management, Volume 18, No. 4, pp. 326-348.

[8] The Department of Commerce, Internet Policy Task Force Report (2010), "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," available at www.ntia.doc.gov.

[9] Fuchs, C. (2011), "The political economy of privacy on Facebook," The internet & Surveillance, Research paper 9 series, Vienna, Australia. Available at www.uti.at.

[10] Debatin, B., Lovejoy, J.P., Horn, M.A. and Hughes, B.N. (2009), "Facebook and Online Privacy: Attitudes, behaviors and unintended consequences," Journal of Computer-Mediat ed Communications, Volume 15, pp. 83-108.

[11] Aleecia, M. McDonald and Cranor, L.F. (2008) "The cost of reading privacy policies," Information System: A journal of law and policy for the information society. Available at www.is-journal.org.

[12] Chaffey, D. and White, G. (2011), "Business Information Management," Prentice-Hall, Financial Times, 2 edition.

[13] Turban, E., Leidner, D., Mclean, E., and Wetherbe, J. (2008) "Information Technology Management: Transforming organizations in the digital economy," 6 edition, John Wiley & Sons, Inc.

[14] Kalakota, R. and Whinston, A.B. (1996), "Frontiers of Electronic Commerce," Reading, Mass, Addison-Wesley.

[15] Hoffman, D., Novak, T.P. and Peralta, M. (1999), "Building Consumer Trust Online, " Communications of the ACM, 42 (4): 80-85.

[16] Bhasin, M.L. (2005) "Challenges of Guarding Privacy: Practices Prevalent in Major Countries," The Chartered Accountant Journal, November 2005, published by The Institute of Chartered Accountants of India, New Delhi, pp. 739-749.

[17] Federal Trade Commission (2010), "Protecting Consumer Privacy in an Era of Rapid Change: A proposed framework for business and policymakers," December. Available at www.ftc.org.

[18] Haag, Cummings, McCubbrey (2004), "Management Information Systems for the Information Age," Mc Graw-Hill Irwin, Fourth edition.

[19] Organization for Economic Co-operation and Development (1980), "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," available at http://www.oecd.org.

[20] Branscum, D. (2000), "Guarding On-Line Privacy," Newsweek 135 (23): 77-78.

[21] Stair, R. and Reynolds, G. (2006), "Fundamentals of Information Systems," Third Edition, Thomson Course Technology, USA.

[22] Harris Interactive (1999), "IBM Multinational Consumer Privacy Survey," Study Commissioned by IBM Global Services, October 1999. Available at www.ibm.com.

[23] Pew Internet and American Life Project (2000), "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," available at: http://www.pewinternet.org/reports/toc. asp?Report=19.

[24] Goldberg, I. (2007), "Privacy enhancing technologies for the Internet III: Ten years later," Digital Privacy: Theory, Technologies, and Practices, Alessandro Acquisti, Stefanos Gritzalis, Costos Lambrinoudakis, Sabrina di Vimercati, editors. Auerbach, December 2007.

[25] Tang, Z., Hu, Y.J. and Smith, M.D. (2007), "Gaining Trust through online Privacy Protection: Self-regulation, mandator y standards, or caveat emptor," Heinz College Research paper 49, available at www.repository.cmu.edu/heinzworks/ 49.

[26] Markert, B.K. (2002) Comparison of Three Online Privacy Seal Programs, GSEC Practical Assignment Version 1.2e, SANS Institute,

[27] Ahmad, T. (2009), "Right of Privacy: Constitutional Issues and Judicial Responses in USA and India, particularly in Cyber age," available at www.ssrn.com/abstract=1440665.

[28] Culnan, M. (2002), "Georgetown Internet Privacy Policy Study," McDonough School of Business, Georgetown University, see http://www.msb.edu/faculty/culnan/gippshome.html.

[29] Green, H., Yang, C. and Judge, P.C. (1998), "A Little Privacy, Please," Business Week 3569: 98-99.

[30] Shah, A. and Zacharias, N. (2001), "Right to privacy and data protection," Nitin Desai Associates, Mumbai.

[31] Privacy Working Group of the National Information and Infrastructure Task Force (1995), "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information," 6 June. Available at: http://nsi.org/Liberty/Comm/niiprivp.htm.

[32] Krill, Paul (2002), "DoubleClick Discontinues Web Tracking Service," InfoWorld, 9 January, available at: http://www.infoworld.com/articles.

[33] EOS-Privacy & Data Protection Task Force (2010), "EU policies on privacy and data protection and their impact on the implementation of security solutions," September, European Organization for Security, pp.1-17.

[34] European Commission (2011), "Workshop on Privacy protection and ICT: Research ideas," Workshop report, September 21, Brussels.

[35] Bowman, L.M. (2001), "House Pulls Carnivore into the Light," ZDNet News (23 July): http://zdnet.com/2100-1106-270406.html.

[36] Oz, Effy (2002), "Foundations of E-Commerce," Prentice Hall, NJ.

[37] Laudon, K.C and Traver, C.G. (2003), "E-commerce," 2nd edition, Addison Wesley, NY.

[38] Bayardo, R.J. and Srikant, R. (2003) "Technological Solutions for Protecting Privacy," Web Technologies, September, available at www.almaden.ibm.com/cs/projects/iis/hdb/Publication.