Соціально-економічні проблеми і держава
journal home page: http://sepd.tntu.edu.ua

S
E
P
D

Bhasin, M. (2016). Challenge of guarding online privacy: role of privacy seals, government regulations and technological solutions. *Socìal'no-ekonomìčnì Problemì ì Deržava*. *15* (2), 85-104.

ISSN 2223-3822

Challenge of guarding online privacy: role of privacy seals, government regulations and technological solutions

Madan Lal Bhasin

Universiti Utara Malaysia,
06010 UUM Sintok, Kedah, Malaysia
e-mail: madan.bhasin@rediffmail.com
Dr., Prof., School of Accountancy, College of Business

Article history:
Received: September, 2016
1st Revision: September, 2016
Accepted: September, 2016

JEL classification:
D82
H56
H82

UDC:
342.9
340.11

Abstract: The state of privacy in the 21st century is a worldwide concern, given the Internet's global reach. The privacy violation on the internet is a significant problem and internet users have a right to adequate 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, Japan, Hong Kong, Malaysia and Singapore. It is expected that a growing number of countries will adopt privacy laws to foster e-commerce. Accountability for privacy and personal data protection needs to be a joint effort among governments, privacy commissioners, organizations and individuals themselves.

Technology has always had the power to fundamentally transform any society's way of life. Information gathering on the Web is pervasive in large part because usage tracking and data-mining technology are deeply integrated into most Web software systems, such as tools for building online storefronts. In contrast, tools for managing data privacy are uncommon. This makes addressing user and legislative privacy concerns difficult and costly. Nevertheless, many technologies offer ways to help protect personal privacy on the Web and beyond. We focus here on emerging technologies that may become core features of future information systems and Web infrastructures. Privacy in the age of technology is quickly becoming a paradox. Privacy professionals, regulators and organizations need to work together to innovate new approaches that entrench privacy as a standard rather than an anomaly. Thus, emerging technologies can protect privacy without restricting the information flow crucial to efficient organizations.

Keywords: guarding, online privacy, trust seals, government regulation, technology-based solutions.

Бхасін М. Проблема охорони приватності в Інтернеті: роль конфіденційності, урядового регулювання і технологічних рішень / Мадан Лал Бхасін // Соціально-економічні проблеми і держава. — 2016. — Вип. 2 (15). — С. 85-104.

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 (Laudon and Laudon, 2016). 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 sale, and to make shopping, purchasing, and service more convenient for their clients. As pointed out by Slyke and Belanger (2012), "The more businesses allow access to their services and systems through the Internet, the more they are vulnerable to security breaches. 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 fueled the creation of a new tracking industry. Behavioral advertising, a form of online advertising, is delivered based on consumer preferences or interest as inferred from data about online activities. In 2015, over $122 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" (Stevens, 2011). Web sites, such as Spokeo, an online data aggregator and broker, give site visitors vast quantities of personal information. The use of social networking sites by law enforcement and government agencies, coupled with the fact that information on social networking sites can be used as evidence in trials, reinforces the importance of using restraint in posting information to your profile. Consumers and public interest groups are filing complaints to challenge the collection and use of consumer data without consumer consent or knowledge. Thus, 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, maintenance, and manipulation of personal data more possible, faster, less expensive, and more effective than manual methods (UNESCO, 2011). Recently, Swire et al., (2016) stated, "Based on a factual analysis of today's Internet ecosystem in the United States, ISPs have neither comprehensive nor unique access to information about users' online activity. Rather, the most commercially valuable information about online users, which can be used for targeted advertising and other purposes, is coming from other contexts, such as social networks and search. Market leaders are combining these contexts for insight into a wide range of activity on each device and across devices." 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. According to Slyke and Belanger (2012), "Three parties may violate the privacy of individuals – government, businesses, and employers." 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 (Tsai et al., 2011). 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 (Punch, 2000). Here, Bhasin (2007) observed "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." 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. As Wirtz, Lewis and Williams (2007) stated, "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." 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. In addition, in the online world, data collection can occur even without the knowledge of the individual, through the use of cookies. As Bhasin (2005, 2006) said, "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." As Internet Policy Task Force Report (2010) observes, "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. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it".

In today's technological world, millions of individuals are subject to privacy threats. Recently, Bhasin (2016) pointed out, "By using computer technology, companies can legally collect information about consumers, including what they buy, what medications they take, what sites on the internet they have visited, and what their credit history is. Computer software can organize this data and prepare it for sale and use by direct marketing companies, lending institutions, insurance companies, and credit bureaus." 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. Similarly, Bhasin (2015) remarked, "Facebook is the most popular 'social' networking site. Student life without Facebook 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 Facebook they enter bank and credit card information to various websites." The analysis by Fuchs (2011) shows, "Facebook'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 Facebook 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 rumors 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 (Debatin et al., 2009). 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.

According to Aleecia, McDonald and Cranor (2008), "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." 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 (Chaffey and White, 2011). Here, Bhasin (2006a, 2007) added "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 (Turban et al., 2008). They transmit information about the user and the page being viewed to a monitoring computer. Because Web bugs are very tiny, colorless, and virtually invisible, they can be difficult for unsophisticated Internet users to detect. Marketers use these Web bugs as another tool to monitor online behavior 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. 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. A security threat is defined by Kalakota and Whinston (1996) 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." 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 (Hoffman et al., 1999). 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. As Conroy et al., (2014) concluded, "Consumer product executives should consider viewing data privacy and security not just as a risk management issue, but as a potential source of competitive advantage that may be a central component of brand-building and corporate reputation." As emphasized by E&Y (2014), "In an effort to reinforce privacy protection as a top priority, it is incumbent upon organizations to: (a) Demonstrate privacy accountability and consistently apply privacy policies across functions and borders; (b) Embed privacy policies into new processes, products or services prior to launch; and (c) Create a culture that understands the fundamental importance of privacy beyond reciting the organization's policies."

3. What is Privacy?

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. 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. In this context, Bhasin (2005) observed, "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." 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. As per Federal Trade Commission (2010), "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)." 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 (UNESCO, 2011). 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. As Laudon and Laudon (2016) states, "Privacy is the "claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state." 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.

According to Haag, Cummings and McCubbrey (2014), "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." 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 (OECD, 1980). 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 (Branscum, 2000). 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 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 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 (Stair and Reynolds, 2014). 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. 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. 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. 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. 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, TRUSTe 2006). Similarly, empirical evidence suggests that consumers do not fully understand the meaning of privacy seals (Pew Internet and American Life Project, 2000). In this context, Aleecia et al., (2008) observed, "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." 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 (Goldberg, 2007). 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. According to a study done by Tang, Hu and Smith (2007), "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". 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. As Markert (2002) observes, "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."

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 instill 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.

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. According to Ahmad (2009),

"The oversight procedures include seeding user information to see whether Web sites are complying with their stated policies". 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. 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. WebTrust is considered the most stringent of the three programs. However, due to its costly fees and strict standards, WebTrust had awarded only seals to very limited 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 1,706 company sites). 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, 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.

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 statements.
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 (2012), "E-Business Technologies: Supporting the Net-Enhanced Organization," John Wiley & Sons, Inc.

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.

As Bhasin (2008) remarked, "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 (Culnan, 2002). 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 (FTC, 2010). 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 trustmark 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 (Green et al., 1998). 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. 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. As Shah and Zacharias (2001) stated, "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." Sweden passed legislation that restricts how Web sites can use cookies (Bayardo and Srikant, 2003). 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

Data privacy/protection in Australia is currently made up of a mix of Federal and State/Territory legislation. The Federal Privacy Act 1988 (Privacy Act) and its Australian Privacy Principles (APPs) apply to private sector entities, with an annual turnover of at least A$3 million, and all Commonwealth Government and Australian Capital Territory Government agencies. The Privacy Act was last amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which came in to force on 12 March 2014. The amendments significantly strengthened the powers of the Privacy Commissioner to conduct investigations (including own motion investigations), ensure compliance with the amended Privacy Act and, for the first time, introduced fines for a serious breach or repeated breaches of the APPs. Australian States and Territories (except for Western Australia and South Australia) each have their own data protection legislation applying to State Government agencies (and private businesses' interaction with them). These acts are:

– Information Privacy Act 2014 (Australian Capital Territory)
– Information Act 2002 (Northern Territory)
– Privacy and Personal Information Protection Act 1998 (New South Wales)
– Information Privacy Act 2009 (Queensland)
– Personal Information Protection Act 2004 (Tasmania), and
– Privacy and Data Protection Act 2014 (Victoria).

There is also various other State and Federal legislation that relates to data protection. For example, the Telecommunications Act 1997, the National Health Act 1953, the Health Records and Information Privacy Act 2002 (NSW), the Health Records Act 2001 (Vic) and the Workplace Surveillance Act 2005 (NSW) all impact privacy/data protection for specific types of data or for specific activities. Our focus here, however, is on the application of the Privacy Act to private sector entities. Private sector entities are referred to as 'organizations'. Under the Privacy Act/the APPs, an organization can be an: individual, body corporate, partnership, other unincorporated association, or a trust.

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. 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 honor 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 (OECD, 1980). 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.

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.

According to Internet Policy Task Force Report (2010), "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." 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. Stevens (2011) contend that "this patchwork of laws and

regulations is insufficient to meet the demands of today's technology." 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 (Krill, 2002) . 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-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, 2016

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. 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 favored. 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. 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 (Culnan, 2002). 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 centered 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. Recently, Geller (2016) concluded: "The U.S. uniquely benefitted from a 'safe harbor' provision that allowed domestic companies to self-certify that they comply with certain principles relating to: notice (when personal information is collected); the choice to opt out of such collection, and access to data collected. The safe harbor law further required such data to be kept secure; to be used only for a specified

purpose; and to be kept from being recklessly transferred to third parties. Finally, U.S. companies in the safe harbor program had to implement ways for Europeans to enforce their rights under the provision."

The United States has about 20 sector specific or medium-specific national privacy or data security laws, and hundreds of such laws among its 50 states and its territories. For example, California alone has more than 25 state privacy and data security laws. These laws, which address particular issues or industries, are too diverse to summarize fully in this volume. In addition, the large range of companies' regulated by the Federal Trade Commission ('FTC'), are subject to enforcement if they engage in materially unfair or deceptive trade practices. The FTC has used this authority to pursue companies that fail to implement reasonable minimal data security measures, fail to live up to promises in privacy policies, or frustrate consumer choices about processing or disclosure of personal data.

6.3 The European Union (EU)

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 is 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" (European Organization for Security, 2010). 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.

As Goldfarb and Tucker (2011) observed, "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 centers, customer service, payment systems, sale of financial services to individuals and business, personal and corporate credit reporting, as well as accounting and auditing. According to EU Commission (2011), "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."

According to Morando et al., (2014), "It could be argued that the European Commission proposal for a General Data Protection Regulation is far more 'Internet-aware' than its predecessor (still in force, Directive 95/46/EC), by taking into account challenges related to data exchange happening online. Several rules are being

enhanced, e.g., ex ante privacy assessment for the data controller, new requirements in terms of 'privacy by design' and 'privacy by default' measures, as well as stronger sanctions in case of breach. Moreover, new rights are being introduced, such as data portability (Article 18), for which the data subject has the right to obtain from the data controller a copy of the data, and transfer it to another information system. While the measures may be effective in some regards, there is reason to question if the underlying assumptions about user's valuation of privacy are being taken into account sufficiently." Recently, Weiss and Archick (2016), remarked, "In October 2015, the Court of Justice of the European Union (CJEU, which is also known as the European Court of Justice, or ECJ) invalidated the Safe Harbor Agreement. The CJEU essentially found that Safe Harbor failed to meet EU data protection standards, in large part because of the U.S. surveillance programs. Given that some 4,500 U.S. companies were using Safe Harbor to legitimize transatlantic data transfers, U.S. officials and business leaders were deeply dismayed by the CJEU's ruling. Companies that had been using Safe Harbor as the legal basis for U.S.-EU data transfers were required to immediately implement alternative measures. Experts claimed that the CJEU decision created legal uncertainty for many U.S. companies and feared that it could negatively impact U.S.-EU trade and investment ties. On February 2, 2016, U.S. and EU officials announced an agreement, "in principle," on a revised Safe Harbor accord, to be known as Privacy Shield; the full text of the agreement was released on February 29, 2016. U.S. and EU officials assert that the new accord will address the CJEU's concerns. In particular, they stress that it contains significantly stronger privacy protections as well as safeguards related to U.S. government access to personal data."

6.4 Canada

In Canada, there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, identity theft/ criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, and remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information. The summary below focuses on Canada's private sector privacy statutes:

– Personal Information Protection and Electronic Documents Act (PIPEDA)
– Personal Information Protection Act (PIPA Alberta)
– Personal Information Protection Act (PIPA BC),
– Personal Information Protection and Indentity Theft Prevention Act (PIPITPA) (not yet in force), and
– An Act Respecting the Protection of Personal Information in the Private Sector (Quebec Privacy Act), (collectively, 'Canadian Privacy Statutes').

The 'PIPEDA' applies: (a) to consumer and employee personal information practices of organizations that are deemed to be a 'federal work, undertaking or business' (e.g., banks, telecommunications companies, airlines, railways, and other interprovincial undertakings); (b) to organizations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted 'substantially similar' legislation (PIPA BC, PIPA Alberta and the Quebec Privacy Act have been deemed 'substantially similar'), and (c) to inter provincial and international collection, use and disclosure of personal information. PIPA BC, PIPA Alberta and the Quebec Privacy Act apply to both consumer and employee personal information practices of organizations within BC, Alberta and Quebec, respectively that are not otherwise governed by PIPEDA.

Like members of the European Union, Canada established a privacy commissioner. 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.

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 Sept. 1991, and which issued Guidelines on the Protection of Subscriber Personal Data for the Audience of Broadcast Services in Sept. 1996.

Japan also recently passed its first omnibus privacy law, which is "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 (Laudon and Traver, 2014). The Act on the Protection of Personal Information (APPI) requires business operators who utilize for their business in Japan a personal information database which consists of more than 5,000 individuals in total identified by personal information on any day in the past six months to protect personal information. Amendments to the APPI, which were passed in 2015 and go into effect no later than Sept., 2017 (the 'Amendments'), apply the APPI to all businesses in Japan, regardless of whether the business operator maintains a database of more than 5,000 individuals.

Further, the Amendments clarify the definition of personal information, add two new classes of information, and introduce new requirements for 'opt out' choice for business operators to disclosure personal information to third parties. Finally, as of January 1, 2016, the Amendments created a Privacy Protection Commission (the 'Commission'), a central agency which will act as a supervisory governmental organization on issues of privacy protection. The Amendments must be enacted no later than September 2017, so the Amendments could go into effect at an earlier date.

6.6 India

According to Bhasin (2006b), "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, endeavors 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 leveled 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," said Bhasin (2005). 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.

There is no specific legislation on privacy and data protection in India. However, the Information Technology Act, 2000 (the 'Act') contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically). India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules). Here, Bhasin (2015) stated, "The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal data, including sensitive personal information to comply with certain procedures. It distinguishes both 'personal' information and 'sensitive' personal information." In August 2011, India's Ministry of Communications and Information issued a 'Press Note' Technology (Clarification on the Privacy Rules), which provided that any Indian outsourcing service provider/organisation providing services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is not subject to collection and disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects (providers of information) when providing their services.

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. As Bhasin (2006) pointed out, "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."

6.7 Malaysia

Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on 2 June, 2010 and came into force on 15 November, 2013. The law applies to the processing of "personal data" by entities operating in Malaysia but generally does not apply to data processed entirely outside of Malaysia. Additionally, official registration requirements will extend to many classes of "data users" (those who control or authorize data processing), including those in the communications, banking and financial, insurance, health care, and other industries. "Personal data" is defined broadly within the Act as "any information in respect of commercial transactions" relating to any person "who is identified or identifiable from that information," either by itself or in combination with other data.

The law is structured around seven principles viz., 'general' (to protect legal rights or comply with legal obligations, or to protect the "vital interests" of the data subject), 'notice and choice' (extensive and detailed disclosures to affected data subjects about the use of their data, the source of the data, the kind of data being processed, the data subject's rights to access or inquire about his data, and more), 'disclosure' (disclosure must be limited by the purpose for which the data was originally collected, or, if data is disclosed to third parties, it may only be disclosed to third parties whose identity has itself been disclosed to the data subject in an appropriate notice), 'security'(data users to take "practical steps" to protect personal data from loss, misuses, modification, unauthorized or accidental access or disclosure, alteration or destruction), 'retention' (data may only be retained for so long as is necessary to fulfill the purpose for which it was collected), 'data integrity' (data user must take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-to date) and 'access' (data subjects have the right to access and correct their personal data). Further, the law imposes cross-border transfer restrictions and on the handling of personal data that is used in direct marketing. The Act imposes criminal penalties for violations, which may include fines as well as imprisonment.

6.8 Singapore and Hong Kong

Singapore enacted a new Personal Data Protection Act 2012 (No. 26 of 2012) ('Act') on 15 October 2012. The Act took effect in 3 phases:

– Provisions relating to the formation of the Personal Data Protection Commission (the 'Commission') took effect on 2 January 2013.

– Provisions relating to the National Do-Not-Call Registry ('DNC Registry') took effect on 2 January 2014.

– The main data protection provisions took effect on 2 July 2014.

In Hong Kong, the Personal Data (Privacy) Ordinance (Cap. 486) regulates the collection and handling of personal data. Enforcement is through the Office of the Privacy Commissioner for Personal Data (PCPD). The Ordinance was significantly amended by the Personal Data (Privacy) (Amendment) Bill in July 2012. Most of the amendments introduced by the Bill came into force on October 1, 2012. Two major areas of amendments, namely new restrictions against the use and provision of personal data in direct marketing, and new powers of the PCPD to provide legal assistance to persons in civil proceedings have also come into force on April 1, 2013.

7. Technological Solutions for Protecting Privacy

Council of Advisors on Science & Technology (2014) remarked, "The ubiquity of computing and electronic communication technologies has led to the exponential growth of data from both digital and analog sources. New capabilities to gather, analyze, disseminate, and preserve vast quantities of data raise new concerns about the nature of privacy and the means by which individual privacy might be compromised or protected. The technological manipulation of information refers, among others, to the integration of information (merging of documents), the repackaging thereof (translations and the integration of textual and graphical formats) and the possible altering of information (changing of photographic images) by electronic means." According to Perry (2010), "From a privacy standpoint, the most relevant cyber-security technologies are encryption and access controls. Encryption obscures digitally stored information so that it cannot be read without having the key necessary to decrypt it. Access controls provide privileges of different sorts to specified users. Access controls may also be associated with audit logs that record what files were accessed by a given user." Information gathering on the Web is pervasive because usage tracking and data-mining technology are deeply integrated into most Web software systems, such as tools for building online storefronts. In contrast, tools for managing data privacy are uncommon. This makes addressing user and legislative privacy concerns difficult and costly.

Nevertheless, many technologies offer ways to help protect personal privacy on the Web and beyond. As Bayardo and Srikant (2003) stated, "We focus here on emerging technologies that may become core features of future information systems and Web infrastructures".

Privacy policy encoding: One of the most well-known Web privacy technologies is the "Platform for Privacy Preferences" (P3P) developed by the World-Wide-Web Consortium (W3C). With P3P, an organization with a Web presence can encode its data-collection and data-use practices in a machine readable XML format known as a P3P policy. Browsers, such as Microsoft Internet Explorer and Mozilla can programmatically compare site policies against a user's privacy preferences and take actions based on the comparison. For example, the browser can block the site altogether or limit the types of cookies it will accept. The current P3P standard only provides a mechanism for Web sites to state their intentions regarding use of the personal information that they collect. Mechanisms for enforcing that sites act according to their stated policies are beyond its scope. IBM developed the Enterprise Privacy Authorization Language for encoding an enterprise's internal privacy-related data-handling policies and practices. EPAL and P3P have different goals. While P3P enables automated matching between privacy policies and user preferences, EPAL allows privacy enforcement systems such as IBM's Tivoli Privacy Manager to import and enforce the enterprise's privacy policy.

Hippocratic databases: Inspired by the privacy tenet of the Hippocratic oath Hippocratic databases include responsibility for the privacy of data they manage as a fundamental tenet, and are thus a natural solution for the problem of enforcing privacy policies. Hippocratic databases incorporate 10 fundamental privacy principles. For example, the "purpose specification" principle states that the purposes for which information has been collected should be associated with any personal information stored in the database; the "limited use" principle states that the database will run only queries that are consistent with the purposes for which the information has been collected. To illustrate how Hippocratic databases can automatically enforce these principles, consider what happens when queries, tagged with purpose, are submitted to the database. The database first checks whether the user issuing the query is among the users authorized by the privacy policy for that purpose. Next, the database analyzes the query to check whether it accesses any fields not explicitly listed for the query's purpose in the privacy policy. Finally, the database ensures that only records having a purpose attribute that includes the query's purpose will be visible to the query, thereby enforcing any opt-in or opt-out preferences.

Anonymization: While Hippocratic databases can help organizations appropriately manage and use the information they collect, some customers may prefer to prevent organizations from collecting information about them in the first place. Various anonymization technologies let Web users prevent data collection by hiding or blocking potentially identifying information, such as cookies and IP addresses. These technologies range from centralized privacy proxies, such as anonymizer.com to decentralized Web-browsing networks, such as Crowds from AT&T. In fact, companies like iPrivacy.com even allow users to anonymously purchase items by creating special arrangements with credit-card companies.

Privacy-preserving data mining: Despite their advantages, anonymization methods may prevent sites from understanding their customers and improving their products and services accordingly. As Bhasin (2006a) stated "Privacy-preserving data mining lets businesses derive the understanding they need without collecting accurate personal information. By randomizing customer data, this approach precludes the recovery of anything meaningful at the individual level but still supports algorithms that can recover aggregate information, build mining models, and deliver actionable insights to businesses." The software that online merchants use cannot determine the true age value of visitors. It has access only to the randomized values and the randomization parameters. Solely on the basis of this information, the software can reconstruct a close approximation of the true distribution. This reconstruction will only be accurate over thousands of people – not for single users – thereby preserving privacy. The merchant can then use this reconstructed distribution to build an accurate data-mining model and, for example, understand the demographics of the people who buy something versus those who don't. Or, if the goal is to give the user personalized recommendations, the merchant can ship the data-mining model to the visitor who then applies it locally.

Information sharing across private repositories: In February 2000, DoubleClick announced plans to combine consumer information it collected from Web users with information in the databases of an acquired subsidiary, Abacus Direct, raising the ire of privacy advocates and consumers alike. The message from this uproar was clear: while consumers might in some cases choose to disclose personal information, they do not want the information they disclose combined into massively detailed consumer dossiers. Once again, though, businesses have a legitimate desire to understand their customers. When the information necessary for an accurate understanding is scattered across multiple databases created for disparate purposes, the problem is to allow businesses to compile aggregate models without having to merge – and hence disclose – the individual data on which the models are built. This problem belongs in the general framework of secure multiparty computation: Given two parties with inputs x and y, secure multiparty computation computes a function f such that the two parties learn only f(x, y) and nothing else.

Cryptographic protocols: In 1986, Andrew Chi-Chih Yao showed that for any function computable by a circuit of AND, OR, and NOT gates, a cryptographic protocol exists that can perform the computation in an encrypted space and reveal only the function's output. However, such circuit-based protocols do not scale to

computations over millions of records. There are two broad strategies for improving scalability in the context of computing models or aggregate statistics. The first breaks down the function in such a way that each party can perform the bulk of the computation locally on their unencrypted data, leaving only a small portion for secure multiparty computation protocols. The second strategy involves finding specialized protocols that can solve specific problems much faster than general solutions.

Secure coprocessors: Another approach is to use a secure coprocessor – a tamper-resistant device designed so that any physical tampering will clear its memory. Participants in a group computation can verify that the secure coprocessor is running an agreed-upon program – for example, one that outputs a customer model from its input and nothing else – even if the device is in a remote location. Participants can communicate securely with the device to deliver their share of the input, and the secure coprocessor performs the computation.

Privacy-preserving search: Both data owners and people searching for information might have privacy concerns. Data-owner's privacy – To avoid the privacy concerns raised by merging private information sources, institutions often manage their private information databases with their own incompatible authentication and access-control mechanisms. This approach has privacy advantages over aggregating such information at a central host, but it is inconvenient at best for users. Users searching for access-controlled information that is legitimately available to them must independently search each relevant repository, assuming they know the entire set of relevant providers. Efficient and uniform search of multiple access-controlled repositories would seem to require a central trusted index host. But a typical search index almost perfectly represents the indexed files and databases, so a central host removes any privacy benefits associated with distributed maintenance of private data. Methods from the peer-to-peer domain, however, can uniformly search distributed content without relying on centralized resources. For example, developers could extend query-flooding methods such as Gnutella with decentralized authentication and access control policy-enforcement mechanisms to support uniform searching of access-controlled content. While query flooding does not scale well, recent results show promise for addressing scalability in decentralized search with stronger privacy properties.

Searcher's privacy – The detailed personal information that Web site or data repository owners can infer from a list of a user's searches raises another privacy concern. Anonymization methods can protect a user's privacy in public Web searches by preventing the results from being associated with a user's identity. But authentication requirements keep anonymization methods from protecting privacy in searches of access-controlled data. Techniques from the private information retrieval (PIR) domain may potentially apply to this particular problem. PIR techniques let authenticated users retrieve information from remote databases while preventing the database owner from identifying the specific information accessed. Significant work remains, however, to extend the current theoretical formulations of the problem to the real-world scenarios that arise on the Web.

Recently, the Privacy Commissioner of Canada (2016) stated, "Technology is now moving far too quickly for privacy regulators to keep pace. There are several technologies involved in the Internet of Things, such as radio-frequency identification (RFID), near-field communications (NFC), machine-to-machine communication (M2M) as well as wireless sensor and actuator networks." Some regulatory mechanisms remain effective, such as the European Union's Binding Corporate Rules (BCR). More often, regulations are outdated almost immediately upon release. And then there are some, such as Safe Harbor – the US–EU framework that has been in place for more than a decade – that are under siege. So where does that leave us? How can organizations safeguard privacy in an age of technology? The answer lies more in governance than regulation, in innovation more than compliance. Organizations need to focus on privacy accountability that follows an ethical path as well as aligning with suggestions from regulators, that adheres to the spirit rather than the letter of any regulation, and that engenders the trust of those whose privacy an organization has pledged to protect rather than erode it by not instilling enough importance in privacy within the organization. To sum up, 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.

8. Conclusion and Recommendations

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. 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 (Goldberg, 2007). According to UNESCO (2012), "The right of privacy is well established in international law. Among its key characteristics is the recognition that privacy is a fundamental human right, that it is firmly established in law, and that Fair Information Practices provided a useful articulation of privacy principles in the information world." Hence, legislators all over the world have taken notice and tried to minimize invasion of privacy.

However, Bhasin (2012a) remarked, "The online industry has preferred 'self-regulation' to privacy legislation for protecting consumers by forming the 'Online Privacy Alliance' to encourage self-regulation to develop a set of privacy 'guidelines' for its members. 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" to develop its own privacy policies to help consumers opt-out of advertising network programs and provide consumer redress from abuses. 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 (Joinson et al., 2010). Both trust seals and government regulations were highlighted in this paper. 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 (Bowman, 2001). However, Kugler (2015) remarked, "Concerns over online privacy have brought different responses in different parts of the world. In the U.S., for example, many Web browsers let users enable a Do Not Track option that tells advertisers not to set the cookies through which those advertisers track their Web use. Compliance is voluntary, though, and many parties have declined to support it. On the other hand, European websites, since 2012, have been required by law to obtain visitors 'informed consent' before setting a cookie, which usually means there is a notice on the page saying something like 'by continuing to use this site, you consent to the placing of a cookie on your computer.' Why are these approaches so different?" Common EU rules have been established to ensure that personal data enjoy a high standard of protection everywhere in the EU. As Bhasin (2012) pointed out, "The two main pillars of the data protection legal framework in the EU are: the Data Protection Directive and the ePrivacy Directive (Directive on Privacy and Electronic communications). 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. It is hoped that a growing number of countries will adopt privacy laws to foster e-commerce. 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.

Legislative action, though essential to any comprehensive privacy strategy, is not necessarily guided by the current capabilities and limitations of information technology infrastructures. Privacy legislation that impacts the IT infrastructure is not unique to the US. Sweden recently passed legislation that restricts how Web sites can use cookies, a technology that enables tracking of users across multiple visits. But cookies are also widely used in e-commerce applications, such as implementing online store shopping carts. As pointed out by Greenleaf (2015), "By January 2015, the total number of countries with data privacy laws has increased by over 10% to 109. Information access laws have a somewhat similar trajectory to data privacy laws, having reached the 'significant landmark' of laws in 100 countries in mid-2014. The geographical distribution of the 109 laws by region is: EU (28); Other European (25); Africa (17); Asia (12); Latin America (10); Caribbean (7); Middle East (4); North America (2); Australasia (2); Central Asia (2); Pacific Islands (0). So there are now 53 laws in European countries, but (for the first time) a majority of 56 data privacy laws are outside Europe, over 51% of the total. Because there is little room for increase within Europe, the majority of the world's data privacy laws will now continue to be from outside Europe, and increasingly so. During this 18 month period, the fastest 'growth area' has been Africa, with five new laws, including a new Act in Madagascar in January 2015. Data privacy laws are clearly no longer 'a European thing,' though the influence of 'European standards' remains paramount".

As Bauer (2012) remarked, "Social networks themselves do not necessarily guarantee the security of the information that has been uploaded to a profile, even when those posts are set to be private. This was demonstrated in one May 2010 incident during which unauthorized users were able to see the private chat logs of their contacts on Facebook. While this and other similar information bugs are usually quickly fixed, there is great potential for taking advantage of leaked information." Similarly, Bhasin (2015) warns "Privacy, security and fraud functions need to integrate. What customers and employees see as privacy information will have to change. Lengthy privacy policies, thick with legalese that most services use now, will never go away, but better controls will, and should, emerge." For example, Geller (2016) remarked, "Google is forced to wipe a Spanish

citizen's past financial troubles from its records. The Belgian Privacy Commission tells Facebook it must 'bend or break' to abide by the country's privacy laws. A plaintiff presses privacy cases against Facebook in both Austrian and European courts. Whatever tools are used to protect and collect personal data in the future, it will be important for companies, such as, Facebook and Google to educate their consumers and to provide them with options for all levels of privacy." In each instance, national privacy laws collide with the international nature of the Internet, and with American business expectations. Cross-border issues of the online world are not new, of course. 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.

According to E&Y (2014) Privacy Trends, "We are managing privacy in a time where carefully considered, detailed regulatory requirements do not necessarily result in effective privacy or data protection. Today's privacy regulations, as well as those being considered by regulatory bodies around the world, seem completely inadequate to protect individuals from the privacy risks emerging technologies present. Technology innovations, at work and at home, are pushing the limits of privacy well beyond current regulatory standards and legal requirements." No doubt, 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 surveliants 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. Privacy in the age of technology is quickly becoming a paradox. Today's privacy regulations, as well as those being considered by regulatory bodies around the world, seem completely inadequate to protect individuals from the privacy risks emerging technologies present. Here, Bhasin (2016) advices as: "While the regulation of privacy will continue to evolve, particularly as technology advances, businesses, agencies and individuals must also step up to the challenge of taking control of privacy management. No doubt, governments across the globe are making valiant efforts to protect privacy, but they cannot do it alone."

Finally, we recommend that all organizations can apply the following leading practices, specifically to improve the privacy scenario in the world:

1. Commitment from the top. Gain board support to establish a charter and a long-term strategy for privacy protection.

2. Organizational alignment. As part of the organization's strategy, develop a formal governance and operating model, align all aspects of privacy to the business and build relationships across the enterprise.

3. People, processes and technology. Document and communicate business processes related to privacy, and make them agile enough so that they can be updated when necessary. Consider new technology choices not only in terms of their benefits to the organization, but also the privacy risks they may pose.

4. Operational enablement. Allow good privacy governance to drive compliance, measure leading indicators to monitor performance and make improvements, as opportunities present themselves, and facilitate greater collaboration among functions.

5. Accountability for privacy needs to be everyone's responsibility – from the boardroom to the shop floor. Accountability for privacy and personal data protection needs to be a joint effort among governments, privacy commissioners, organizations and individuals themselves.

6. 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. Ahmad, T. (2009). *Right of Privacy: Constitutional Issues and Judicial Responses in USA and India, particularly in Cyber age*, available at http://www.ssrn.com/abstract=1440665.
2. Aleecia, M. McDonald & Cranor, L.F. (2008). The cost of reading privacy policies, *Information System: A journal of law and policy for the information socie*ty. Available at http://www.is-journal.org.
3. Bayardo, R.J. & Srikant, R. (2003). Technological Solutions for Protecting Privacy. *Web Technologies*, September, available at http://www.almaden.ibm.com/cs/projects/iis/hdb/Publication.
4. Bauer, C., Korunovska, J., & Spiekermann, S., (2012). On the value of information – what Facebook users are willing to pay. *ECIS 2012 Proceedings. Paper 197*. Available at: http://aisel.aisnet.org/ecis2012/197.
5. Bhasin, M.L. (2005). Challenges of Guarding Privacy – Practices Prevalent in Major Countries, *The Chartered Accountant*, January, 735-745.
6. Bhasin, M.L. (2006). Guarding Privacy on the Internet, *Global Business Review, 7(1)*, January-June 2006, IMI, Sage Publications, 137-156.

7. Bhasin, M. L. (2006a). Data Mining: A Competitive Tool for Banking and Retail Industries, *The Chartered Accountant*, October, 588-594.
8. Bhasin, M.L. (2006b). Privacy Protection on the Internet: Privacy Policy, Government Regulation and Technology Solutions, *Amity Business Review*, July-December, 44-59.
9. Bhasin, M. L. (2007). Mitigating Cyber Threats to Banking Industry, *The Chartered Accountant, 50*(10), April, 1618-1624.
10. Bhasin, M.L. (2008). Guarding Privacy on the Internet: Privacy Policy, Government Regulations and Technology Solutions, *International Journal of Internet Marketing and Advertising, 4*(2/3), Special Issue on SME's, 213-240.
11. Bhasin, M. L. (2012). Online Privacy Protection: Privacy Seals and Government Regulations in Select Countries, *International Journal of Finance and Accounting, 1*(6), Nov., 148-161.
12. Bhasin, M. L. (2012a). Guarding Online Privacy: Privacy Seals and Government Regulations, *European Journal of Business and Social Sciences, 1*(9), Dec. 2012, 1-20.
13. Bhasin, M.L. (2015). Menace of Frauds in Banking Industry: Experience of a Developing Country, *Australian Journal of Business and Management Research, 4*(12), April 21-33.
14. Bhasin, M.L. (2016). Integration of Technology to Combat Bank Frauds: Experience of a Developing Country, *Wulfenia Journal*, *23*(2), Feb., 201-233.
15. Bowman, L.M. (2001). House Pulls Carnivore into the Light. *ZDNet News* (23 July).
16. Branscum, D. (2000). Guarding On-Line Privacy. *Newsweek 135* (23): 77-78.
17. Chaffey, D. and White, G. (2011). *Business Information Management. Prentice-Hall, Financial Times*, 2 editions.
18. Council of Advisors on Science & Technology (2014), Big Data and Privacy: A Technological Perspective, *Executive Office of the President*. Available at http://www.whitehouse.gov.
19. Conroy, P., Milano, F., Narula & Singhal, R. (2014). *Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry*, Deloitte University Press, 13 November. Available at http://www.dupress.com.
20. Culnan, M. (2002). *Georgetown Internet Privacy Policy Study*. McDonough School of Business, Georgetown University, see http://www.msb.edu/faculty/culnan/gippshome.html.
21. Debatin, B., Lovejoy, J.P., Horn, M.A. & Hughes, B.N. (2009). Facebook and Online Privacy: Attitudes, behaviors and unintended consequences. *Journal of Computer-Mediated Communications, 15*(2), 83-108.
22. 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, 1-17.
23. European Commission (2011). *Workshop on Privacy protection and ICT: Research ideas*. Workshop report, Sept.21, Brussels.
24. E&Y (2014) Privacy Trends 2014: *Privacy Protection in the age of Technology*. Available at http://www.ey.com.
25. Federal Trade Commission (2010). *Protecting Consumer Privacy in an Era of Rapid Change: A proposed framework for business and policymakers*. December. Available at http://www.ftc.org.
26. Fuchs, C. (2011). The political economy of privacy on Facebook. *The internet & Surveillance, Research paper 9 series*, Vienna, Australia. Available at http://www.uti.at.
27. Geller, T. (2016). In Privacy Law, It is the U.S. vs. the World, *Communications of the ACM, 59*(2), 21-23.
28. 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, Dec.
29. Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management Science, 57* (1), 57-71.
30. Green, H., Yang, C. & Judge, P.C. (1998). A Little Privacy, Please. *Business Week 3569*, 98-99.
31. Greenleaf, G. (2015). Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority, 33 Privacy Laws & Business International Report, February, *UNSW Law Research Paper No. 2015-21*.
32. Haag, Cummings & McCubbrey (2014). *Management Information Systems for the Information Age*. McGraw-Hill Irwin.
33. Hoffman, D., Novak, T.P. & Peralta, M. (1999). Building Consumer Trust Online. *Communications of the ACM, 42* (4), 80-85. Available at http://zdnet.com/2100-1106-270406.html.
34. Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction, 25*(1), 1-24.
35. Kalakota, R. & Whinston, A. B. (1996). *Frontiers of Electronic Commerce. Reading, Mass*, Addison-Wesley.
36. Krill, P. (2002). DoubleClick Discontinues Web Tracking Service. *InfoWorld*, 9 January. Available at: http://www.infoworld.com/articles.
37. Kuglee, L. (2015). Online Privacy: Regional Differences, *Communications of the ACM, 58*(2), 18-20.
38. Laudon, K.C & Traver, C.G. (2014). *E-commerce* 10th edition, Addison Wesley, NY.
39. Laudon, K.C. and Laudon, J.P. (2016) *Management Information Systems: Managing the digital firm*. Pearson, 14th edition.
40. Markert, B.K. (2002). *Comparison of Three Online Privacy Seal Programs, GSEC Practical Assignment* Version 1.2e, SANS Institute.
41. Morando, F., Iemma, R., & Raiteri, R. (2014). Privacy evaluation: what empirical research on users' valuation of personal data tells us, *Internet Policy Review, 3*(2), May, available at http://policyreview.info.
42. Office of the Privacy Commissioner of Canada (2016). *The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments*, available at https://www.priv.gc.ca.

43. 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.
44. Perry, W.J (2010). Protecting Individual Privacy in the Struggle against Terrorists, *Journal of Privacy and Confidentiality, 2*(1), 57-71.
45. 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.
46. 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.
47. Punch, L. (2000). Big Brother Goes Online. *Credit Card Management, 13*(3), 22-32.
48. Schwaig, K. S., Segars, A. H., Grover, V., & Fiedler, K. D. (2013). A model of consumers' perceptions of the invasion of information privacy. *Information & Management, 50* (1), 1-12.
49. Slyke, C.V., & Belanger, F. (2012). *E-Business Technologies: Supporting the Net-Enhanced Organization*. John Wiley & Sons.
50. Stair, R. & Reynolds, G. (2014). *Fundamentals of Information Systems*. 7th Edition, Thomson Course Technology, USA.
51. Stevens, G. (2011). Privacy protections for personal information online, April, *Congressional Research Service Report 7*-5700, available at http://www.crs.gov.
52. Swire, P., Hemmings, J. & Kirkland, A. (2016). *Online Privacy and ISPS, working paper of The Institute for Information Security & Privacy*, Fen. 29. Available at http://www.iisp.gatech.edu.
53. Tang, Z., Hu, Y.J. & Smith, M.D. (2007). Gaining Trust through online Privacy Protection: Self-regulation, mandatory standards, or caveat emptor. *Heinz College Research paper 49*, available at http://www.repository.cmu.edu/heinzworks/49.
54. 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 http://www.ntia.doc.gov.
55. Tsai, J.Y., Egelman, S., Cranor, L. & Acquisti, A. (2011). The Effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), June, 254-268.
56. Turban, E., Leidner, D., Mclean, E., & Wetherbe, J. (2008). *Information Technology Management: Transforming organizations in the digital economy*. 6th edition, John Wiley & Sons, Inc.
57. UNESCO (2011). *Global Survey on Internet Privacy: Calls for proposals*. June, 2011. Available at http://www.unesco.org.
58. UNESCO (2012). *Preserving Privacy in the Information Soci*ety. Available at http://www.unesco.org.
59. Weiss, M.A. & Archick, K. (2016), U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, *Congressional Research Service, 7*-5700. 1-16. Available at http://www.crs.gov.
60. Wirtz, J., Lewin, M.O. & Williams, J.D. (2007). Causes and Consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18*(4), 326-348.