Privacy in the USA

Background Report in Draft Form

Prepared by
Emily Smith, Researcher

For the Globalization of Personal Data Project
Queen's University

August 2005

c/o Department of Sociology
Queen's University
Kingston, ON K7L 3N6
(613) 533-6000, ext. 78867
(613) 533-6499 FAX
surveill@post.queensu.ca
http://www.queensu.ca/sociology/Surveillance

Table of Contents

Privacy in the USA – Draft Report

Privacy Policies and Laws

Government Regulation of Privacy

The United States has very limited legislation regarding privacy. Privacy is not a guaranteed right under the Constitution, there is no independent or federal privacy oversight body and no comprehensive federal or commercial privacy legislation exists. Instead, the US favours a self-regulatory model, relying on the free market economy to balance the privacy needs of individuals with that of organizations. A patchwork of federal and state privacy legislation does exist with regard to the protection of information held certain public and private sectors, in the areas considered the most sensitive. Individual states are currently expanding privacy legislation, as a response to growing data abuses and privacy concerns.

Despite popular belief[1], privacy is not explicitly addressed as a right in the US Constitution. Limited constitutional rights of privacy are granted under the Bill of Rights, including the right to privacy from government surveillance into areas where a person has a "reasonable expectation of privacy" and in matters of marriage, procreation, contraception, family relationships, child rearing and education (Privacy International 2003). The Fourth Amendment gives Americans the right to security of the person, against unreasonable search and seizure, as well as against the issue of warrants without probable cause. Some states also give explicit privacy protection in their Constitutions, such as Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, New York, Pennsylvania, South Carolina, and Washington (Weston 2005). Individuals can also challenge their personal right to privacy in the legal system.

[1] For example, a Gallup Poll conducted in February of 1999 surveying 1,054 adults found that 70 percent of respondents believed that the Constitution guaranteed citizens the right to privacy.

Many cases involving privacy have been heard in the courts, from drivers licence information to grading in schools, mostly with regard to Fourth Amendment Rights.

The Privacy Act was passed in 1974, which defines privacy as a fundamental right and sets provisions for the protection of records held by the US government and companies that they conduct business with (Privacy International 2003). This Act requires that agencies holding this information use basic Fair Information Principals (FIPs), such as the collection of necessary information only, collecting information directly from the individual, the use of data only for routine purposes, obtaining consent from individuals for information disclosure, providing access to an individuals personal records, rights for individuals to correct information about themselves, use of information only for the purposes originally collected unless authorized by the individual and prohibiting the use of secret databases (Lyon and Bonikowski 2002). However, these laws are subject to interpretation by administrative bodies and certain records are exempt, such as the National Crime Information Center. An investigation by the General Accounting Office found uneven compliance with the Privacy Act in 2003, with lack of leadership and guidance of the Act, low priority of implementation, insufficient training, and the absence of consistency in compliance. Thus, the provisions of the Privacy Act are not adequately protected (Privacy International 2003).

There is no independent agency in the U.S. dedicated to privacy oversight for the government. The Office of Management and Budget have a limited role in setting policy for federal agencies under the Privacy Act and appointed a Chief Counsellor for Privacy to coordinate these efforts in 1999. However, this oversight position was deemed ineffective and was eliminated by the Bush administration (Privacy International 2003).

The Freedom of Information Act (FOIA) was enacted in 1966, with amendments in 1974 and 1976, to reduce government secrecy and give citizens access to information held by the federal government (Privacy International 2003). Many exemptions apply to this Act, including protection for issues of national security, trade secrets, medical files, investment records, and financial information (Lyon and Bonikowski 2002). Access to government records are also permitted by some state laws (Privacy International 2003).

The Federal Trade Commission (FTC) has some oversight and enforcement powers for laws protecting children online, consumer credit information and fair trade practices, but not privacy rights in particular. Their use of the federal law on "unfair and deceptive" practices has been important for bringing privacy suits against companies that affect the entire industry where the law is ruled (ibid). The FTC conducts extensive research on internet privacy and despite a belief in industry self-regulation, has recommended to the US Congress that legislation is necessary to protect consumer privacy online (ibid). Legal efforts of the FTC are focussed on telemarketing laws, spam, pretexting and children's privacy. Of greatest media attention was their changes to the Telemarketing Sales Rule to create a do-not-call list of individuals wishing to opt-out of telemarketing. The FTC proposed Fair Information Principles (FIPs) for handling personal data, including notice, choice, access, integrity, and enforcement, based on principles defined by the U.S. Department of Health, Education, and Welfare (Bellman et al 2003).

Privacy Laws and the Private Sector

The United States does hot have comprehensive federal legislation to govern privacy and information collection practices in the private sector. Various federal laws cover certain categories of privacy and personal information collection in the private sector that are perceived

to be the most sensitive, such as financial records, health information, and children's privacy (Cockfield 2004). The US federal government relies on the rationale that the market will be more effective in balancing and regulating the commercial needs of business and privacy interests of consumers (ibid). Some examples of the most significant federal privacy regulation include: the Gramm-Leah-Bliley Act, the Children's On-Line Privacy Protection Act, the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, and the Videotape Privacy Protection Act (ibid).

The Gramm-Leah-Bliley Act (GLBA) was passed in 1999, also called the Financial Modernization Act, under administration by the FTC, and is designed to regulate privacy practices in the financial sector (Cockfield 2004). The Act came at a time of increased scrutiny of financial privacy, after the Michigan Attorney General sued several banks for revealing they were selling information about customers to marketers; other banks around the country also admitted to this (Privacy International 2003). The Act sets weak protections on financial information that is shared among merged institutions and provides individuals with limited opt-out abilities for information shared with non-affiliated institutions (ibid). The Act enforces an 'opt-out' standard, where onus is placed on customers to contact their financial institution to request that constraints be placed on sharing their personal information with unrelated third parties. This law also requires financial institutions to have a privacy policy that is brought to the customers' attention, but does not set out what principals these privacy policies must include (Cockfield 2004).

Also administered by the FTC is the Children's On-Line Privacy Protection Act (COPPA), which was passed by Congress 1998 and came into effect in 2000, to protect children's personal information collection and misuse by online services (Cockfield 2004). This

Act dictates that commercial websites must obtain parental consent prior to the collection of information from children under 13 and must provide parents with notice of their information collection practices. Parents must have the ability to review and correct their children's information online (ibid). This is the only federal law regulating the use of information online (Privacy International 2003).

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 to prevent employers from denying employment based on the medical condition of job applicants (Cockfield 2004). This Act is administered by the Office of Civil Rights in the Department of Health and Human Services. The HIPAA Privacy Rule, formally called the Standards for Privacy of Individually Identifiable Health Information, became the first federal regulation protecting individual health information in 2003 (Privacy International 2003). HIPAA establishes minimum standards for the treatment of healthcare information by healthcare providers. Expressed consent is required for disclosure or transfer of personal health information to third parties. This law also gives individuals the right to access and correct their health information, as well as to know who has been given their information (ibid).

The Fair Credit Reporting Act (FCRA) was passed in 1970, with the most recent amendments in 2003, which regulates aspects of privacy practices in the credit reporting industry (Cockfield 2004). This Act requires that businesses report credit information fairly and accurately, by keeping records up to date and confidential, identifying purposes for collection, using credit reports for stipulated purposes only, giving individuals access to their reports, correcting errors and including customer disputes in reports (ibid).

Lastly, the Videotape Privacy Protection Act (VPPA) prohibits video stores from giving out customer records without consumer consent. Personal information collected at video stores

must also be destroyed after one year of the date it is deemed necessary. The above list of laws in not intended to be completely exhaustive, but represents the most significant sector-specific laws regulating privacy in the American government and commercial areas. Despite these limited privacy restrictions introduced since the 1960s and 1970s, surveillance by the public and private sector has been continually increasing in intensity and scope (Lyon and Bonikowski 2002).

Debate over Government Regulation of the Private Sector

Debate has escalated in recent years about regulating privacy in the private sector in the United States. The US government and private sector organizations want to maintain the self-regulatory model, and do not want new laws to control privacy in the commercial sector, only for sensitive data, such as the current laws on medical, financial and children's information. Presently, the majority of US businesses use an opt-out model of customer information regulation, where consumers must be vigilant about protecting their personal information, rather than an opt-in model, where customers are first given the choice to participate.

The Online Privacy Alliance was formed in 1997, involving a coalition of over 50 US companies and trade associations that adopted comprehensive privacy principals and acknowledged the need for enforcement. However, an FTC report to congress on privacy online in June of 1998 suggests that much greater self-regulation is needed to improve consumer protection and confidence online. Of the 1400 US websites the FTC examined, only 14 percent complied with self-regulatory guidelines by providing notice of information collection practices, and less than 2 percent provided comprehensive privacy policies. FIPs including, notice, choice, access and security are the industry standard. Enforcement mechanisms and industry incentives are needed for compliance (Screeton 1998).

Introduction of New State Laws

More substantial legal activity regarding privacy has occurred recently at the state level. Privacy laws are being proposed and introduced after numerous data breaches have been exposed in private organizations, such as ChoicePoint, Bank of America, LexisNexis, and CardSystems Inc. These cases are highlighting the lack of data protection for consumer information and are resulting in public debate about addressing the security of customer information. Many new privacy laws are now being launched at the state level to protect against data theft, selling and leaks. Over 200 bills have been introduced in the House and Senate since January of 2001 (Privacy International 2003). Laws are being proposed that restrict how companies buy, sell and dispose of consumer information and restrict what information is allowed to be contained.

California leads the way with privacy legislation, by passing the Database Protection Law, requiring that businesses notify individuals when their information has been accessed as a result of a security breach or accident when data was not encrypted. These laws have been instrumental in getting companies, colleges and government agencies to confess to the loss of millions of consumers' personal data, such as social security numbers, addresses, and financial account numbers, due to theft, misplaced files and hackers. California has proposed another law requiring firms to provide notice of all breaches, covering all data forms, including paper, non-encrypted data, and back-up tapes. Legislation has also been passed in California to prevent the printing of social security numbers on forms, invoices or identity badges, and that gives consumers greater control over their credit reports when fraud is suspected.

Many other states are modelling laws after those of California to counter the problem of personal data breaches by companies (Kollars 2005). Thirty-five states have introduced legislation requiring notification of security breaches involving personal information, and

thirteen have passed new legislation this year. Connecticut, Florida, Hawaii, Illinois, Massachusetts, Minnesota, New Mexico, New York, North Dakota, Vermont, Washington and Wisconsin also have introduced extensive privacy legislation. Some of these states are requiring businesses to get consumer permission to share data, or opt-in (Weston 2005). New laws on data disposal have also taken effect, making businesses responsible for destroying files with personal identifiers of customers on them by shredding or obliterating files within a certain time frame after use.

As these issues suggest, privacy legislation is currently a hotly debated topic within the government and commercial sectors of the United States. Public opinion has also been escalating on the topic, which will be addressed later.

International Privacy Law Affecting the US

Many other developed countries have much farther-reaching privacy legislation than the US to protect consumer data in transactions. European countries have extensive privacy protection that regulates both business and government. For example, the European Union introduced the Privacy Directive in 1998 that includes wide-ranging privacy protections for consumers. These consist of FIPs, such as requiring that individuals be consulted about transfers of their information to third parties, that they be given the chance to correct errors in data about them, it also prohibits companies from using universal identifiers such as social security numbers in transactions, record collating, and data sharing or selling without consumer consent. American businesses are relatively free to collect and sell consumer information, whereas European companies must first obtain individual consent. The EU Directive has prompted other countries to follow suit. For example, Canada enacted the Personal Information Protection of Electronic

Documents Act (PIPEDA) in 2001, which requires consumer consent to trade personal information, allows consumers to correct inaccuracies and is enforced by the national privacy commissioner (Privacy Security 2005). The US model is much less comprehensive, relying on a system of self-regulation and an opt-out regime (ibid). Consumer protection of online privacy will be essential in maintaining trade in the global economy (Screeton 1998).

A Safe Harbor agreement was reached between the US Department of Commerce and the European Commission in June 2000 in order to allow US companies to continue business transactions involving personal data from the EU. This agreement was necessary in order to allow cross border flows of customer data by making US companies agree to raise their level of privacy regulation to be consistent with the EU Privacy Directive. Over 350 US companies have joined the Safe Harbor agreement, and must meet a certain criteria of customer data protection in order to be protected under this act (Privacy International 2003).

Legal Changes after September 11th, 2001

Many laws that increase the surveillance capacity of police and government have also been introduced within the United States since the terrorist attacks in New York and Washington on September 11th, 2001. As a response to the attacks, the Bush Administration declared a 'war on terror' and aimed to increase state-sponsored surveillance (Lyon and Bonikowski 2001). The Department of Homeland Security was established in 2002, which is a cabinet-level agency that has increased the law enforcement and information sharing powers of twenty-two US agencies responsible for national security. Some privacy protections were included in this government body, such as a civil rights officer and a privacy officer responsible for providing privacy impact assessments and reporting annually to Congress (Privacy International 2003).

Most significantly, the USA PATRIOT Act, Uniting and Strengthening American by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, was quickly introduced by the Department of Homeland Security and passed 45 days after 9/11 with little debate. This Act gave the US government unprecedented surveillance power over all of its citizens (Lyon and Bonikowski 2002). The Act greatly extends the search powers of police in cases of suspected terrorist activity and significantly weakens privacy protection in federal wiretapping statutes. Several states also loosened wiretapping laws. In addition, the Cyber Security Enhancement Act (CSEA) decreased privacy protections against wiretapping. This Act permits communications providers to voluntarily release customer communications without their consent if it is believed to be an emergency situation. The PATRIOT Act enables law enforcement officials to more easily obtain permission to use wiretaps on communications and to collect medical records, tax records, traffic data and library borrowing records that are considered relevant to an ongoing terrorist investigation (ACLU 2005). Computers can also be tapped and traced without a court order (Privacy International 2003). The PATRIOT Act has been widely criticized for infringing on the civil liberties of American citizens (Lichtblaw 2005).

A sunset clause was included in the PATRIOT Act, which brought some of these increased surveillance powers up for review two years after the legislation was introduced. These sections of the Act are currently being debated in the Senate. President George W. Bush and Republican leaders on the Senate Select Committee on Intelligence Consultation are fully supporting the continuation of increased surveillance powers under the Act and are proposing to include additional search powers, such as giving the FBI the ability to demand business records in terrorist investigations without obtaining the approval of a judge (Lichtblaw 2005). Civil liberties groups, such as the American Civil Liberties Union (ACLU), are strongly opposing

these changes as invasions of personal privacy. On July 29th 2005 the U.S. Senate unanimously supported the reauthorization of most of the PATRIOT Act, while some components were given new expiry dates. The reauthorized legislation is expected to be signed into law on September 11 2005 (Talvi 2005).

Several other controversial surveillance enabling programs were introduced in the U.S. following 9/11. Total Information Awareness (TIA) was a proposed extreme data mining program that was later abandoned. Afterwards, MATRIX, the Multistate Anti-terrorism Information Exchange, was introduced by Seisint Inc. of Florida. This program compiled government and private sector information on US citizens and made available for searching by federal and state law enforcement officials. MATRIX was designed to search through citizen profiles for terrorist and anomalous activity. It was terminated in April 2005 by the Pentagon (ACLU 2005). In air travel, the government also implemented no-fly lists for air passengers suspected as terrorists. The Transportation Security Administration (TSA) introduced CAPPS II, the Computer Assisted Passenger Pre-Screening System, which is a surveillance system that profiles air passengers for security risks. This was done without public consultation or oversight.

The Real ID Act was approved by the US House of Representatives in February 2005 and passed by Congress in May. This legislation passed with little or no debate because it was attached to another emergency spending bill that was mandatory for US troops in the Middle East. This Act requires states to design drivers' licences to comply with federal anti-terrorist standards by 2008, with the possibility of including biometric identifiers on driver's licenses. Under the Act, states must share licensing information with the Department of Homeland Security, in order for citizens to have access to government buildings, airports, trains, or any other identity-required activities. Information is collected on driver histories, violations,

suspensions, as well as name, date of birth, gender, address, a digital photograph, and signature. This information is shared with Canada and Mexico. The Act is designed to combat terrorist activity and illegal immigrants. Real ID gives the Department of Homeland Security authority over designing state identity cards with tracking and smart technologies, such as Radio Frequency Identification, fingerprinting and digital photos. The Act has prompted criticism by many civil liberties organizations, conservative groups and citizens as a threat to privacy, liberty, safety and against profiling and discrimination, and has led to suspicion about the creation of a national identity card. Smart ID cards have already been issued to military personnel, federal government officials, and the new drivers licences will be issued as old cards expire.

Cultural Values, Attitudes and Public Opinion on Privacy

Hofstede's Cultural Values Index

Public opinions on privacy issues are affected by national cultural values and attitudes. Privacy is tied to the norms of society, such as what personal conduct is regarded as beneficial, neutral or harmful to the public good (Westin 2000). Bellman, Johnson, Kobrin and Lohse (2003) argue that cultural values and regulation have a significant influence on privacy concerns within a nation. Geert Hofstede defines cultural values as "a set of strongly held beliefs that guide attitudes and behaviour" (Bellman, Johnson, Kobrin and Lohse 2003, 8). In 1980, Hofstede conducted a five-dimensional analysis of cultural values within 40 countries in *Culture's Consequences*. Milberg, Smith and Burke (2000) found significant positive relationships between four of Hofstede's dimensions of cultural values and information privacy concerns. Hofstede's research data, although dated, can provide valuable insight into US culture and values and its influence on public opinions towards privacy.

The USA ranked 25th out of 40 countries on the Power Distance Index (PDI), with a score of 40 percent (Hofstede 1980). This lower PDI score indicates that cultural values in the US rest in belief of equal rights, cooperation, legitimate power, a political system based on representation, pluralism and majority voting. Low PDI also tends to show that greater national wealth is more widely distributed in the US, with a strong middle class (ibid). Smith, Milberg and Burke (1996) found that countries with a low PDI scores tend to have less concern for informational privacy (Bellman et al. 2003).

On the Uncertainty Avoidance Index (UAI), the United States ranked 31st, with a score of 46 percent (Hofstede 1980). This low score suggests that the US has a low level of anxiety, are less resistant to change, have stronger achievement motivation and take more risks. In these older democratic societies authorities serve the citizens and citizens have optimism that they can control political decisions. There is a belief that there should be as few rules as possible, and that these rules can be broken for pragmatic reasons (ibid). Societies with low levels of UAI do not rely on high levels of government regulation to alleviate concerns about information privacy (Milberg et al 1995; Bellman et al. 2003). Americans discourage centralized authority and are reluctant to implement government regulation on private sector industry; they prefer a self-regulatory approach to privacy (Screeton 1998).

The United States has the highest level of Individualism (IND) in Hofstede's analysis, at 91 percent (Hofstede 1980). This strongly indicates that Americans believe in the importance of the individual and personal life, with emphasis on freedom, individual choice, initiative and self-orientation (ibid). Countries with high levels of Individualism prefer independent lifestyles and the right to a private life and opinion (Bellman et al 2003). Democratic societies respect individualism and value the private sector as a force for social progress and morality. The

government is viewed by citizens as Useful, but constitutional rights guarantee civil liberties of citizen's private beliefs, associations and acts (Westin 2000). US citizens may be more willing to disclose personal information because they have lower privacy concerns than other countries and greater trust in private organizations to protect their information.

Finally, the US scored 13th out of 40 countries on the Masculinity (MAS) index, with a score of 62 percent (Hofstede 1980). This shows that the US holds somewhat masculine values, with sex roles differentiated and men dominating in earnings, recognition and advancement. Achievement is defined by wealth and motivation and successful performance is rewarded. Countries with higher scores of MAS tolerate greater levels of inequality between males and females and accept the interference of organizations in to private lives as legitimate (ibid).

Overall, Americans have the highest scores on IND, medium scores on MAS and low levels of PDI and UAI. Milberg, Smith and Burke (2000) show positive associations with PDI, IND, and MAS with the effect of cultural values on information privacy concerns, and a negative association for UAI. Bellman et al. found the opposite, that countries with higher score on PDI, IND and MAS, and lower scores on UAI have lower overall levels of concern about information privacy. Based on these findings, the US scores generally indicate low concerns with privacy, with high levels of individualism, belief and trust in private organizations with personal information and a preference for self-regulation. These results are contrasted with high concerns over privacy and desire for regulation in national public opinion polling discussed below.

Public Opinion Polling on Privacy in the US

National public opinion surveys are prevalent in the US, and play an important role in debates about privacy. Colin Bennett and Charles Raab suggests that public opinion surveys are

largely an American phenomenon and invention (Bennett and Raab 1996). Jim Harper and Solveig Singleton claim that the privacy debate is consumed by 'survey madness' and that the high number of surveys results in confusion for policymakers (2001). Surveys on privacy issues are primarily conducted by private sector organizations, and tend to show that privacy and data protection are prominent concerns within the United States. These opinion polls usually coincide with larger reform and policy efforts, suggesting that privacy is of elevated importance within the political agenda. For example, because comprehensive data protection legislation has not been reached in the US, public opinion polls are featured within this debate. Public opinion surveys on privacy in the US are difficult to compare because they address different aspects of privacy and use varying levels of quality measures. Overall, Colin Bennett and Charles Raab argue that these studies tend to indicate that a large majority of Americans are concerned with personal privacy as a value and see it threatened by new information and communication practices by government and commerce (Bennett 1996).

There is significant debate over the value of public opinion polling on privacy. Some experts in the privacy field, such as Alan Westin, argue that social surveys on consumer privacy are valuable to informing the process of creating fair consumer information collection in e-commerce in addition to informing the policymaking process (Westin 2000). While others, such as Harper and Singleton, argue that when examining public opinion poll data on privacy this information must be taken 'with a grain of salt' (2001). These authors are sceptical about privacy surveys because their design is often used to manipulate results in order to influence the policymaking process. Harper and Singleton claim that more objective measures are needed that do not 'push' or 'pull' respondents in a certain direction. Similarly, John Gilliom claims that

surveys on privacy are too mechanically structured and only cover a limited aspect of the issue (Gilliom 2005).

High quality surveys on privacy are very difficult to achieve, requiring large time commitments and a great expense (Harper and Singleton 2001). Thus, when examining polling results on privacy, attention must be paid to who is reporting the information and for what purpose. A number of organizations conduct public opinion polling on privacy, such as advocacy groups, government agencies, think tanks, research centres, and commercial polling organizations (Zureik 2004). Depending on their affiliation and funding partners, this can affect question wording and reporting of results. For example, business studies often distort the debates by overstating the costs to business, as well as ignoring the costs to consumers and the benefits of privacy to commerce and society (Gellman 2002).

Additionally, the concept of privacy is a complex one to study in public opinion polling. As Gellman states, the term is an elusive and value-laden concept (Gellman 2002). Consensus on the precise definition of privacy has not been reached (Zureik 2004). Many of the groups conducting polling do not clarify how they are addressing the issue of privacy or clarify the term for respondents. Privacy competes with other social values and is situated within the economy, society and politics and studies that address this are the most useful (Westin 2000; Bennett 1996). Some of the prominent themes of public opinion polling on privacy in the US will be outlined below.

High Concern

Many polls continue to suggest a high level of concern about information privacy in the US For example, a Privacy & American Business/Harris survey found in 1998 that 87 percent of

consumers were concerned about their personal privacy (Privacy 1998). Similarly, IBM conducted a study in 1999, which found that three quarters of consumers express concern about information privacy in the US (IBM 1999; Bellman et al. 2003). The IBM survey also found that 94 percent of respondents claimed they were worried about the misuse of their personal information. Consumer privacy in particular is a great concern, with 80 of those in the IBM study agreeing that consumers have lost all control over how their personal information is collected and used by companies. In 2004, the Ponemon Institute also found that individuals increasingly view their privacy as important, and worry about how organizations collect, use and share their personal information (Ponemon 2004). It is important to note that high reporting of privacy concerns in public opinion polls does not indicate actual threat, and that real world actions may reflect different attitudes than polls reveal (Harper and Singleton 2001).

Internationally, there is very limited comparative data on privacy. Without surveys that are designed explicitly for cross-cultural inferences about attitudes and preferences, it is difficult to compare non-equivalent survey instruments (Bennett and Raab 1996). One multi-national Consumer Privacy Survey conducted by IBM-Harris found that people in the US were more concerned that their personal information is vulnerable to misuse than respondents in the UK or Germany (IMB-Harris 2000). In this survey, 94 percent of consumers in the US thought that personal information was vulnerable to misuse, compared to 78 percent in the UK and 72 percent in Germany. In a 1984 six-nation Gallup Poll, respondents were asked whether they agreed or disagreed with the statement, ‘there is no real privacy because the government can learn anything it wants about you”. Forty-seven percent of US respondents agreed with this statement, compared to 68 percent in Canada, 59 percent in Britain, 18 percent in West Germany, 18

percent in Switzerland, and 43 percent in Brazil (Bennett 1996). Further cross-national research is needed that compares equivalent survey questions.

Alan Westin and the Privacy Dynamic

Some of the most well-known studies on privacy in the US have been conducted by Louis Harris and Associates and Dr. Alan F. Westin from 1978 to the present. These public opinion surveys track US consumer concerns and new developments in the consumer privacy arena and have found that there are two main driving factors in privacy attitudes: individual levels of distrust in institutions, and fears of technology abuse (Westin 2000). Westin uses a four item distrust index to measure distrust in government, voting, and business, as well as fears that technology is out of control. For example, in 1990, Harris-Equifax conducted a survey with a cross-section of the American public, interviewing a total of 1,255 people over the telephone (Louis Harris and Associates 1991). Privacy was found to be a great concern with Americans, with 79 percent of those interviewed being concerned with threats to personal privacy. A general and rising distrust in government and technology was revealed with concern growing over having to reveal personal information (ibid). As consumers, many believed that their privacy rights were not adequately protected by law and business practice. Individuals desired improved business practice, new legislation, opt-out options and government oversight (ibid).

Dr. Alan F. Westin provided analysis of these results and created a general concern about privacy index where three groupings emerged, which he called the Privacy Dynamic. Within this Dynamic, the Privacy Fundamentalists represented 25 percent of responses (ibid). These individuals possess high privacy concerns, are distrustful of organizations asking for their personal information, worry about the use and accuracy of their information and favour new

privacy laws and controls. Eighteen percent were called the Privacy Unconcerned. This group have low to no concern about consumer privacy issues, are trustful of organizations collecting personal information, comfortable with existing procedures, ready to give up privacy for consumer benefits and did not want new privacy laws (ibid). The largest group was the Pragmatic Majority, at 57 percent. These individuals weigh the benefits and opportunities with the preservation of public safety, are willing to trade privacy for some convenience and look for practical procedures to guide privacy protection. This group is made up of mostly young adults that adopt varying positions on privacy according to whether they perceive Fair Information Practices (FIPs) are being followed. Westin argues that companies and the government must gain support and trust from this Pragmatic Majority in defining fair information principles to sway their opinion to either side of the Dynamic (ibid).

Similar findings were made in Harris/Westin surveys from 1990 to 1998. For example, in a 1999 survey, 25 percent were Privacy Fundamentalists, 20 percent were Privacy Unconcerned and 55 percent were Privacy Pragmatists (Westin 2000). Westin continues to claim that the battle for the Pragmatists can go either way, towards supporting existing rules and practices or to seek legal or regulatory measures (Westin 2000). He argues that consumers are highly concerned with privacy threats and shrewdly balance privacy by examining whether FIPs are being followed by companies. With safeguards such as FIPs in place, he claims consumers approve of personal information collection by companies.

More recently, the Harris/Westin polls have shown greater change in public opinion on privacy, reflecting a weakened trust of citizens and consumers. Since 1999, numbers have varied within each segment of the Privacy Dynamic. In February 2003, a cross-section of 1,010 American adults were surveyed over the telephone. The majority of respondents were Privacy

Pragmatists, at 64 percent or two-thirds of all adults, an increase of 10 percent in this category since 1990 (Taylor 2003). These individuals feel strongly about protecting their privacy from government and business misuse, but will sometimes trade their privacy for other benefits when they believe care is being taken with their information. The Privacy Unconcerned dropped to only 10 percent of adults who do not have real concerns over privacy, a decline of 12 percent since the 1990 survey (ibid). Twenty-six percent of respondents were Privacy Fundamentalists, feeling they had lost their privacy already and were strongly resisting further erosion. These changes in public opinion may be attributed to transformations in citizen privacy issues in recent years, such as the terrorist attacks of September 11th 2001, the recent highly publicized breaches in privacy in the marketplace, or by new state and federal regulations, to be discussed in greater detail later (ibid).

For the most part, surveys by Alan Westin and Harris Interactive are respected in the field. For example, Harper and Singleton who are critical of privacy surveys, claim that Harris Interactive uses more neutral questions in their surveys, such as comparing privacy concerns in relation to other choices and have the most unprompted questions, which elicit more accurate results (Harper and Singleton 2001). Alan Westin also recently received an honour by his peers for his work on privacy[2]. However, it is also important to note criticisms of Westin's Privacy Dynamic. The Electronic Privacy and Information Center (EPIC), a privacy advocacy group interested in highlighting privacy concerns, challenges the results of Westin's surveys. They critique Westin's wording of categories, statistical measures, lack of dealing critically with privacy issues and the involvement of business funding in their research (EPIC 2005).

[2] The International Association of Privacy Professionals awarded Dr. Alan Westin with the Privacy Leadership Award of 2005. Westin was recognized for his authorship of three books on privacy, being the co-founder of Privacy & American Business and for his voice as an expert for over 30 years on a range of privacy issues for government and private industry.

In terms of wording, EPIC refers to Westin's Dynamic as a segmentation that uses pejorative terms to describe its members, such as using the term 'fundamentalist' to describe those who hold very strong concerns about privacy. EPIC claims that by labelling this highly concerned group of individuals 'fundamentalist', Westin is suggesting that they are too extreme and irrational in their views and should not be considered in policy decisions (EPIC 2005). EPIC argues that in fact these individuals have reasonable concerns. For example, Oscar Gandy claims that the extent to which individuals in Westin's study had heard or read about potential misuse of consumer information was a strong explanatory factor in their concern and deteriorating trust (ibid). Similarly, by labelling the largest category as pragmatists, Westin projects this group in a positive light with balanced privacy attitudes and as the only group worthy of policymaking decisions (ibid).

The categorical distinctions of the Dynamic are further questioned by EPIC due to the fact that individuals in all three sectors of the Privacy Dynamic take special measures to protect their privacy (ibid). A Harris June 2004 poll showed that privacy fundamentalists and pragmatists both engaged in a high level of privacy activism. Out of seven actions, three quarters of privacy fundamentalists had taken four, and 65 percent of pragmatists had taken at least four of the seven actions. Forty-six percent of the unconcerned group had also taken at least four steps to protect their privacy (ibid).

Statistically, EPIC also calls into question the mutual exclusivity of categories in Westin's survey results. They claim that Westin presents results in order to portray more favourable outcomes for those funding the research, when alternate interpretations are available. Also, in terms of question wording, EPIC argues that Westin does not ask questions that deal critically with privacy issues, such as opt-out or opt-in requirements (EPIC 2005). Westin's

surveys are funded by many private businesses. His surveys are published by Privacy & American Business, a project of the Center for Social & Legal Research, which is supported by major banks, airlines, credit reporting agencies, and credit card companies that all have a strong interest in preventing the progress of privacy legislation. Some of these organizations include Equifax Inc., GlaxoSmithKline PLC, First Data Corp, ChoicePoint, Visa International, Double-Click Inc. and Verizon. These companies are consulting clients as well as contribute to the research. EPIC suggests that conclusions of Westin's studies coincide with the interests of these companies (EPIC 2005).

Factors Influencing Opinions

Demographic factors have been demonstrated to have an affect on public opinions of privacy in the U.S., with age, gender and race being the most influential in various studies. In the Harris/Equifax study of 1990, age was the most significant demographic factor explaining attitudes towards privacy. Americans in the 30-49 age group had the highest concerns about privacy and had experienced the most loss of privacy (Louis Harris and Associates 1991). The older age group expressed the most concern and young adults were the least upset about consumer privacy and the most accepting of business use of personal information, especially for benefit (ibid). Bellman et al. (2003) also found that overall concern with information privacy increased with age. Older consumers were more concerned with the amount of private information being collected, unauthorized access to their data and errors in their data, as well as the collection of data of higher sensitivity (ibid, 33).

Gender has sometimes also been considered a factor impacting public opinion on privacy. Bellman et al. report that females were more concerned than males about unauthorized secondary

use of information on the internet, but less concerned in a lower-sensitivity context, such as a physical store (Bellman et al. 2003). However, Bellman et al. found no association with education level and privacy concerns. In addition, the Harris/Equifax survey on health information in 1993 found that certain demographic groups felt their privacy was less protected; race, income and education helped to explain these different attitudes. In particular, those with higher levels of income and education were less concerned with privacy in general (Bennett 1996). Demographic breakdowns of public opinion data are a valuable factor in obtaining the complete picture of privacy attitudes.

The level of consumer privacy concern also varies based on the sensitivity and context in which the data is collected. Medical and financial information are more sensitive than other data, and higher levels of concern are expressed in less secure contexts such as the internet (Bellman et al 2003). Consumers are more concerned with privacy in online transactions, however, sensitivity to privacy issues online decreases with internet experience (Bellman et al. 2003). Consumers are mostly concerned with how financial and medical information is handled. Alan Westin claims that strong majorities of these individuals favour enacting new privacy laws and rules for medical and financial information (Westin 2000). Concern is higher when personal or financial information is sold by one company to another without consumer permission (Wang and Pertison 1993; Bellman et al 2003). Less concern is demonstrated over the sale of information when a prior relationship exists, if consumers are first contacted, if it is relevant to the transaction taking placer and if the individual can control future use. Sensitive data such as racial origin, political or religious beliefs, health and sex life, criminal behaviour are considered more risky and require greater safeguards by the public (Bennett 1996).

Consumer Concerns and Reporting of Changed Behaviour

There is also some indication in public opinion polling on privacy that Americans are changing their behaviour to protect their personal information. In 2000, IBM-Harris found that 78 percent of Americans reported that they had refused to give information to a business for privacy reasons. In this study, 55-64 percent refused to give personal information to financial, retail, health or insurance web sites or refused to purchase goods of services because of concerns (IBM-Harris 2000). In 2002, a Harris Interactive poll surveyed 1,529 adults and found that 87 percent had refused to give information to a business they felt was too personal or unnecessary and 83 percent asked a company to remove their name from a mailing address (Harris 2002). In June 2004, a Harris poll by Privacy & American Business, sponsored by Microsoft, surveyed 2,136 adults online. They found that two-thirds of Americans have taken serious steps to protect their privacy, such as 60 percent not shopping at a store because of doubts about the companies' privacy protections, 87 percent requesting a company remove their information from a marketing database and 65 percent not registering on an e-commerce site because of privacy concerns (Privacy 2004). A Harris Interactive national poll of 1,962 Americans conducted for Office Depot in 2005, found that 67 percent of respondents shred credit-card offers and bills, 25 percent do not sign the back of their credit cards so that service clerks will ask for their identification and 7 percent used only cash for purchases to prevent a paper trail (Harris 2005).

Furthermore, in addition to Harris polls, according to the 1999 IBM survey, seventy-eight percent of respondents refused to give out their information to a business or company because they believed it was not needed or too personal (Westin 2000, 9). A Pew Internet and American Life study found that 24 percent of internet users gave false information on a web site and 20 percent gave alternative or secondary email addresses (Pew 2000). Despite all of the public

opinion reporting that indicated individuals are taking steps to protect their privacy, Harper and Singleton claim that only a small percentage of individuals actually change their actions based on their privacy concerns, such as opting-out of marketing, using encryption, regularly changing their passwords, or disabling cookies (Harper and Singleton 2001). This may be due to the fact that individuals must balance many competing priorities with privacy concerns.

September 11, 2001 and Changes in Public Opinion

Levels of surveillance by government and private organizations in the US have greatly increased since the terrorist attacks of September 11th 2001 (Lyon and Bonikowski 2001). This has prompted polling on changes in public opinions of privacy after the event. Immediately following the attacks, polls showed a greater willingness by Americans to accept more invasive police surveillance technologies, such as biometric and facial recognition technologies and a decreased concern over privacy (EPIC 2005; Bellman et al. 2003; Taylor 2003). Americans also began to report a higher trust in government (EPIC 2005). This initial support for increased surveillance of transactions, emails and the internet have now subsided and concern over privacy is again increasing.

As an illustration, the longitudinal Harris/Westin surveys showed lessened concerns over privacy after 9/11. A 2003 Harris Interactive survey reported that 69 percent of consumers agreed that consumers have lost all control over their privacy, a decline from 80 percent in 1999. Fifty four percent of respondents disagreed that most businesses handled consumer information properly and confidentially, up from 35 percent in 1999. Lastly, 53 percent agreed that existing laws were reasonable, an increase of 15 percent since 1999 (Taylor 2003). These results

indicated that privacy concerns were declining and becoming is less important to American consumers from 1999 to 2003.

Also after 9/11, support grew for invasive surveillance technologies such as national identification cards and biometric technologies. A Harris poll, conducted soon after the attacks, found that 68 percent of Americans supported implementing a national identity system and that 86 percent supported facial recognition technology (Harris 2001). This report also found that respondents were concerned that new surveillance technologies would increase the risk of police abuse. Forty-four percent of respondents were highly concerned about the risks of profiling based on nationality, race, or religion as well as 45 percent being highly concerned with the monitoring communications by innocent people (Harris 2001). A January 2003 Harris poll also found that the majority of the US public, 56-91 percent, find it acceptable for the private sector to use biometric technologies, as long as privacy safeguards are set in place by legislators and adopted voluntarily by companies to protect misuse (Harris 2003).

Using various studies to support their claims, EPIC argues that public support for national identity cards continues to wane. For example, a Washington Post poll from November 2001 reported that only 44 percent of Americans supported national ID. In March 2002 the Gartner Group found that 26 percent of Americans wanted a national ID, and 41 percent opposed the suggestion (EPIC 2005). However, the Ponemon Institute, a think tank dedicated to ethical information management practices and research, conducted 2004 Survey on the Public's Perception of Identity Management. This survey suggests that Americans support the introduction of a universal verification credential, only if managed by a trusted organization. More than 74 percent of respondents in this survey believed a universal identity card would be more convenient (Ponemon 2004). This same study also found that consumers support the use of

biometrics for identity management. Over 70 percent of respondents said they would accept certain kinds of biometrics, such as fingerprinting and voice recognition. Convenience was the top reason; with 88 percent of responded believing this will make identification more accurate and convenient. Only 11 percent were opposed to biometrics and were concerned about secondary uses of the data (Ponemon 2004).

Since the recent terrorist bombings on the transit system in London, England on July 7th 2005, American anxiety over terrorism has again risen. A CNN/USA Today Gallup poll conducted immediately following the event showed a sharp increase in the percentage of Americans believing an act of terrorism is likely to occur in the US within the next weeks, from 35 percent in June to 55 percent in July. This poll also found that two-thirds of Americans support metal detectors and identity verification as a routine part of entering buildings and public places, as well as the establishment of national identity cards. These individuals however, were also reluctant to expand government surveillance of private communication or unreasonable searches (Saad 2005).

With the increasing levels of surveillance by government after 9/11, debate about government openness versus security and privacy has arisen. Many advocates for open-government claim that the government has become more secretive at the expense of democracy, while government supporters argue that national security concerns are currently more important than openness and privacy. Complaints about government openness have prompted the US Senate to revisit the Freedom of Information Act. A poll was conducted by Ipsos for Public Affairs for Sunshine Week, a coalition of media organizations and other groups fighting for government access. Ipsos surveyed 1,003 adults from March 4-6 and found that over half of Americans believe the government should provide more access to government records (Tanner

2005). Seventy percent of those surveyed are concerned with government secrecy and 52 percent claim there is too little access to government records. However, there was little change in these public opinions compared to a similar poll in February of 2000, showing constant concern over the importance of access to information (ibid).

Public Opinion on Privacy and the Law

It is generally accepted that the level of government involvement in the regulation of information privacy is associated with the level of privacy concern in that country (Bellman et all 2003; Milberg et al 1995). Milberg et al (1995) found an "inverse-u" relationship between the level of government regulation and concern for information privacy within a country. In other words, high levels of concern over information privacy are associated with high levels of government regulation and low levels of concern with lack of regulation, but the highest levels of concern are associated with the most moderate level of government regulation of privacy practices. Thus, highly publicized infringements on privacy raise levels of privacy concern and create pressure for increased regulation (Milberg et al 1995; Bellman et al 2003). However, Bellman et al did not find the 'inverse-u' effect in their research. The USA has a low level of government involvement with a self-regulatory approach to privacy regulation, suggesting a low-level of privacy concern. However, this is changing due to recently publicized privacy breaches in business as well as legal changes.

EPIC argues that American public opinion polling consistently finds strong support for legalizing privacy rights to protect their personal information from government and commercial organizations (EPIC 2005). For example, a February 2002 Harris Poll found that 63 percent of respondents believed current laws were inadequate to protect privacy. In June 2001, a Gallup

poll showed that two-thirds of those surveyed preferred new federal legislation to protect privacy online (Gallup Poll 2001). The Markle Foundation conducted a study in 2001 indicating that 64 percent of respondents favoured rules to protect consumers online, while 58 percent reported that self-regulation was not enough to ensure accountability (Markle 2001). A telephone study of 1,000 adults by the Center for Survey Research & Analysis at the University of Connecticut for the First Amendment Center and American Journalism Review found that 81 percent reported the right to privacy was “essential” (First 2002). Lastly, a Business Week/Harris Poll showed that 57 percent of respondents favoured laws that regulate how personal information is used, and only 15 percent supported industry self-regulation (ibid). There is also some opposition to these claims, for example IBM found that fifty-nine percent of respondents believed the existing laws and organizational practices in the United States provide a reasonable level of consumer privacy protection (IBM 1999).

US Public awareness of privacy issues in the private sector have recently been heightened due to increased reporting of commercial privacy breaches within the media. With the introduction of new privacy laws in California in 2004, businesses and agencies are required to notify consumers of all security breaches involving their personal information. Data security is increasingly being questioned by the public because large amounts of personal financial data have been misused or lost by banks, data brokers and universities. For example, over sixty cases of data breaches have been reported in the US media, involving the personal information of over 50 million people (Privacy Rights 2005). This reporting began with ChoicePoint Inc. who sold information to fraudulent customers on over 145,000 consumers in October of 2004; information on the breach was not released until February of 2005 at the request of law enforcement. Also in February, the Bank of America Corporation lost several tapes containing credit card information

on 1.2 million customers. In March, DSW Shoe Warehouse lost 1.4 million credit card records to hackers, including drivers' licences and checking account numbers from 96,000 checking transactions (Acohido and Swartz 2005). LexisNexis lost password data on 310,000 customer files in March and April. The largest breach occurred in June of 2005 at CardSystems Solutions, an Atlanta-based payments processor that had 40 million account records stolen from customers from MasterCard (13.9 million), Visa USA, American Express and Discover cards (Acohido and Swartz 2005; Sahadi 2005).

It is difficult to predict if there has been an increase in data security breaches since the California laws were introduced in 2004, or whether cases of data loss were previously merely unreported to the public. These new state laws are providing incentive for companies to provide more security to their clients to prevent data breaches that cost the company in damage to public reputation as well as financial losses (Sahadi 2005). These instances of data breaches are creating pressure on lawmakers at the state and federal level to increase protective privacy legislation, which suggests a growing concern with privacy by consumers. National debate has arisen and legislative hearings have been set in Washington to increase consumer protection. A trend toward increased privacy protections for consumers is growing.

Another example of successful privacy regulation over the private sector is the Federal Trade Commission's Do-Not-Call Registry for telemarketing. Ninety-seven million Americans have registered their phone numbers to opt-out of being called by telemarketers (Bruce 2005). A Harris Poll in January of 2004 surveyed 3,378 adults and found that 91 percent had heard of the Registry. Fifty-seven percent signed up on the registry and 25 percent reported not receiving any telemarketing calls since signing up. Fifty-three percent claimed they still received some

telemarketing calls, but less than before they registered. This poll demonstrated the success of the program and the desire of the public not to be disturbed at home (Taylor 2004).

E-Commerce, Privacy and Trust

E-Commerce

The US have one the most developed e-commerce markets in the world because of a highly developed and affordable information technology infrastructure, as well as a wealthier population which enables access. The US has been the world leader in PC penetration rates since 1995, with 60 percent of the population having PCs. They also have the highest internet diffusion with approximately 35 percent of the population having access (Gibbs et al. 2002). The internet reaches 60 percent of households in the US (Harris Interactive 2002b).

The use of the internet for business has skyrocketed in the US due to globalization, consumer demand, and government promotion of IT. Global and national factors impact the growth of e-commerce in the US. Business-to-business (B2B) e-commerce is pushed by global competitiveness, whereas business-to-consumer (B2C) e-commerce is pulled by consumer market demand for convenience and service (Gibbs et al. 2002). Global production networks, MNCs, trade and global competition drive e-commerce and consumers accept the development of IT. The entrepreneurial business culture in the US encourages the development of e-commerce to reach new markets and gain a competitive advantage. National liberal telecommunication policies, industry support, as well as government promotion by the Clinton/Gore administration have also influenced e-commerce development (ibid).

Privacy Concerns

The growth of the internet and e-commerce in the US has created increased concern over privacy online. Concerns over privacy on the internet are higher than offline because the scope and depth of information collection is far greater than offline; information online can be stored, compared and linked. Privacy is one of the greatest concerns of online consumers; many studies provide evidence of this. Harris Interactive show that privacy concerns are magnified online, with 92 percent of users concerned for threats to privacy online, and 72 percent very concerned (Westin 2000). In an online survey of 1,500 AOL and PC World Internet users in July of 2003, 95 percent claimed they were highly concerned with web sites collecting personal information (PC World 2003). A Yankee Group survey of 3000 online consumers in 2001, found that online privacy continues to be a major concern with consumers, with 83 percent of respondents being somewhat or very concerned about privacy on the internet (Yankee 2001). An American Express survey of 11,000 consumers reported that 79 percent sited privacy and security as major concerns with shopping online (Consumers 2001). A Pew Internet & American Life study found that 54 percent of respondents believed that web site tracking of consumers is harmful and invasive to privacy (Pew 2000).

In particular, consumers are concerned with tracking online habits and sharing of personal information. The PC World survey found that seventy-six percent of respondents were concerned with website's tracking habits (PC World 2003). A 2000 Harris Interactive poll reported that 89 percent of adults were uncomfortable with connecting browsing tracking habits with an individual's identity. Ninety-five percent were uncomfortable with profiling that includes tracking browsing habits, identity, and other data such as income and credit information (Harris 2000). Also, 92 percent were not comfortable with web sites that share their user information

with other organizations and 93 percent were uncomfortable with web sites that sold user information to other organizations (ibid). In 2002, Harris Interactive found that 75 percent respondents were concerned with privacy risks involved in companies selling data to others without permission, 70 percent were concerned with transactions that are not secure, and 69 percent were concerned with hackers stealing personal data (Harris 2002).

Privacy and Trust

E-commerce is dependent on consumer trust in websites because trust is necessary for consumers to make transactions online. Bennett argues that consumer trust and confidence plays a key role in business and government e-commerce (Bennett 1996). Many surveys are indicating that Americans are becoming increasingly concerned with privacy and security on the internet and are more reluctant to make purchases online as they become aware of possible risks involved with sharing their information.

Consumer trust in companies and brands tends to be the largest predictor of product use. The willingness of the public to disclose information with a company depends on the level of trust the consumer has with that companies reputation in handling personal information (Schoenbachler and Gordon 2002; Bellman et al. 2003). The Ponemon Institute found that more consumers give permission to be contacted by the most-trusted companies, and withdraw support for companies with poor privacy performance between 2003 and 2004 (Ponemon 2004). Consumers are willing to trust companies when their concerns are met and sixty-five percent of those surveyed used their credit cards to make purchases online (ibid). A study by Princeton found that experienced internet users were more likely to use their credit card online, with 79 percent using their credit cards online after 3 years of internet experience, and only 36 percent

with 6 months or less experience (Princeton 2002). Earning customer trust and confidence through improved privacy practices is commonly cited as necessary to achieving long-term profitable customer relationships.

Consumer trust in web site protection of personal data is low. Only six percent of US customers had a “high level of trust” in 2001 (Carroll, 2002; Bellman 2003). IBM conducted an international poll and found that 80 percent of consumers in the US believe they have lost all control over how personal information is collected and used by companies (IBM 1999). Harris Interactive conducted a study of 1,529 adults in February of 2002, they found that most consumers do not trust businesses to handle their personal information properly, and 84 percent agreed that an independent verification of company privacy policies should be a requirement (Harris 2002). A study conducted by the Consumers Union and Princeton Survey Research Associates also suggests that consumer trust in buying online is low (Princeton 2002). In a telephone survey of 1,500 adult internet users in 2002, only 29 percent reported that they trust web sites that sell products and services, and only 33 percent trust websites giving advice about products and services. As a comparison, 58 percent of these respondent trust newspapers and television, and 47 percent trust the federal government. The majority of consumers in this study said it was very important to be able to trust a website, very important to post information on how personal information will be used and to display privacy policies (ibid).

A consumer study by RSA Security suggests that one-quarter of online shoppers have reduced their purchases in the past year because of rising concerns over identity theft. Consumer confidence in companies dealing with identity theft is declining as awareness of the issue grows (Kawamoto 2005). Twenty-one percent of customers will not use online banking and seventy percent of consumers felt that online merchants were not doing enough to protect their personal

information (ibid). Consumers International also found that concerns over confidentiality and security rank highly in why consumers do not buy online. They predict that e-commerce will suffer immensely if this issue is not addressed (Consumer 2001). Forrester Research estimated that online sales were reduced by 2.8 billion in 1999 due to privacy concerns (ibid).

The PEW Internet and American Life Project revealed high anxiety in the future of the internet by a group of experts in the field. PEW surveyed 1,286 individuals in 2004, ranging from experienced technology leaders, scholars, industry officials, government and the public. Most of these experts expect attacks on the network infrastructure in the next decade, with 66 percent agreeing that at least one devastating attack will occur. The majority of those surveyed, 59 percent, also believe that surveillance by government and business will grow as computing devices become embedded in appliances, cares, phones and clothes (PEW 2002).

Give up Privacy for Benefits

Despite high levels of concern about privacy online and low ratings of website trust, the number of consumers buying online continues to grow on the internet (Turner and Varhese 2001; Harper and Singleton 2001; Bellman et al 2003). Americans conduct the greatest amount of online payments in the world (Gibbs et al. 2002). Fifty percent of Americans bought online in 2000, up 20 percent from 1998, and credit card transactions online are growing (Harper and Singleton 2001). Consumers continue to use websites and are not aggressive in seeking privacy information even when it is available. Consumer actions are the best indicator of true preferences and real world actions tend to reflect different attitudes than polls suggest (Harper and Singleton 2001). However, some research suggests that online buying would greatly increase if privacy concerns were more effectively addressed (Bellman et al 2003).

Americans tend to be willing to exchange their information privacy in return for social or economic benefit (Long and Quek 2002; Bellman et al 2003; Ponemon 2004). Individuals assess the costs and benefits of revealing their personal information. The Ponemon Institute found that despite increases in privacy concerns, the majority of people are willing to take significant risks in sharing their information in exchange for a small benefit, such as free software, services or coupons (Ponemon 2004). Their studies also show that the American public will choose convenience over privacy, such as sharing large amounts of personal information with the federal government in order to pass more quickly through airport security checkpoints (ibid).

Berendt, Gunther and Spiekermann conducted a large scale online shopping experiment with 206 participants and found that privacy statements had no impact on user behaviour. These researchers first conducted a survey which revealed that individuals were opposed to data collection and doubted the privacy protection of web sites. When they performed an online shopping experiment with these same users, individuals did not act in accordance with these opinions. These authors uncovered that users would give away personal information in return for benefits, in particular for a 60 percent discount on shopping (2005).

Public Opinion of Privacy Regulation Online

Gibbs et al. suggests that the lack of legislation in the US may be hampering growth of e-commerce in the US (2002). Additionally, Bellman et al. claim that cross-national differences in privacy laws have been identified as one of the ten most important trends to impact the internet in the next five years (Erbschloe 2001; Bellman et al. 2003). Protection of consumer data will be very important to trust in online transactions to minimize privacy concerns in various regions. Data protection and assurance of FIPs in self-regulation play a key role in establishing consumer

trust. Trust, privacy and financial safeguards are the greatest possible enhancements of consumer engagement in e-commerce activities (Gibbs et al. 2002). The strongest legislation in the US is emerging in the areas of greatest public concern.

Opinion polls indicate that consumers prefer legislation to protect their privacy online. A Harris Interactive poll in 2000 found that 57 percent of respondents favoured laws to regulate how personal information is collected and used. Thirty-five percent reported that privacy notices were absolutely essential and 40 percent reported that privacy notices were very important, for a total of 85 percent (Harris 2000). A 2003 Harris poll, surveying 1,010 adults found that fifty-three percent disagreed that existing laws and organizational practices provide a reasonable level of protection for consumer privacy (Harris 2003). Forrester Research found that only 6 percent of Americans have a high level of trust in the storage of their personal information by web sites and that 7 out of 8 are interested in legislation that will protect internet privacy (Forrester 2001).

Similarly, consumers report that they want to have control over their information online. A Harris poll found in 2003 that 79 percent of respondents find it extremely important to be in control of who can access their personal information. Sixty-nine percent also reported that it is extremely important to control the collection of personal information (Harris 2003). Ponemon found that 84 percent want to be notified if there has been unauthorized access to their data (2004). A Pew Internet & American Life Project of 2000, conducted a survey of 2,117 Americans, and found that 86 percent would support opt-in privacy policies before companies use personal information (Pew 2000). In a 2000 Harris study, 88 percent also agreed that websites should gain opt-in consent before sharing personal information with others (Harris 2000).

Regardless of these consumer desires, the majority of websites do not have effective privacy policies to protect consumer information. Consumers International reports that the majority of websites in the US and the EU do not meet international standards for providing data protection and ignore basic practices of FIPs. Sixty-seven percent of websites collected personal information for using the site and only 58 percent had a privacy policy. Merely 32.5 percent of the websites that collected information had a privacy policy alert to consumers and many do breach their own privacy policies. The most popular sites were more privacy conscious (Consumers 2001). Also, Bellman, Johnson and Lohse 2001 found that online organizations can guarantee consent to privacy policies with the right combination of question framing and default answers. For example, if marketers want individuals to agree with their privacy policy, they must merely make yes the response for taking no action (Communications 2001). This indicates that privacy regulations should include reference to the form of question wording to attain consumer consent.

Some studies have demonstrated public ignorance of business practices and the use of personal information online. A national poll of 1,500 Internet users in the US was conducted by the Annenberg Public Policy Center of the University of Pennsylvania. They discovered that while 80 percent of respondents were aware that companies have the ability to track internet users on the web, about half of respondents believed falsely that online consumers could see their own data, they could erase their information from the company, companies are barred from selling their personal information. Seventy-three percent believe falsely that companies cannot share information with affiliates, and 75 percent falsely believe that the presence of privacy policies on web sites means that the company cannot sell their information to others (Turow et al. 2005). A similar 2003 poll found that 59 percent of respondents did not know that websites

collect information even if there is no registration requirement on the site (Turow 2003). Likewise, Pew found that 56 percent of respondents could not identify a cookie, a common internet tracking technology (Pew 2000).

Academic studies typically suggest there is a greater need for consumer education on privacy (Culnan 1995; Bellman et al 2003). Knowledge about internet privacy will decrease privacy concerns and demands for increased government regulation. However, Bellman et al. (2003) found no correlation with familiarity with privacy policies online and privacy concern. They also argue that public education about privacy laws and policies will make little difference in privacy concern.

Forrester Research interviewed legal, academic, industry experts and application and content developers in 2001. These individuals concluded that companies need to institutionalize respect for privacy in order to become credible organizations (2001). Harper and Singleton point out that this demand for laws in public opinion polls is used as justification for regulation, but fails to address what types of laws are needed and does not take into account the high cost of regulation (Harper and Singleton 2001). Data protection policies are good business practice, but it is costly for companies to implement security measures to minimize breaches, such as IT support and encryption technologies.

Conclusions

Cultural values in the US lean towards individualism, achievement, trust in private sector organizations and lack of government regulation. This has resulted in very limited privacy oversight by the government in the US, with reliance instead on a free-market approach with a model of industry self-regulation. The spattering of privacy legislation that does exist is not

always properly enforced. Additionally, pro-surveillance legislation has greatly increased since the terrorist attacks of 9/11 as well as the degree of public willingness to give up certain aspects of privacy for national security. This raises concerns for the civil liberties of US citizens as well as international business partners for the protection of consumer information in trans-border transactions. Public opinion polls of varying levels of quality indicate high levels of privacy concern, which are used within policy debates on privacy. While these survey results help to indicate trends in public opinions on privacy, they do not offer answers why the public feel this way or proper policy choices; a gap may exist in these opinions and reality. Increased reporting of privacy breaches in the private sector is leading to rising public concern for the protection of personal information and the demand for privacy legislation in this area. This has resulted in new privacy laws at the state and federal level. Privacy protections online will be important to the development trust and the growth of e-commerce. Despite being an individualistic culture that does not tend to favour regulation, the public is beginning to demand increased privacy protections over the storage and use of their personal information in electronic transactions by business and government, as well as take their own steps to this end.

References

Achido, Byron and Swartz, Jon. 2005. "ID thieves search ultimate pot of gold- databases", *USA Today*, June 21, Available: http://www.USatoday.com/money/perfi/general/2005-06-21-big-score-USat_x.htm.

Bellman, Steven, Johnson, Eric J., Kobrin, Stephen J. and Lohse, Gerald L. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers". *The Information Society*, Vol. 20, pp. 313-324.

Bellman, Steven, Johnson, Eric J., Kobrin, Stephen J. and Lohse, Gerald L. 2003. *International Differences in Information Privacy Concern: Implications for the Globalization of Electronic Commerce.* May 7, Columbia Center for E-Business; Wharton Forum on Electronic Commerce.

Bennett, Colin J. 1996. *How do public attitudes on privacy vary among nations: A comparative analysis of national privacy surveys.* Prepared for the Global Privacy Project of the Center for Social and Legal Research, September 1996, Available: http://www.privacyexchange.org/iss/surveys/Codesum.html.

Bennett, Colin J. and Raab, Charles D. 1996. *The Governance of Privacy: Policy instruments in global perspective*. Burlington, VT: Ashgate.

Berendt, Bettina, Gunther, Oliver, and Spiekermann, Sarah. 2005. "Privacy in E-Commerce: States preferences vs. actual behaviour", *Communications of the ACM*, Vol. 48, No. 4, pp. 101-106.

Business Week/ Harris Poll. 2000. "A Growing Threat", *Business Week Magazine*, March.

"California lawmakers back tougher identity theft law", 2005. *Reuters*, June 21, Available: http://www.reuters.com/newsArticle.jhtml?type=topNews&storyID=8856054.

Cockfield, Arthur J. 2004. *A Comparative Analysis of Canadian and Foreign Private Sector Privacy Laws: Background Paper for the SSHRC Global Data Project*. Queen's University, November.

Cranor, Lorrie Faith, Reagle, Joseph and Ackerman, Mark S. 1999. "Beyond Concern: Understanding net Users' attitudes about online privacy", *AT&T Labs-Research Technical Report TR 99.4.3*, Available: http://www.research.att.com/library/trs/99/99.4/

EPIC. 2005. *Public Opinion on Privacy*. Available: http://www.epic.org/privacy/survey/

Forrester Research. 2001. *Surviving the Privacy Revolution*, March 2001

Gallup Poll. 2001. *Majority of E-mail Users Express Concern about Internet Privacy But only 28 % are "very" concerned*, June 28.

Gallup Poll. 1999. February 8-9.

Gardner, David W. 2005. 'Poll: Consumers Fret About Online ID Theft But Still Don't Protect Themselves', *InternetWeek.com*, AugUSt 5, Available: http://www.internetweek.com/news/167600309

Gay, Lance. 2005. "National ID cards may be on the way", *Scripps Howard News Service*, April 26, Available: http://www.knoxstudio.com/shns/story.cfm?pk=IDCARDS-04-26-05&cat=AN

Gellman, Robert. 2002. *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, Privacy and Information Policy Consultant, Washington DC, March, Available: http://www.epic.org/reports/dmfprivacy.html

Gibbs, Jennifer, Kraemer, Kenneth L. and Dedrick, Jason. 2002. *Environment and Policy Factors Shaping E-commerce DiffUSion: A Cross-Country Comparison.* Center for Research on Information Technology and Organizations, November, University of California: Irvine.

Harper, Jim and Singleton, Solveig. 2001. *With a Grain of Salt: What consumer privacy surveys don't tell US*. June.

Harris Interactive Survey. 2005. May.

Harris. 2003. March 19.

Harris Interactive. 2002. Privacy *On and Off the Internet: What Consumers Want*, February 19.

Harris Poll. 2001. August 14875.

Kawamoto, Dawn. 2005. "Study: Security fears daunt online shoppers", *CNET News*, February 14, Available: http://news.com.com/2100-1029_3-5575569.html

Knowing it by Heart: Americans Consider the Constitution and its Meaning. 2002. Public Agenda and the National Constitution Center, September 17.

Kollars, Deb. 2005. "US follows state's lead on data-theft notification", *Sacremento Bee*, June 22, Available: http://www.sacbee.com/content/news/courts_legal/story/13107155p-13951810c.html.

Lichtblau, Eric. 2005. "Plan Would Broaden F.B.I.'s Terror Role", *The New York Times*, May 19, Available at: http://www.nytimes.com/2005/05/19/politics/19terrror.html?ex=111.

Lustigman, Andrew B. and Ezor, Jonathan I. 2005. "Privacy Policies: A trap for the unwary", DM News, February 11, Available: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=31855.

Louis Harris and Associates. 1991. *Harris-Equifax Consumer Privacy Survey*. Atlanta, Georgia: Equifax Inc.

Lyon, David and Bonikowski, Bart. 2003. *The History of Privacy in the United States*.

Magnuson, Gail and Reid, Peter. 2004. Privacy and Identity Management Survey: Summary of Results and Findings, White Paper: Privacy and identity management survey, EDS, Available: http://www.eds.com

Mark, Roy. 2005. "Somebody has got to pay", *InternetNews.com*, May 17, Available: http://www.internetnews.com/security/article.php/3505826

Online Privacy Continues to be a Major Concern for Consumers. 2001. Yankee Group Trend Summary, August.

Pew Internet & American Life Project. 2005. *The Future of the Internet*, January 9, Report number 202-419-4500.

Pew Internet & American Life Project. 2000. *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, The Internet Life Report, August 20, Available: http://www.perinternet.org

Ponemon, Larry. 2004. "Top 5 privacy issues for 2005", *ComputerWorld*, December 21, Available: http://www.computerworld.com/securitytopics/security/story/0,10801,98448,00.html

Princeton Survey Research Associates. 2002. *A Matter of Trust: What Users want from web sites*, Results of a National Survey of Internet Users for Consumer WebWatch, January.

Privacy & American Business. 2003. *Identity Theft: New survey & trend report*. Conducted by Harris Interactive, August.

Privacy & American Business. 2004. June 10.

"Privacy & American Business' Alan Westin Presented with 2005 Privacy Leadership Award", 2005. *I-Newswire.com*, March 11, Available: http://i-newswire.com/pr9832.html

Privacy International. 2004. *Privacy and Human Rights 2004: An International Survey of Privacy Laws and Developments: The United States of America*, in Cooperation with the Electronic Privacy Information Centre (EPIC), Available: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-83512

Privacy Rights. 2005. A *Chronology of Data Breaches Reported Since the ChoicePoint Incident*, July 20, Available: http://www.privacyrights.org/ar/ChronDataBreaches.htm

"Privacy Security Abroad Might Help US", 2005. *Associated Press*, June 15, Available at: http://www.newsfactor.com/story.xhtml?story_id=36460.

Saad, Lydia. 2005. 'Americans Reject Extreme Anti-Privacy Security Measures', *Gallup News Service*, AugUSt 8, Available: http://www.gallup.com/poll/content/?ci=17686

Sahadi, Jeanne 2005. "ID data breaches: As rampant as it seems", CNN Money, June 21, Available: http://www.money.cnn.com/2005/06/21/pf/breach_followup/?cnn=yes.

Screeton, Lisa Scott. 1998. "There's no business like your business: protecting consumer privacy online, *Business America*, AugUSt.

State of the First Amendment. 2002. First Amendment Center, AugUSt.

Talvi, Silja J. A. 2005. 'One Nation, Under Watch', *AlterNet*, AugUSt 8, Available: http://www.alternet.org/rights/23917/

Tanner, Robert. 2005. "Poll shows concern about gov't secrecy", *Grand Forks Herald*, March 13, Available: http://www.grandforks.com/m1d/grandforks/11123119.htm.

Taylor, Humphrey. 2004. "Do Not Call Registry is Working Well, More than half of all US adults say they have signed up and they now receive fewer telemarketing calls or none at all", *The Harris Poll #10*, February 13.

Taylor, Humphrey. 2003. "Most People are "Privacy Pragmatists", Who, While Concerned about Privacy Sometimes Trade it Off for Other Benefits", Harris Interactive Poll, March 19, Available: http://www.harrisinteractive.com/harris_poll/printerfriend/index/asp?PID=365.

"The Great American Privacy Makeover", 2003. *PC World*, November.

"To Opt-In or Opt-Out? It Depends on the Question", 2001. *Communications of the ACM*, February.

"The IBM-Harris Multi-National Consumer Privacy Survey", 2000. *Privacy & American Business*, Vol. 7, No. 6, January

The Internet and the Family 2000: The View from Parents, The View from Kids. 2000. University of Pennsylvania's Annenberg School for Communication, May.

Toward a Framework for Internet Accountability. 2001. The Markle Foundation, Greenberg Quinlan Research, July.

Trust and Privacy Online: Why Americans Want to Rewrite the Rules. 2000. Pew Internet & American Life Project, August 20.

Turow, Joseph. 2003. *Americans and Online Privacy: The System is Broken*, Annenberg Public Policy Center, June.

Turow, Joseph, Feldman, Lauren, Meltzer, Kimberly. 2005. *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, June 1.

UNESCO. 2002. *Country Profiles of E-Governance*, The Commonwealth Network of Information Technology for Development Foundation (COMNET-IT), United Nations Educational, Scientific and Cultural Organization, Paris.

Westin, Alan F. 2000. "Intrusions: Privacy tradeoffs in a free society", *Public Perspective*, November/December, pp. 8-11.

Weston, Liz Pulliam. 2005. "The top 10 states for privacy protection", *MSN Money Central*, March 8, Available: http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P57067.asp