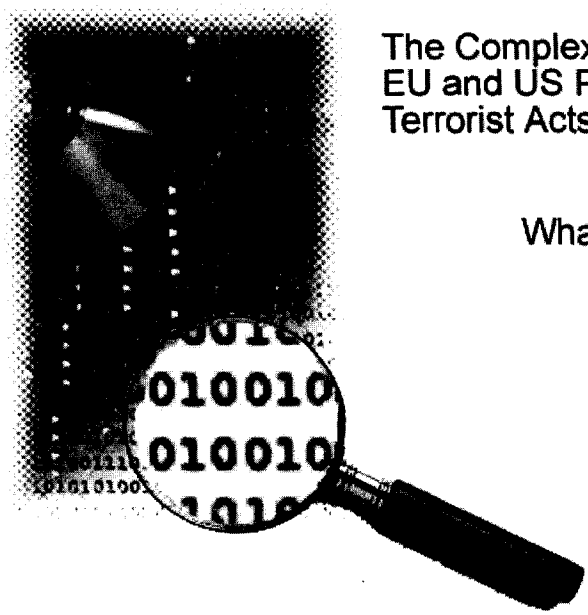


The Complexities of Privacy Concerns in the EU and US Pre and Post 21st Century Terrorist Acts in the Digital Age:

What Does the Future Hold?

By John Karbaf
April 28, 2006

University Of Tennessee – Knoxville

College Scholars/University Honors Senior Project

Mentor: Dr. Karen Levy

The Complexities of Privacy Concerns in the EU and US Pre and Post 21st Century Terrorist Acts in the Digital Age: What Does the Future Hold?

By John Karbaf

Mentor: Dr. Karen Levy

Table of Contents

Introduction	1
The European Data Protection Directive and the US Response	4
Privacy in the US and Europe – An Overview of Differing Positions	11
A Data Protection Solution – Courtesy of Europe	18
Prevalence of Internet in Daily Lives	21
Terrorism in the 2000s and its Apparent Role in Reversing Previous Privacy Policies	30
Culture of Privacy	35
In Conclusion: Should the US move to create national privacy legislation?	40
Appendix I: Microsoft Privacy Legislation Letter	44
Appendix II: Poll/Survey Data Regarding the Public's Opinion on Privacy	54
Works Cited	57
Bibliography	60

The Complexities of Privacy Concerns in the EU and US Pre and Post 21st Century Terrorist Acts in the Digital Age: What Does the Future Hold?

Privacy is a constantly evolving concept that affects all individuals. Since privacy is never restricted to one medium, it is a very fluid concept that can be applied in many different areas affecting many different entities. Given the breadth of its application, this project will concern the handling of privacy in two arenas: the United States (US) and the countries in the European Union (EU).

The concept of privacy evolved into a more important issue in light of two recent changes within modern society. The first concerns the introduction and evolution of the internet and World Wide Web. Privacy has always been an important matter, but its implications in terms of personal data collected on individuals has, in the past, always been limited by the practicality of the ability to collect, store, manage, and transfer that data. With the advent and proliferation of computers in the mid-twentieth century, large-scale data collection, storage, and management became an actuality. Still, the worry over the transfer and dispersion of that data had yet to be realized, as computer storage at that time was largely localized to the machines (large and immovable), and the availability of computer devices was still restricted to mostly large businesses and governments, as the cost to purchase and maintain these machines was extremely prohibitive for the average individual.

That all started to change in latter half of the twentieth century, with the introduction of the personal computer. Further development in the 1980s and 1990s gave rise to PCs for the general population, creating an increase in personal use in homes. In the early 1990s the World Wide Web was unleashed to the general public, and its use too,

grew amongst individuals. With the growth of the internet, large scale data transfers now became a reality, with transfers that could take place all over the world, from anyone with a computer and a transmission line (telephone, fiber optic, etc.). While this was a positive development in terms of commerce and communication, it presented itself as a problem for slow-moving governments and authorities who were ill-equipped to deal with this type of technological advance. At least in the case of the US, where the policy tends to be a reaction to privacy concerns, the laws had yet to catch up with the fast pace of technology.

While the advent and proliferation of the internet was an important and serious threat to personal privacy, there was another change in recent history that transformed how privacy is viewed and applied: terrorism. Though hardly a new subject, terrorism in the early twenty-first century had a great impact on privacy in Western nations. Now that the ability to transfer and store information has become relatively easy and commonplace, so too have governments' abilities and desires to control that data, and possibly invade that privacy. Terrorist attacks in the United States in New York City and Washington D.C. and recent bombings in London and Madrid have encouraged governments to pass legislation in the interest of national security, while possibly invading the privacy of private citizens. This legislation includes the United States' Patriot Act and the European Union's Data Retention agreement.

The study of privacy concerns between the US and EU holds importance for several reasons. The US and EU, arguably the two main powerhouses in the West, both have privacy issues to confront, especially in light of recent events. Though their citizens may ultimately feel the same regarding the protection of their data and information, the

two entities' approaches to addressing the problems remain very different. Ultimately, the main difference remains either the presence or lack of national, broad-sweeping privacy legislation. Already implemented in the EU, the US has yet to affect the same type of policy. However, as threats to personal privacy grow, especially data privacy, it will become more pertinent that actions be taken, preemptively, to protect the personal data of individuals. Its importance has greater implications than simply protecting one's phone number. In a society where information equals power, the people who can collect and use this information should be regulated with regard to purpose, intent, and ultimately responsibility. As such, this project will examine the differences in the ways that personal data privacy is handled between the two powers (US and EU), centering on the EU's Data Protection Directive and focusing largely on electronic communication and the challenges presented to data privacy as a result of its constant innovation. This project also seeks to investigate the effects of terrorism in western nations in the early twenty-first century and the threat to privacy that these acts have created.

The European Data Protection Directive and the US Response

The EU, through its development of the European Data Protection Directive, created comprehensive privacy legislation governing the flow of data of European citizens outside of Europe. Its primary goal was to protect member nations' citizens' data, particularly in terms of data flows or transfers. For the most part, this dealt with business transactions. The legislation, known as the European Data Protection Directive came into binding existence in 1998.[1] The directive's purpose was not so much the desire to create data protection within Europe, rather, its purpose was "to promote the free flow of personal data by harmonizing privacy laws among the 15 member states" of the European Union.[2] The directive allowed the member states to implement the directive in a variety of ways, yet still required that all of the elements be present within their implementation. Furthermore, the European Court of Justice possessed the jurisdictional ability to force a member state to bring its law in accordance with that of the directive. Finally, the directive was deemed binding on the day it became law, October 25, 1998[3], regardless of whether the member states had implemented their own flavor of it yet.[4]

Consisting of seven chapters (General Provisions, General Rules on the Lawfulness, Judicial Remedies, Liability and Sanctions, Transfer of Personal Data to Third Countries, Codes of Conduct, Supervisory Authority, and Community Implementing Measures)[5] the Directive's role really existed within the member states. Data protection commissioners employed within each member state could monitor the data flows, and could only prosecute any data flows deemed to be in violation within that

member state[6]. So, in essence, the practice of the directive remained at a national level and never even encountered the EU, except in the case of the national data protection commissioners working with the Article 29 Working Party and Article 31 Committee to determine, "whether a third country had 'adequate' data protection laws or mechanisms to allow EU data exports to that jurisdiction."[7]

In essence, the Directive required that businesses sending information on persons, personal data, make sure the receiving party was bound under comprehensive data protection laws in their country of residence.[8] By definition, the directive termed this – "adequacy." So, the directive followed similar to this: If a company in the EU wished to send marketing or payroll data to another company in another country, that country had to have an adequacy finding under the directive. This meant countries with comprehensive data privacy protection legislation were deemed adequate; those without were left little option but to enact it (as many did) or risk halting international trade between their country and the EU altogether. Heisenberg illustrates an example:

> ...once the Commission determined that, for example, Canada met the adequacy standard, it was no longer permissible for national data protection commissioners to prevent data flows to companies located in Canada. The Canadian company could be prosecuted by Canada's data protection commissioner for violating the country's laws, but the Europeans would not be allowed to block transfers to that company, unless it were found guilty of violating Canada's privacy law.[9]

Again, as Heisenberg hints above and notes later on, the European Data Protection Directive was hardly an effort to exert influence over other countries. Within the EU, all data protection occurred at the member nation level, and any interaction involving the

stoppage of data flows to foreign companies only occurred once the company in question violated its own native country's data protection law. Only then was action taken within the EU, in the form of a possible halt of data flows.

Conflict with the Directive, for our purposes, arose with regards to trade between the EU and US and the potential for a halt of data flows. As a rule, the US legal system and constitution grants and attempts to protect a fundamental right to privacy for all citizens. However, this rule, unlike the Bill of Rights in our constitution, is unwritten:

> In the United States, unwritten law takes on a variety of forms. In constitutional law the Supreme Court has ruled that the Due Process Clause of the Fifth and Fourteenth Amendments to the U.S. Constitution protects the right to privacy even though the word *privacy* is not mentioned in the written text of the Constitution.[10]

Thus, as demonstrated, privacy exists as record in judges' opinions, court case precedents, and overall court interpretation on a case-by-case basis. As such, there is no comprehensive, strictly prescribed, broad-sweeping privacy legislation in the US.

Privacy, thus, in the US, is legislated in a different context. History has shown that the government and business within the US are not without concern for data privacy protection; legislation does exist to protect it, however, that effort is largely sector-based, with legislation corresponding to specific practices within specific industries. Efforts to attempt national legislation in the past failed, often without ever gaining ground. All too often, businesses' opposition to such legislation erased its future existence. Additionally, in the spirit of a capitalist and free market society, government interference and control is often seen as a bad thing, and a barrier to trade. In fact, it was claimed that if the market

required and demanded it, it would be done, more in a business/economic sense than anything else.

The introduction and creation of the Data Protection Directive posed a problem and created headaches on both sides of the Atlantic. The US, in no hurry to be forced into drastic legislation by another global economic power, vehemently opposed national privacy legislation. Rather, they favored and put forth the idea of business self-regulation according to privacy principles (for businesses in the US) instead. The EU, not about to withdraw and/or amend (and subsequently weaken) its own privacy directive aimed to protect its citizens was unwilling to accept the US self-regulatory approach. As a result, transcontinental trade was about to be derailed between the two and, at least in the general public, hardly a soul knew about it.

As a result of the United States' lack of comprehensive privacy legislation, or merely, data protection legislation, the EU could not grant the US an adequacy finding for transnational data flows.[11] By very definition within the Directive, the only way the EU could take action against a foreign company improperly handling personal data was if the country violated data protection laws within its own nation. Of course, therein lays the problem, in how can data be protected and monitored against certain guidelines, if those guidelines simply do not exist?

Fortunately, for business and trade interests, a breakdown in transatlantic data flows between the US and EU did not occur. The solution presented itself in a manner that was acceptable to the US government, designed primarily by US business, and somewhat grudgingly accepted by the EU. The solution came in 2000 under the title of Safe Harbor. The US Department of Commerce describes it fairly well:

> The safe harbor -- approved by the EU this year -- is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Certifying to the safe harbor will assure that EU organizations know that your company provides "adequate" privacy protection, as defined by the Directive.[12]

Safe Harbor was the solution to solve the stalemate brewing between the US and EU over the Directive. As it has been explained, the conflict arose after the passage of the Directive. The US, not possessing comprehensive privacy legislation, would not meet an adequacy finding under the qualification of the Directive and its Article 29 Working Party ("The Working Party gives advice about the level of protection in the European Union and third countries."[13]). As such, billions of dollars worth of trade depending on transborder data flows from the EU to the US were in jeopardy of being halted. In the interest of trade, a solution would have to be reached. Of course, there were certain sentiments that arose after the passing of the Directive, and those played heartily into the creation and deliberation surrounding Safe Harbor. David Aaron's testimony before Congress highlights some of those sentiments,

> The first thing we established was that the United States was not going to negotiate a treaty or an executive agreement that would apply the EU Directive in the United States...The second thing we made clear is that we were not going to accept the jurisdiction of European law in the United States...We were prepared to have voluntary self-regulation within the framework of existing U.S. law. We were not going to pass new legislation.[14]

With the idea that the US would absolutely not create new legislation to bend to the will of the EU, both sides began to work out the possibility of self-regulation. The idea was that if the government "couldn't get the country to be considered, 'adequate,' maybe what we could get considered adequate are the companies."[15] The Safe Harbor Agreement is, in theory, fairly simple. It is a self-regulatory approach for businesses that operate globally, particularly those who operate in both the EU and US. As an example, the following illustrates the steps a webmaster would have to perform to act in accordance with the Safe Harbor Agreement: first, write a privacy policy that conforms to what the standards and operations of the website are; second, an optional step, is to sign up with a third party auditing program for your privacy policies. Notable examples include BBBOnline[16] and TRUSTe[17], third, certify yourself with an application filled out and filed with the Department of Commerce. Finally, the last step is to respond to inquiries and complaints with regards to your privacy policies.[18]

The road to Safe Harbor, however, was hardly an easy journey. "Among consumer groups in both Europe and the US there was a (well founded) fear that the Clinton administration was heeding only special interests' views on the issue of privacy."[19] Furthermore, amongst the different reasons against self-regulation from the Europeans came the fear that the US stance on the Directive and their desire for self-regulation would set a dangerous precedent that other countries outside the EU would wish to follow; in essence weakening the adequacy and transborder data flow portions of the Directive.[20] However, with very few other options for resolution on the table, it seemed as though the concept of self-regulation would have to be taken seriously.

As deliberations between the US and EU continued over self-regulation, it became more apparent that while the Europeans might be willing to allow self-regulation for the US, they were still going to contest the characteristics of whatever system was going to be put into place. Of chief concern to the Europeans was protection concerning the privacy of individuals dealing with financial services. "US banking and financial interest had argued that the newly passed Gramm-Leach Bliley (GLB) Act (signed into law on November 12, 1999) and the Fair Credit Reporting Act should be considered 'adequate' for the European Data Protection Directive purposes.[21]" The European Commission, however, remained skeptical, and "countered that several of the Directive's elements, e.g., notice, were not included in these bills, and thus, the acts could not be deemed adequate."[22]

As March 2000 drew nearer, however, it became increasingly apparent that an agreement over privacy covering financial services was not going to be reached. The Department of Commerce, in the interest of expediting the implementation of Safe Harbor, separated "financial privacy from the primary agreement."[23] The new draft (now devoid of financial privacy) of Safe Harbor was delivered March 17 to the member states of the European Union. Shortly thereafter on March 31 the member states then "unanimously approved the Safe Harbor Agreement that the Commission had negotiated, and thereafter, the threat of commercial disruption vanished."[24]

Privacy in the US and Europe – An Overview of Differing Positions

Privacy, though not broadly defined in a national context, does and has existed in the US for sometime now. The difference being, whereas the EU has broad-sweeping legislation concerning data privacy, the US has it in different manners. Manners that include sector-based legislation and through the years upon years of case record, precedent, and judges opinions.

This section's purpose is to give an overview of privacy laws in the United States. While the US was considered inadequate for lacking comprehensive privacy legislation, it was not for lack of legislation. The first inkling of privacy law or record in the United States hails from an article entitled *The Right to Privacy* published in the 1890 Harvard Law Review by Samuel Warren and Louis Brandeis. This article spoke of a "right to be left alone."[25] [26] "However, the codification of principles of privacy law waited until Prosser, *Privacy*, 48 Cal.L.Rev. 383 (1960), which Prosser subsequently entered into the Second Restatement of Torts at §§ 652A-652I (1977)."[27] Prosser defined four parts of the right to privacy as follows:

1. Intrusion upon a person's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about an individual.
3. Publicity placing one in a false light in the public eye.
4. Appropriation of one's likeness for the advantage of another (Prosser 1969, 389).[28]

These definitions of the right to privacy were used as the foundation for several privacy laws, ones such as the 1970 Fair Credit Reporting Act and the US Privacy Act of 1974.

The 1970 Fair Credit Reporting Act (FCRA) was designed and enacted to protect consumers during the disclosure of the personal information by consumer reporting agencies. Its main goal was to prevent the disclosure of inaccurate or irrelevant data. The FCRA does not regulate the type of information collected; however, it does regulate how and to whom that information is disclosed. Specifically, personal data can only be disclosed to third parties under prescribed conditions. Furthermore, the FCRA grants that "information may be released to a third party with the written consent of the subject of the report or when the reporting agency has reason to believe the requesting party intends to use the information:

1. for a credit, employment or insurance evaluation;
2. in connection with the grant of a license or other government benefit; or
3. for another "legitimate business need" involving the consumer."[29]

The US Privacy Act of 1974 actually created its own statement of privacy principles, as a result of a committee created in 1972 by the Department of Health, Education and Welfare whose duty it was to examine the widespread use of computer technology, and in particular, how it applied to government agencies and their respective automated record-keeping systems.[30] The statement of principles, known as the "Code of Fair Information Practices" that resulted from the US Privacy Act of 1974 is as follows:

1. Principle of Openness: The existence of recordkeeping systems and databanks that contain personal data must be publicly known, along with a description of the main purpose and uses of the data.
2. The Principle of Individual Participation: Individuals should have a right to view all information that is collected about them. They must also be able to correct or remove data that is not timely, accurate, relevant, or complete.
3. The Principle of Collection Limitation: There should be limits to the collection of personal data. Data should be collected by lawful and fair means, and should be collected, wherever appropriate, with the knowledge or consent of the subject.

4. The Principle of Data Quality: Personal data should be relevant to the purposes for which it is collected and used. It should be accurate, complete, and timely.
5. The Principle of Finality: There should be limits to the use and disclosure of personal data: data should be used only for purposes specified at the time of collection. Data should not be otherwise disclosed without the consent of the data subject or other legal authority.
6. The Principle of Security: Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification, or disclosure.
7. The Principle of Accountability: Record-keepers should be accountable for complying with fair information practices.[31]

The lead-up and follow through of the creation of 1974 US Privacy Act underscores the concern that Congress placed in the threat for government misuse or abuse of personal records and/or data in light of the computerization of those records. The aim of the Fair Information Practices principles was to give individuals the power to control the collection, preservation, and distribution of their personal information, and to further require that government agencies wishing to disperse information about individuals to third parties acquire consent of the individual in question. Unfortunately, that latter provision was weakened by exceptions, and "as early as 1977, the Privacy Protection Study Commission found that the Privacy Act was vague and would likely not meet its stated purposes."[32]

The Privacy Protection Act of 1980 (PPA) reinforced the idea of potential problems relating to the computerization of government records. The PPA conveys protection to publishers through prohibiting the government from searching and/or seizing any work product or documentary materials held by a "person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication" unless probable cause exists to show that

said publisher in question has either broken a law or is breaking a law to which the said materials in question relate.[33] The PPA's application to online materials and systems is still in the air. Many believe it extends to apply to online bulletin board systems and other online forms of publication under the guise of the "other form of public communication" clause of the act.[34]

> However, the only case to present this question to a court, Steve Jackson Games, Inc. v. United States Secret Service, failed to resolve the issue. In *Steve Jackson Games*, the Secret Service seized a computer game publisher's electronic bulletin board system, e-mail and electronic files to search for evidence involving an employee of the company. The court decided the PPA protected the seized property, but based its decision on the fact that the company published traditional books, magazines and board games.[35]

Even though the PPA of 1980 seemed to define a "hands-off" approach for the federal government with regards to information held by a third party, as certain industries and sectors became more popular and began to collect more personal information, accordingly, they became more regulated as well. "The Cable Communications Act of 1984, the Video Privacy Protection Act of 1988, the Telephone Consumer Protection Act of 1991, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and the 1999 Financial Services Modernization Act (Gramm-Leach-Biley) all applied privacy and fair information practices to sensitive sectors."[36] The regulation of the aforementioned sectors and industries usually arose as a result of abuse or potential abuse as a result of a lack of privacy legislation. Unfortunately, as time and technology progressed, "the potential for privacy abuse in commercial settings, indicating significant

deviation from the fair information practices, increased dramatically."[37] However, even in light of the federal regulations and the measures taken to protect privacy of individuals in certain sectors, some states still permitted the open sale of state records such as information relating to driver's licenses.[38] That appears to have been remedied (despite exceptions) with the Driver's Privacy Protection Act of 1994 which "restricts the public disclosure of personal information contained in state department of motor vehicle ("DMV") records."[39] The aforementioned act shows how many sector-based regulations occur after possible misuse and/or abuse.

As demonstrated above, the concept of privacy, much less data privacy, is not comprehensively legislated, delineated, or defined within the United States. Privacy rights are dictated in areas where abuse has occurred or where it is deemed of utmost importance to secure the privacy of information. Furthermore, the first amendment rights granting free speech within the United States Constitution often come at odds with the concepts of privacy. However, all is not lost. While the federal government has no comprehensive law granting a right to privacy to its citizens, individual state governments have the ability to protect privacy for its residents. California, a prime example, has legislated in its state constitution an individual's inalienable right to privacy.[40] California has even gone several steps further through the activity of its state legislature in crafting laws that deal with data privacy head on. "The Californian Online Privacy Protection Act (OPPA) of 2003 requires operators of commercial web sites or online services that collect personal information on California residents through a web site to conspicuously post a privacy policy on the site and to comply with its policy."[41]

Conversely to what is found in terms of privacy laws, data privacy in particular, in the United States (nothing comprehensive, and really a patchwork quilt of precedent and sector-based regulation striving to cover possible holes), Europe legislates very heavily and rigidly the concept of data privacy. For the most part, data privacy had existed inside of Europe for around twenty years before any effort was taken to coordinate the data protection of all the countries within the Union. The first step took place in 1968 when the United Nations flagged data privacy as a potential issue when commemorating the twentieth anniversary of signing the Universal Declaration of Human Rights.[42] Considering the issue in terms of whether restrictions should be placed with regards to electronics, only the advanced, industrialized nations seemed worried about its potential conflict arising between technical progress and human rights.[43] All that withstanding, however, two organizations, the Organization for Economic Co-operation and Development (OECD) and the Council of Europe, took it upon themselves to examine the problems and potential solutions dealing with the protection of individual data privacy. The organizations, following several symposiums and groups set up to discuss and analyze the concept of data privacy, both released their respective rules/guidelines in 1980 concerning data privacy and their recommendations. The OECD's flavor, entitled "the 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data"[44] came out alongside the Council of Europe's "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" with whom the OECD had worked closely with throughout this entire time in hopes to remove any possible conflict between the two.[45] The OECD's guidelines, being voluntary, proved much more specific than the Council of Europe's recommendations, which, being

binding to the signing states, allowed more flexibility. The creation of these two sets of guidelines is important to be noted, as they provided part of the framework and foundation for future legislation such as the data protection directive.

It should also be noted, however, in contrast to the US side, that these regulations and recommendations were completed strictly in the presence of privacy advocates, with a notable lack of presence from any representatives from business or industry.[46] The US, being a part of the OECD, did not wholeheartedly support the idea of monitoring the compliance of data processing and communication industries, nor did it entirely trust the motives of the Europeans. However, in the spirit of creating non-binding guidelines, the differences were summarily ignored. "The Reagan administration urged US companies to voluntarily comply with the OECD Guidelines, but by 1983 only 182 large multinational companies and trade associations had officially endorsed the OECD Guidelines."[47]

It is interesting to note, that when US business complained about the intervention and action required on part of the European Data Protection Directive, the European authorities reminded them that the US had already endorsed most of what was in the former OECD guidelines, which essentially helped provide the framework for the current Directive. The difference being that the Europeans were simply more actively enforcing the guidelines than were the Americans.

A Data Protection Solution – Courtesy of Europe

As the US grapples with issues related to personal data protection and privacy as a result of, amongst other factors, the expansion of the internet and other personal technology, the EU, as early as 1998, presented a strong front in dealing with the protection of personal data. It came in the form of the Data Protection Directive.

While the Directive was an important step in protecting individuals' data rights, as it is often said, the "proof is in the pudding," and the Directive is no exception. Chocked full of details, the Directive is very specific about what is handled where and how so. The Directive specifies that data may be collected on individuals, and stored, but the controllers must meet certain standards. They must notify the individual on whom the data is collected, as well as offer an option to "opt out" of the collection. Furthermore, only certain types of data may be collected individuals. Certain statistics require, "special protection for 'sensitive' data, relating to health, religion, ethnic origin, sexual life, political opinions, membership of a trade union and criminal convictions."[48] Additionally, data controllers must make every effort to insure that the data collected is correct, and give the individuals on whom the data is collected the option to correct said information.

Finally, the last and possibly the most controversial condition (with regards to the US), deals with personal data transferred to parties outside of the EU. Simply put, one cannot proceed with a transfer without meeting certain conditions. More specifically, data can only be transferred to nations who meet a finding of "adequacy" with regards to their standards for personal data protection. As it turned out, most nations that had national, comprehensive privacy legislation protecting individuals' personal information

met with a finding of adequacy from the EU through the Article 29 Working Party; which plays an advisory role on most issues related to the Directive.[49] Many nations without comprehensive privacy protection, noting the shove from the EU, passed comprehensive privacy legislation at the national level and thus met with a finding of "adequacy." Canada, for example, "was one such nation to squeeze under the wire. It joined the world by introducing a Personal Information Protection and Electronic Documents Act into Parliament."[50]

The US, being one of those nations who did not (and still currently do not) have comprehensive privacy legislation did not meet adequacy for data transfers. In essence, this meant a halt of transatlantic trade between the EU and US. The US, determined not to be forced into creating privacy legislation, vehemently opposed it. The EU, not about to have their own directive undermined, held fast to their legislation. An international grudge match was about to begin.

It was not so much that the US opposed personal data protection; the reason remained more that those (primarily business and industry interests) within the nation opposed it being mandated in the form of a federal law. As it turned out, the US pushed for self-regulation with regards to personal data protection. This was due in no small part to the committee selected by President Clinton and his administration, that hand-picked a Silicon Valley pioneer of the dot-com boom era to head the committee and its operations. Ira Magaziner[51], leading the committee, consulted almost unanimously only members of business and business interests, with no input from privacy watchdogs or regular voting citizens in the United States. The committee did not want comprehensive privacy legislation, and it certainly did not want it written into law. Instead, as previously

discussed, the committee preferred a self-regulatory approach - independent of the government with little or no oversight, and with little impediment to business.

Business within the US did not want comprehensive legislation for a number of reasons. First and foremost, the numerous firms who deal exclusively in personal data mining and trade did not want to compromise their way of life. These businesses that collect phone numbers and demographics for use for telemarketers, direct mail marketers, surveyors, background check services, and any other trade where the buying and selling of personal information holds the potential to reap profit feared the possibility of being regulated out of business. Furthermore, businesses who collected and managed personal data did not want to have to spend the time and money to reform their systems to meet European standards. They could not imagine the time, money, effort, and mostly money that would be required to manage the data (specifically the certain parts collected as well as allowing individuals the ability to opt out and correct the information collected about them).

The EU strongly opposed the self-regulatory approach put forth by the US government. Aside from the lack of accountability there were no prototype plans to demonstrate the approach or any motive/incentive for businesses to play along. As the Directive was written, enforcement could only take place on the EU side, at the member state level if non-compliance was found. It could not punish data receivers in the US nor control what happened to the data once within that country's borders. Fortunately for the US, and for trade between the two entities, a self-regulation solution did emerge, in the previously discussed Safe Harbor Agreement.

Prevalence of Internet in Daily Lives

Without question, the internet has made an incalculable impact on the world and the people in it. From communication, to commerce, to mere entertainment, the internet has revolutionized the way nearly everything is done. Its far-reaching links to all corners of the globe facilitate its ability impact virtually every area of modern society.

In the past, where one might have corresponded with a distant friend or relative through the post, electronic mail (e-mail) is often used in its stead. Nearly free in usage and accessible most everywhere, its advantages are more than apparent. Its instant delivery qualities trump even the fastest physical mail courier adding further advantages. Business transactions and contract negotiations take place in minutes rather than months as bits and bytes fly across transatlantic fiber optic lines much faster paper and type.

Commerce has not only been revolutionized by the growth of the internet; in many ways it has helped spur its growth. At first, profits realized through the internet proved relatively restricted to those who helped create its networks and provide users access. Personal computer makers and online service providers reigned supreme early on. As more people acquired internet access and adopted internet usage, they expected more by way of convenience and value. Naturally, online shopping met this demand. With simple clicks of a mouse and pecks on the keyboard, nearly anyone could order any product from anywhere and have it delivered to their doorstep within days. Comparison shopping, once never possible for hard to find products or in locales with a shortage of stores, becomes commonplace, with websites such as Shopping.com[52] springing up catering toward users trying to find the best deal. Businesses can finally reach customers

they never dreamed of, while customers can find products and services they never knew existed. Microsoft's CEO, Bill Gates, speaks on how the Internet relates to business:

> The Internet makes the world simpler. For businesses, the Internet breaks down logistical barriers, offering greater flexibility and power in the way they do business. It shrinks time and distance, simplifies complex business processes, and enables more effective communication and collaboration--a giant corporation can now be as nimble as a tiny startup, while a family firm located in a remote rural village now has the world as its marketplace. Combined with advanced productivity software, the Internet enables individual knowledge workers to use their time more efficiently, and to focus on more productive tasks. And it gives consumers the ability to shop smarter, to find the best products at the right prices. In fact, it empowers them in ways that once were available only to large companies, enabling them to join with others to buy products at lower prices, and bid competitively around the world.[53]

While the Internet has revolutionized the way we communicate and do business, it has also changed the way we get information and entertainment. Websites with animations provide comic relief, while video repository sites entertain and inform a worldwide audience. People now use the internet to download music and movies, without ever having to leave their homes, without ever having to enter a store. Internet video and radio provides live information and entertainment anytime, any place. And the internet has changed the way we get our information as well. Whereas encyclopedias were once considered the best source of general knowledge, they have now been replaced by the likes of Google[54], Wikipedia[55], and topic-specific message boards/forums. News,

once delivered in newspapers and scheduled radio and television broadcasts, now comes in the form of web pages and webcasts available any time, up to date by the second. Medical information, articles on how to repair one's vehicle, etc. are all easily accessible to the masses through a simple search string. Again, Bill Gates affirms:

> The Internet brings people closer together. Before the Internet, it was possible to keep in touch with relatives and friends across the country or around the world--but it was also expensive. Today, communicating with a friend in Japan is as easy and cheap as communicating with a friend across town, and families regularly use the Internet to keep in touch with far-flung relatives. Millions of people with shared interests--no matter how obscure--exchange information and build communities through Web sites, email and instant-messaging software. Using innovative accessibility aids, people with disabilities can use the Internet to help overcome barriers that prevent them from leading more productive and fulfilling lives.[56]

But has all this convenience and ease of use provided us with a false sense of security? Sure, we think nothing of entering our credit card information and personal information in that order form on Amazon.com[57], but where is that information going? That intimate conversation you had over e-mail was certainly private for you and your recipient, but who can access the numerous copies of that e-mail that have replicated themselves on every server it passed through on its way to its destination? Who receives that information? And most importantly, who has the power to view it, keep it, sell it, or give it away?

All these are important questions, and most importantly, data protection, data privacy questions. What keeps Amazon.com from tracking what products one buys, and what products one views on their site? What keeps the local grocery store from recording one's purchases after using the store-supplied discount card? What prevents any of these companies from compiling information about any individual, storing it, and selling it to third parties for their own uses? What if that information is wrong, or irrelevant? Does one have the power to correct and/or remove it? According to *Wired News,* "there are no standards for assuring the accuracy of data...A 2004 report by the National Association of State Public Interest Research Groups found that 79 percent of credit reports may contain some type of error. There's no reason to believe that criminal records [often found in background checks] are any more accurate."[58] Inaccurate data might not seem that important now, but it could have serious implications for anyone seeking credit to make large purchases or during a background check in the application phase for a new job.

The bottom line is that these questions deal with issues that one may or may not have been aware even existed. It also emphasizes the idea that technology has moved faster into more areas of our lives than we previously could have imagined. This means that in a world of slow bureaucracy and legislative processes, for the most part, our legal system and its protections have yet to catch up. As Peter Swire notes, "The trends are toward growing international flows of data, growing numbers and power of processors, and declining availability of data protection expertise (due to the much wider range of people who have the power to transfer personal data)."[59] In a world where privacy

borders have been erased by anyone with a personal computer and a phone line, anyone can be a data receiver, a data controller, and furthermore, a data manipulator.

As we have/will see, the regulations in place vary by business sector and locale. In the United States, we have no comprehensive legislation protecting personal data privacy. Some business and industry sectors have legislation concerning the protection and privacy of personal data, but that does not extend to all across the country. The Europeans, on the other hand, have the Data Protection Directive.

Without a doubt, US data borders have been erased. Anyone can send any data anywhere. Before the advent of the internet, data on millions of people required large physical space capable of holding millions of physical paper files and folders. The space issue aside, the accessibility of all that data in paper form is hard to utilize and process. The bottom line, however, is that before the internet, data on individuals was hard to collect, hard to manage, hard to store, and hard to move around. Now, with digital databases and electronic communication, data collection, storage, manipulation, and communication is as easy as sending an e-mail.

On the E-commerce front, transborder data flows resulting from the prevalence of the internet in everyday lives grew exponentially. A company that owned and/or operated mainframes in the US and EU would likely contain certain records such as, "telephone call records, credit card transaction records, or the billing records kept by an Internet service provider (ISP)."[60] Said company might for whatever reasons need to share the aforementioned data between the two mainframes; "For example, accounting and other departments may need to create unified reports, or the computer in the United States may serve as a vital backup for operations usually done in Europe."[61] The internet

helps expedite and simplify this process of information sharing, but poses problems in terms of data protection. In the given example, the purpose seems expressly legitimate, but every situation that arises may not be the case. Furthermore, such a procedure, as listed above, could come into violation of data protection policies in other nations, such as ones in the EU under the Data Protection Directive.

E-commerce over the internet introduces a slew of personal data protection issues. Aside from the normal business processes, such as the collection, storage, and processing of customer orders, there is additional information which is stored on hand. Typically, shipping information is stored for remote customers (as most internet e-commerce customers generally are). Furthermore, billing information is generally collected and stored on record. Sensitive information, including billing addresses, credit card numbers, in some cases even social security numbers. No one need state the implications of the insecurity of this information. But what about the information collected on individuals, especially, without their knowledge?

Some websites, through the use of "cookies," track and monitor the places on the site people visit, the items they click through, and the way they navigate the same items. "A 'cookie' is a short piece of data used by web servers to identify web users. They may be used to track the habits of users of the world wide web."[62] Some websites, such as Amazon.com, use this to help better target their marketing. They may do so by placing other "suggested products" that one might like based on the other products they have purchased or browsed. They may use the information to target the banner advertisements you see on the website. For example:

> The advertising firm sends a cookie along with the advertisement, and that cookie is sent back to the advertising firm the next time you view any page containing one of its advertisements. If many web sites support the same advertising firm, that firm will be able to track your browsing habits from page to page within all the client sites. They will be able to see what [you are] viewing, how often you view them, and the IP address of your computer. This target[s] advertising to you based on those inferences. [63]

Most of this information, at first glance, seems pretty benign. After all, a company trying to better serves customers while shopping is hardly something to get worked up about. However, questions should be asked; exactly what information is being collected? Can it be linked to a user and his or her identity specifically? Is the information they have collected on said person correct? Is the method they use to store the information secure? To whom do they transfer the information, and under what circumstances for what purposes?

Innocent as it seems, the information and how it is used has implications. The book that one thought intriguing based on its title but turned out to be embarrassing adult content when clicked could be stored and collected as a type of item one enjoys looking at. Now that information may or may not be correct, but does one have the ability to correct it? Do they even know that it was collected? The true test comes when one wonders to whom does the information go? If that information is sold to data brokers who do nothing more than collect user data for marketing and background check purposes, it might present an unwanted picture when a potential employer does a check on that person's history. Furthermore, anyone with enough money could possibly

purchase anyone's own details, from what they like to look at to what they typically buy, to where they live, where they have lived, who their relatives are, and what content they typically read. Anywhere in the world. A recent article/investigation[64] by Tom Owad describes what could happen with Amazon.com and its wishlists. The following is a synopsis:

> Tom Owad at applefritter.com has posted a detailed story on how he was able to use Amazon wishlists to profile thousands of people. By using the search function at Amazon, he accessed and downloaded over 260,000 publicly-available wishlists. He then searched the lists for "suspicious" books and authors, including Fahrenheit 451, Michael Moore, Rush Limbaugh, the Koran/Quran and, of course, Build Your Own Laser, Phaser, Ion Ray Gun and Other Working Space Age Projects.
>
> At this point, Tom had a list of Amazon usernames and had identified any "suspicious" books and authors that appeared on each user's wishlist.
>
> But there was still more to do. Amazon allows a user to include their city and state information on their wishlist, so Tom had the information to take it to the next level: plotting his suspects on a Google map.
>
> By inserting the information taken from the Amazon wishlist page, Tom was able to use Google Maps to pinpoint the exact location of people interested in a particular book or author. He simply took the user's name, city and state information from the wishlist, ran it through an address finder, and then plotted the address on Google Maps. Now he could see the location of everyone interested in, say, Michael Moore or 1984.

Spying on your neighbors has never been so easy.[65]

Finally, business and trade has exploded, exponentially, on a global scale as the internet has grown. As we have seen, potential problems arise when dealing with personal data. Now that the internet facilitates easy collection, storage, and transfer of said data, the issue is more concerned with the governing of this storage. Some would say that different cultures have different sets of norms and standards of care and conduct when handling sensitive personal data. This is true, but it also leads to an ethics/legality debate, where the unethical thing to do is not always illegal, and thus, is done. This allows the opening for potential abuse/misuse of personal data.

And in an attempt to head off that potential misuse/abuse of data, the Directive covers the Europeans very well. However, in the US, where policy is often formed as a reaction to unethical or potentially illegal behavior, there lies a gap for potential exploiters to do as they please with little legal repercussion. Some laws have been implemented to protect individuals and their privacy. Others, such as a recent (2003) California law (California Information Privacy Act)[66] simply require businesses to notify individuals that their information has been compromised. Unfortunately, as is the case with most privacy policy in the US, it is part of the patchwork quilt of legislation protecting privacy for some individuals in some places, only in certain cases. The lack of comprehensive privacy policy covering the nation leaves many holes in the protection of personal data.

Terrorism in the 2000s and its Apparent Role in Reversing Previous Privacy Policies

The terrorist attacks within the western world during the early 2000s were nothing short of cataclysmic. Aside from the death, destruction, and feeling of insecurity came a rash of changes in way that individuals' lives were lived: from everyday operations to the functions and actions of federal governments. In the realm of personal data protection this was no exception.

Following the terrorist attacks on September 11, 2001 in the US in Washington, DC, New York City, and over the skies in Pennsylvania, legislators rushed to combat the terrorists and strengthen national security. Unfortunately, in all the rush, personal freedoms and rights to privacy (however unwritten they may have been) were nearly completely overlooked and/or forgotten.

In the United States, personal privacy was dealt a blow with the introduction of the Patriot Act. Passed in fury of Patriotic fever and unprecedented bipartisanship, the US Congress enacted possibly one of the most privacy-damaging acts since the introduction (and later repulsion) of the Alien and Sedition Acts of World War II. The Patriot Act allowed for, among other things, the authority for the United States government and its agents to invade various facets of privacy, such as "sneak and peek" which allowed authorities to search an individual's private domain secretly without a warrant.[67] It also allowed for other invasions such as reviewing the movies one rents, the library books one checks out, and the like. As noted by the American Civil Liberties Union:

> One of the most significant provisions of the Patriot Act makes it far easier for the authorities to gain access to records of citizens' activities being held by a third

> party. At a time when computerization is leading to the creation of more and more such records, Section 215 of the Patriot Act allows the FBI to force anyone at all - including doctors, libraries, bookstores, universities, and Internet service providers - to turn over records on their clients or customers.[68]

The Patriot Act also meant collecting and searching commercial airlines' passenger lists as well as any personal information collected about them, particularly on international passengers.

As one might imagine, the collecting and manipulation of airline passenger data, particularly on passengers from Europe, fell into opposition with the European Data Protection Directive. "The conflict resulted from the US government forcing firms to violate the European Data Protection Directive by requiring all airlines to collect, transfer (to the Department of Homeland Security), and retain thirty-nine data items on each passenger,"[69] flying into the US. The US insisted that foreign airlines flying into the US provide them with the information they demanded at the penalty of fines in the amount of $6000 per passenger or even so far as losing their US landing rights.[70] The EU, insistent that their citizens' data not be compromised under the Directive, pressured those same airlines not to comply by issuing their own warnings.[71] There had to be, and ultimately was, a breaking point. Fortunately, or unfortunately, depending on how one looks at it, there was another compromise. That resulted in the Passenger Name Record Agreement.[72] The Agreement allowed the US to get the passenger lists and data they demanded, while the EU was able to specify the types of data on individuals divulged and for how long it could be kept on record. The US originally demanded approximately 50-60 fields of data on individuals to be shared with any government agency it wanted with a

retention period of 50 years, but ultimately only received 25 fields of data shareable only within the Department of Homeland Security for a period of no longer than 3.5 years under the deal.[73] Hardly a loss for the US, it was more a victory for the States and an allowance on part of the EU.

Terrorist attacks affecting legislation during the 21st century were not unique to the US, however. On March 11, 2004, terrorists struck in Madrid, Spain by exploding bombs on packed commuter trains. And little more than a year later, on July 7, 2005, a number of Subways and Passenger buses were bombed in London, England. Resulting from this attack followed a loss of privacy for citizens as well, as the UK pushed hard for a Data Retention Directive[74] within the EU. The Data Retention Directive required and implemented a policy that all electronic communication be logged by their respective service providers for a period of 6 months up to 2 years.

> Telecommunications providers will now have to keep data such as the time of each fixed and cell phone call made in Europe; whether a call is answered or not; the duration of the call; and other details that can help trace the caller. On the Internet side, they will be required to retain information on the times people connect to the Internet, people's IP addresses, and details pertaining to e-mail messages and VoIP calls.[75]

The idea remained that it would be benefit to national security, though privacy groups worried over an invasion of personal privacy. In an interesting turn of events, businesses in Europe, particularly interests concerning movies and music, supported the Data Retention Directive.[76] Desiring the ability to pursue file-swappers illegally trading copyrighted works on the internet, the new act would serve two purposes: 1) By

requirements of the act, any and all evidence regarding the file swapping would have been retained by the ISPs, and 2) Under the new act, it could open the door for criminal prosecution of file-swappers through criminal courts using taxpayer money, rather than the respective industries using their own money to pursue file swappers in civil courts.[77] Perhaps businesses are not so anti-privacy after all.

The idea that business and industry in the US and government in the EU have started to change their minds with regards to data protection signals a bit of role reversal within the US and EU. Whereas the EU was first in the realm of personal data protection, the US is now more increasingly aware and interested in such legislation. More importantly, the very parties against national legislation protecting personal data, businesses, are now in favor of its implementation. For example, on November 3, 2005 Microsoft[78] drafted and sent a letter (see Appendix I) to Congress, demanding that privacy protection legislation be put into place. It even went so far as to request policy similar to EU structure and requested an end to industry self-regulation. Actions such as these are in direct contradiction to what business (including Microsoft) and the US wanted less than ten years ago when the EU directive put transatlantic trade into jeopardy.

Further role reversal has reared its head in the EU. A place more concerned with personal data protection, and furthermore, filled with people more trusting of government and less trusting of business, the implementation of legislation such as the Data Retention Directive[79] has caused rifts within the European Union. Its creation, in the name and idea of national security, has in essence created a huge invasion of privacy for benefit of the government, and potentially for business as well (in the aforementioned case of file

swappers). Whereas before invasion of privacy by the government, at least in the EU was somewhat tolerated, this new legislation opens up the possibility for invasion of privacy for business interests, and not national security.

Culture of Privacy

It is often said that the discrepancies in the way privacy is handled between the US and EU ultimately lead back to cultural differences. While this may be true in certain parts of the theory, it hardly holds true for all people for all issues on either side of the Atlantic. In fact, one may be surprised to see that thoughts amongst the public, both within the EU and US, are surprisingly the same with regards to personal data privacy.

Culture, however, does play a role with respect to the ways in which people on different sides of the Atlantic view their privacy.

> In general, Americans are far more comfortable than Europeans with business handling their information, and far more skeptical of putting it in government hands. The tradition of making government records - like tax records, mortgage information and census data - easily accessible to the public is uniquely American.[80]

So, possibly as a result of our "laissez-faire" approach in business, Americans are more trusting of business with their personal information than they are with the government. Conversely, the Europeans tend to place less trust in business but allow for what could be viewed as more intrusion of privacy by the government. For example, exemptions in the Directive allow the government to deem all "actions necessary to safeguard national security or actions pertaining to criminal proceedings"[81] as outside the scope of the Directive. Additionally, recent legislation such as the Data Retention Directive require that many details of electronic communication over phones and the internet be kept on record for a period of 6 months up to 2 years. "Police will have access to information

about calls, text messages and internet data,"[82] to be used for criminal proceedings and security purposes.

Furthermore, Americans see their privacy and personal information in a different light than do the Europeans. Peter Swire, chief advisor to the Clinton White House on privacy policy notes, "In Europe, privacy is seen as a human right. Your individual data is protected by human rights. In the United States, there's often the legal treatment of the data as it belongs to the company. If you do a transaction with the company, the company uses that information for its next transaction, it sells the information to who it wants to."[83] Other indicators point to cultural differences as a source of dissimilarity in privacy policy: "Whereas the EU preferred a regulatory approach consistent with it administrative infrastructure, the US wanted a decentralized, self-regulatory system that comported with its traditional regulatory approach."[84] In accordance with "laissez-faire," the US wanted to keep the hands off of this issue as it related to business as much as possible. The traditional idea that if the market demanded data protection, only then would it require implementation, followed here.

But while cultural differences obviously exist, did opinions and desires for personal data privacy among Americans and Europeans remain all that different? Opinion polls and surveys taken throughout the late 90s and early 2000s (see Appendix II) "in the US show reasonably strong majorities in favor of more government regulation that are similar to European beliefs."[85] A more recent poll in 2005 went so far as to say that, "71 percent of people believe Congress needs to pass new laws to keep the Internet safe,"[86] with respect to issues such as identity theft (a data privacy/protection issue in the

greatest sense). The aforementioned polls indicate three areas where similarities between American and Europeans desire for personal data privacy seem to exist,

> First, citizens in the EU and the US (as well as Canada) agree that they should be asked before a company uses personal information, and should be consulted before that information is passed along. Second, terrorism did not make the US less supportive of privacy. The US was less willing to allow monitoring of phone calls and emails to fight international terrorism than the Europeans, and finally, the old stereotype, that the US is more sanguine about the motives of businesses while the Europeans are less worried about government, is also not borne out by these opinion polls.[87]

Additionally, the polls found that US respondents did indeed worry about how businesses handled their personal information.[88]

So, while it may have been true to an extent that Americans and Europeans differed culturally with respect to their views on privacy, as well as a fundamental difference in the groups of whom they trusted more with their privacy, there also remains a third factor that played a part in crafting each group's privacy legislation (or lack thereof). As noted by Heisenberg with respect to privacy policy in the US, "the willingness of government actors to include business in the formulation of the policy to solve the privacy problem was the most significant difference between the US and the EU."[89] During the debacle involving the introduction of the European Data Protection Directive, the US consulted almost exclusively with business, which at least in this country, has great interest to prevent restrictive privacy legislation. Whole industries based on the mining, collection, management, and sale of data depend on the ability (and

it exists) to do with it what they want within the US. "This has helped create the world's largest data collection industry by far, with companies like ChoicePoint and AxiCom to collect and analyze those records. The flourishing consumer data industry spends millions of dollars each year lobbying against more restrictive data policies."[90] And lobbying by this industry, coupled with the fear of extravagant costs due to new privacy legislation to other types of industry, have helped prevent the US from instituting broad-sweeping privacy legislation that is found within the EU.

As demonstrated earlier, the US was not devoid of privacy legislation nor was it completely against it. However, in the case of the impending conflict over the Directive, the US chose to cater to big business rather than consult citizen or privacy groups. Business interests in the US were not averse to privacy policy, especially in the compelling light of the European Data Protection Directive aiming to block transborder data flows to the states. Rather, instead of strict, written, privacy legislation, they favored more of a self-regulatory approach. A paper published by Ira Magaziner, "A Framework for Global Economic Commerce,"[91] advocated several stances in the examination of technology privacy and policy issues in the US. Chiefly, it noted that the role of the US Government should be minimal in any issues and policy that may arise. This too was used as the framework for the then Clinton administration's stance on personal data privacy with respect to the Directive. This self-regulation stance was no accident. The committee that published the paper was composed of almost exclusively industry types, as noted by the chief lobbyist for the Intel Corporation, Michael Maibach, "virtually all the leading high-technology companies were involved in the drafting of [the Framework paper], arguing against too much regulation of the Internet."[92] As such, it is no wonder

that the stance taken by the US was pro-business. The policy and stance on privacy was virtually crafted by business alone without consultation from any other groups. And "although there were increasing numbers of pro-privacy interest groups that the administration could have consulted to get a different view of the costs and opportunities, there is little evidence that the White House ever called on these interests."[93]

Conversely, the EU did something rather out of the ordinary when crafting their privacy legislation, at least by American standards. "In the EU, when crafting the European Data Protection Directive in 1990, only pro-privacy interests (the data protection authorities of several member states) were consulted, and businesses were unable to make significant changes to the Directive after it had been drafted by the EU Commission."[94] So, while the US consulted almost exclusively business, the EU largely left them out of the picture. "Sources within the Commission [European Commission] confirm that business interests were not consulted in the preparation of the draft, or given advance notice; business and industry groups were largely unaware that the Commission was going to act on this matter, and the few that were, mistakenly believed the Directive would be appropriately responsive to their business needs."[95] That changed shortly after the publication of the draft in 1990, however, as businesses realized the potential expense that the regulatory measures might impose. Furthermore, even US-based businesses "like American Express and Readers Digest also lobbied against the Directive, but did so behind the scenes for fear of being seen as 'anti-privacy.'"[96] In summation, business interests, for the most part not consulted in the drafting of the Directive, did try to lobby against it, but ultimately at too late a time to make any real changes to the legislation.[97]

In Conclusion: Should the US move to create national privacy legislation?

This is the quintessential question asked, and hopefully answered with this paper. Should the US move to personal data privacy protection, à la EU Directive? While it is true that early on in the consideration of personal data privacy the US did not want to, in essence, kill the goose that laid the golden egg (in reference to over-legislating the growing tech sector and potentially killing off profits), it seems as though times have changed and that demands, not simply from the people, but also within business have changed. While past polling data shows that Americans have been largely in favor of and in support of government-regulated privacy protection, particularly with regards to electronic communication and the internet, business has been the real holdout. And with business lobbying and contributing to so many politicians' campaigns, they held a great deal of weight in controlling the legislation passing through Congress and the White House. Times, however, have begun to change.

Even though it appears that cultural differences do play a serious a role in the privacy differences between the US and EU (in terms of legislation), we must note that polls and surveys taken in the respective populations signal that both groups favor stronger policy protecting their personal data privacy. As such, we begin to note that the real cause seems to be that business/industry seems to have had a firmer grasp on privacy legislation in the US than they did in the EU. Consultation in the US in forming the policy utilized strictly interest groups with virtually no input from citizens or privacy groups. Recent news, however, has begun to note a shift. More citizens now than ever, possibly in light of identity thefts and personal information being compromised and distributed over the internet, seem to be in favor of government-regulated personal data

privacy protection in the form of legislation: "I don't think the public knows what it wants Congress to do, but it wants Congress to do something," [98] was the summation of a recent poll of persons in the US. Members of Congress, recognizing that their constituents have an interest in personal data privacy, have even begun introducing bills to address comprehensive privacy protection in the US. "It is the Personal Data Privacy and Security Act of 2005, introduced by Sens. Arlen Specter, R-Pa., and Patrick Leahy, D-Vt."[99] Even more dramatically, business has started to be in favor of and demand privacy legislation. Microsoft, one of the largest tech companies in the US if not the world, usually on the forefront of technology, sent a letter[100] in 2005 to Capitol Hill requesting privacy legislation...not unlike that found in the EU Directive:

> Microsoft Corp. believes a comprehensive, yet flexible legislative solution is required at the federal level to provide robust and complete protection for consumers, and to provide consistency for organizations facing increasing risks and costs associated with managing and protecting personal information.[101]

The letter goes on to define several areas that need to be addressed very similar to that found in the Directive (See Appendix I).

So, what has caused the push for privacy legislation here in the US? Aside from business now loosening its stranglehold, it appears that citizens want it more than ever now. The explosion of technology and the prevalence of the Internet has made data transfer, especially about persons, easier than ever. Websites compromised by malicious hackers and crackers often gain access to databases containing the personal information on hundreds if not thousands or even millions of people. And now, with some companies

forced to reveal publicly when identity and personal information has been compromised (at least in the state of California[102]) more common people are aware of the potential dangers of their data being uncontrolled and unregulated. Identity theft is on the rise, credit card fraud is a grave concern, and in general, people have become increasingly averse to direct-marketing as a result of their information being distributed, no matter whether contacted through postal mail, e-mail, or by telephone. Businesses, likewise, would prefer to adhere to legislated policy in the realm of privacy if not only to spare themselves the expense of creating and enforcing their own but also perhaps as a method to spread the blame onto others if and when personal data is compromised.

Or perhaps it has to do with the rise in terrorism, and the appropriate response and loss of privacy that has occurred at the hands of our respective governments. Legislation such as the Data Retention Directive in the EU, the Patriot Act in the US, and the more recent secret, warrant-less wiretaps authorized by President George W. Bush, have people more concerned than ever about the control and privacy of their information, particularly when their governments seem so keen on intruding upon it.

At a time in the early 90s and 2000s, when the tech sector was a booming growth sector, and no one knew really how to handle the explosion of new ideas and technologies, the idea of creating broad-sweeping privacy legislation was probably shocking, and moreover, possibly harmful to its growth. However, with the maturation of the PC world and the everyday presence of the Internet in most people's lives, it probably is time for the US to step up and offer legislation protecting individuals' personal data privacy. With the explosion of new tech infrastructure and services the laws have failed to keep up with the innovative pace of today's world. In the past, sector-

based privacy legislation created to address problems that cropped up was satisfactory; today, however, at the speed at which things change and at which data can be transferred, a reactionary stance is not the way to go. Personal data protection needs to be proactive, most likely based on the European model. Business and citizens are now ready to accept it, and the tech industry is not going to drown itself as a result of its implementation. Terrorism, an ever-present threat now, likely not to subside any time soon, can live in harmony with privacy. But comprehensive policies must be developed, protecting the individual, the state, and other bodies that both interact with. It can be done, and there is no better time than now.

Appendix I

Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation

Brad Smith
Senior Vice President, General Counsel and Corporate Secretary
Microsoft Corp.

November 2005

Microsoft

Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation

Concern is growing among consumers, businesses, policymakers and privacy advocates about the misuse of personal information, the loss or theft of sensitive data files containing individuals' confidential information, and related privacy considerations.

A bewildering jumble of overlapping state and federal laws intended to address these concerns — though well intended — is creating confusion among consumers about how best to protect their personal information. It is also creating major challenges for businesses trying to comply with the growing complexity of inconsistent legal requirements.

Microsoft Corp. believes a comprehensive, yet flexible legislative solution is required at the federal level to provide robust and complete protection for consumers, and to provide consistency for organizations facing increasing risks and costs associated with managing and protecting personal information.

Historically, Microsoft has favored market-driven solutions and self-regulatory efforts to address data privacy and security issues. We believe that focusing on technology and industry best practices are the most immediate and effective ways to protect individual privacy. For example, Microsoft has developed innovative technical solutions such as advanced spam filtering in our e-mail software, the Microsoft® AntiSpyware tool, and cookie management in Internet Explorer. And we have collaborated with law enforcement, other industry leaders, privacy organizations and policymakers on a variety of efforts to create a trusted environment for users of the Internet and other technologies.

A Call for Uniform Federal Privacy Legislation

Over the past few years, however, several factors have altered the privacy landscape in such a way and to such a degree that we now believe the time has come to support national privacy legislation as a component of a multifaceted approach to privacy protection. As a strong supporter of free-market solutions, Microsoft did not come to this decision without careful consideration. But it is one we now believe is the right course in order to provide meaningful protections for individuals, while avoiding unnecessary obstacles to legitimate business activities.

As we see it, the goal of federal privacy legislation should be twofold: to establish ***baseline privacy protections*** for consumers, and to provide organizations with ***a uniform standard*** on which they can build effective privacy policies and compliance efforts. There are several reasons why this is an appropriate time to consider such legislation:

- An increasingly complex patchwork of state and federal laws is not effectively serving the interests of consumers, but *is* requiring businesses to navigate and adhere to a growing web of inconsistent legal obligations.

- Growing concerns among consumers about privacy and identify theft are eroding public trust in the Internet and threatening to dampen online commerce.
- Widely-publicized security breaches in recent months have exposed the need for comprehensive measures to improve not just security, but also consumers' understanding and control over their personal information.

The Legislative Collage

Today, much of the privacy regulation in the United States occurs at the state level, where many of the 50 states have enacted privacy laws that govern specific industries, issues or practices. Often, these laws are inconsistent, so that a set of business practices that is legal and commonplace in one state may be prohibited just across the state line. In addition, the *number* of state privacy laws is increasing quickly — for example, more than 20 states have passed separate financial privacy laws just since the beginning of 2004.

At the same time, Congress has enacted federal privacy legislation specific to certain industries. For instance:

- The Gramm-Leach-Bliley Act applies to financial institutions;
- HIPAA applies to health care providers;
- The privacy provisions of the Cable Act apply to cable operators;
- The privacy provisions of the Communications Act apply to telecommunications carriers;
- Specific privacy laws address children's online privacy, spam, telemarketing and junk faxes;
- And concerns over spyware and identity theft are now prompting an array of federal legislative proposals.

While all of these are well-intended efforts, this ad hoc approach to privacy legislation has many drawbacks. It has led to an overlapping, inconsistent and incomplete patchwork of state and federal laws that creates compliance chaos for businesses and uncertainty for consumers.

Consumers and businesses alike are often faced with the daunting task of determining whether one or more of the existing laws applies. The answer may depend on the type of data involved, the kind of company that collects it, where and how it's collected, and how it might be used.

For example, personal information collected by a bank is covered by one privacy standard, but that same information collected by a hospital is covered by a different standard. If that information is from a child under the age of 13, it's protected by yet another standard if it's collected online, but it may not be protected at all if it's collected offline. And each of those standards may be affected by state law, but in a different way from state to state. Yet, despite all of these legal distinctions, the consequences of misuse of that information could be exactly the same in each scenario.

Microsoft believes that a legislative framework that encompasses the core components of data privacy and security would obviate the need for a proliferating array of issue-specific, stopgap measures, and create a logical foundation on which appropriate, incremental legislative, technology and industry solutions can be built.

Privacy Concerns Are Growing

There is little question that the Internet and information technologies continue to bring enormous social and economic benefits to individuals and nations worldwide. They're empowering school children and seniors to learn, communicate and exchange ideas with family, teachers and new friends they've just met halfway around the globe. They're creating a whole new world of online commerce for individuals and for business. And, perhaps most important, they offer powerful tools to help individuals and governments participate in the opportunities of the 21st-century knowledge economy.

But the potential of information technology to continue to drive social and economic advances depends on building and maintaining a solid foundation of trust. Individuals will not take full advantage of the Internet or any other commercial medium if they believe their personal information could be compromised or disclosed in unexpected ways. A CBS News/New York Times Poll in September reported that nearly nine in 10 Americans are concerned about identity theft, with more than half saying they're "very concerned." This was underscored by a recent survey by Consumers Union, which indicated that 25 percent of Internet users have stopped making purchases online, and 29 percent of those who do shop online have cut back because of concerns about identity theft.

Effective federal legislation will help provide consumers with the confidence and knowledge that the legitimate businesses with which they engage are following an established set of baseline privacy practices.

A Comprehensive Approach to Identity Theft

The final reason Microsoft believes it's the right time for privacy legislation is that it has become increasingly clear that a comprehensive approach is needed to help protect consumers from identity theft and other misuse of their personal information.

Recent, highly publicized security breaches have resulted in the theft or loss of personal information about millions of American consumers. In response, numerous state and federal lawmakers have proposed or enacted legislation requiring businesses to implement security procedures that apply to personal information, and to notify individuals of certain security breaches.

Many of these measures make sense, and Microsoft has supported them. But these approaches do not fully address an underlying concern: a lack of transparency about how companies are collecting, using and disclosing personal information in the first place.

In many instances, prior to the publicity of a security breach consumers didn't realize these particular companies even existed, let alone that they maintained personal

information about them. It's now clear that people want to understand who has their personal information, what information they maintain, how they use that information, and with what third parties they share it. Two out of three Americans think the government should be doing more to regulate the personal information that can be collected about them, according to a CBS News/New York Times Poll.

A tailored but more complete approach to privacy and security legislation at the federal level will help address these concerns by better informing consumers about who is using their personal information and how. And it will empower them to exercise meaningful control over their personal information both before and after any security breach occurs.

A Framework for Federal Privacy Legislation

With this context, Microsoft has outlined some core principles and specific proposals that we believe should be reflected in a comprehensive legislative approach to privacy and data security.

4. A Baseline Privacy Standard

The first goal is to create a baseline standard that applies across all organizations and industries. Such a standard should address the need for privacy legislation regarding both online and offline data, federal pre-emption, and harmonization with international privacy law.

Online and Offline

Federal privacy legislation should apply to both online and offline data collection, and to data stored in either electronic or paper form. This is important to avoid inconsistent standards that could jeopardize the free flow of information between the two media. It's also important because the potential risks to consumers are the same, regardless of where or how the data was originally collected.

Indeed, the consequences of the loss or misuse of personal information can be just as devastating whether that information is in paper form or electronic form. Of course, notification and security requirements may need to be different in offline and online environments, and any privacy legislation should recognize those differences. But these operational differences should not deprive individuals of core protections with respect to that data or obviate the need for businesses to keep the data secure. A single, flexible framework for all personal information will create broader and stronger protections for consumers, while enabling businesses to comply with one coherent set of privacy and security requirements.

Federal Pre-Emption

To address the current patchwork of state and federal law, federal privacy legislation should pre-empt state laws that impose requirements for the collection, use, disclosure and storage of personal information. Only a uniform national standard can address the complexities, inconsistencies and incompleteness of current laws, and bring the clarity and consistency needed to benefit consumers and businesses.

Federal legislation must do more than just create a "floor" above which states are free to impose additional requirements. That approach would still require any company that participates broadly in the national economy to either abide by the strictest applicable state law — transforming that state's law into default federal legislation — or to somehow compartmentalize its transactions on a state-by-state basis, which is impracticable and potentially to the detriment of the more important goal of protecting the privacy interests of consumers. The only realistic solution that protects consumers, while minimizing the operational burdens on responsible businesses, is to adopt a nationwide privacy standard. That standard should certainly be robust, but it should apply uniformly.

However, it's important that state attorneys general play a vital role in ensuring that companies adhere to sound privacy and security practices. In the spam and spyware arenas, Microsoft has successfully partnered with several state attorneys general to bring illegal actors to justice. Accordingly, in the privacy context, Microsoft supports any clarification that enables state attorneys general to enforce the federal legislation, and which ensures they can continue to rely on their enforcement authority under state consumer protection laws.

International Harmonization

To the extent possible, federal privacy legislation should be generally consistent with privacy laws around the world. Many U.S. companies operate globally — whether by doing business with consumers in other countries or having operations that require data to flow freely across national borders. Conflicting national privacy laws may thwart this global commerce by imposing inconsistent legal obligations that are at best confusing and at worst irreconcilable. A U.S. privacy law that is largely compatible with those of other countries would not only help reduce the complexity and cost of compliance, but also promote international business. Such legislation may help reduce barriers to data flowing into the United States — particularly from those countries that already have robust privacy laws. At the same time, U.S. legislation should avoid imposing new burdens on data flowing out of the United States, since there is no privacy need for such barriers if it is made clear that U.S. companies will remain responsible and liable for how that information is handled by their service providers, whether domestic or overseas.

2. Transparency

The second major goal of data privacy legislation is to increase transparency regarding the collection, use and transfer of personal information. This can be achieved in several ways.

Privacy Notices

Some form of privacy notice is a key component of virtually every privacy law and legislative proposal, and such notices have been widely adopted by industry. It's important that federal privacy legislation provide flexibility in how a privacy notice may be presented. At the same time, we believe it's important to establish basic,

uniform standards that apply to the collection of personal information from an individual.

- The privacy notice should be made available *before* collecting personal information from an individual;
- It should describe what types of data are collected, how that information will be used, to whom and for what purpose it will be disclosed, and how and when an individual can limit its use and disclosure;
- It should permit and encourage innovative notification approaches such as "layered" privacy notices — typically a one-page or shorter privacy notice that is consumer-friendly, and supplements the traditional longer privacy statement.

This flexibility and support for innovative privacy notices is very important. For example, at Microsoft — where we offer online services on a global basis — we are faced with many different requirements for specific items that must be contained in a privacy notice. And in interactions with regulators, privacy advocates and others, Microsoft is often asked to add additional detail or explanation into our privacy notices. As a result, privacy statements tend to get longer and more complex with time. And while that may make them more complete and precise, it makes them very difficult for the average consumer to read and understand.

Layered notices are an innovative way to bridge these competing needs. Microsoft's MSN® division has been a leader in developing and deploying layered notices, and we believe it represents a significant step forward in helping users understand a company's privacy practices and make informed decisions.

Material Changes to Privacy Practices

Federal legislation should also establish clear standards for handling material changes to privacy practices. An organization that wants to use or disclose personal information in certain ways not described in its privacy notice at the time the data was collected should first be required to take additional steps to ensure individual notice and choice. Those steps should include updating the applicable privacy notice; affirmatively notifying each individual of the new use or disclosure; obtaining an acknowledgement of that notice from the individual; and providing the individual with an opportunity to provide or withhold consent for the new use or disclosure.

Individual Access to Personal Information

Another way to increase transparency is to permit individuals to see the information about them held by organizations. Thus, federal legislation should mandate that businesses provide individuals with access to the personal information maintained about them, as well as a means to correct or amend incomplete or inaccurate information. Certain reasonable exceptions must accompany this legislative requirement for it to be workable, of course. For example, access should be required only if the requesting party reasonably verifies that he or she is the person to whom the personal information relates. The obligation to provide access may also need to be limited where providing access would be unlawful; violate the rights of other persons;

compromise proprietary or confidential information, technology, or business processes; affect certain litigation or judicial proceedings; or impose a burden on the organization that is disproportionate to the risk of harm to the individual.

Breach Notification

Finally, individuals should be informed in the event of a security breach that could reasonably result in the misuse of their unencrypted sensitive financial information. Several current bills focus specifically on this point, and as is the case in most current legislative proposals, the standard must be narrowly focused in order to prevent notifications from becoming so frequent that consumers disregard them, or find that they're unable to differentiate between those that indicate a significant risk and those that don't. The requirements for the notification itself should be flexible — taking into account the size and type of the entity providing it, the number of people required to receive it, the relative costs for different methods of providing it, and the ways in which the entity typically communicates with its customers. Microsoft believes the Interagency Guidance interpreting the Gramm-Leach-Bliley Act, which gives discretion to covered entities to provide notice in any manner designed to ensure that a customer can reasonably be expected to receive it, is a sound model for federal legislation.

3. Control Over Personal Information

A third goal of federal privacy legislation is to provide individuals with meaningful control over how their personal information is used and disclosed. Specifically, Microsoft believes federal privacy legislation should require organizations to obtain the consent of an individual *before* an organization can use or disclose personal information for "secondary purposes" — that is, purposes not reasonably related to why the individual provided the information in the first place.

Here again, the requirements for this consent should be flexible: The greater the risk to the consumer, the more robust the required consent should be. And these requirements should avoid mandating excessive and unnecessary levels of choice for consumers which would bombard them with a confusing and annoying stream of warnings and options every time a piece of personal information is collected or used. The consent requirements should be grounded firmly in common sense. For example, explicit consent would make sense before certain sensitive personal information — such as information about a medical condition or access to a bank account — can be used or disclosed for a secondary purpose.

Explicit consent may also be appropriate to prevent certain unauthorized reuses or redisclosures of information by third parties. For instance, a third party may receive personal information from an organization either because the information was disclosed to the third party for a primary purpose described in a privacy notice, or because the individual consented to its disclosure for a secondary purpose. But that third party should not be free to later decide that it wishes to use that information in a way that goes beyond the original notice provided to, or consent obtained from, the individual. In order to prevent the complete loss of control over data once it has been transferred, third parties

that receive personal information for one purpose generally should not be permitted to reuse or redisclose that information for other unrelated purposes without obtaining additional explicit consent from the individual.

Where the privacy risk is *lower* — for example with the disclosure on *non-sensitive* personal information for a secondary use — organizations should be able to obtain consent by offering individuals a meaningful opportunity to opt out. This would give consumers who are particularly concerned about their privacy an up-front choice. Explicit consent should not be mandated because most secondary disclosures of personal information do not pose a high across-the-board risk to consumer privacy, and the benefits of explicit consent do not outweigh its burden on legitimate business activity.

Finally, where the privacy risk is *lowest* — for example, where an organization uses personal information for its own internal purposes — the consent option should be the least onerous. In that case, the organization should be able to condition the receipt of an ongoing service on individual consent to such use — *if* that condition was made very clear to the user at the time he or she registered for the service. For example, many online services rely upon the display of targeted advertising to users in order to provide these services free of charge. If these companies could not require users to consent to receive ads as a condition of the service, many free or discounted online services would disappear.

5. ***Information Security***

The fourth major objective of federal privacy legislation should be to ensure that organizations in possession of personal information take reasonable steps to protect against unauthorized access, use, disclosure, modification or loss. These steps should include administrative, technical and physical safeguards that are appropriate given the sensitivity of the personal information, the potential risks, the state of the art and the cost of implementation.

The security provisions of the Gramm-Leach-Bliley Act and the FTC's implementing regulations provide a good model — a flexible framework that gives organizations the discretion to implement the most appropriate technologies and procedures for their respective environments. This makes sense, because each business is in the best position to understand the particular security measures that are right for the different types and forms of personal information it maintains.

In contrast, a prescriptive set of federally mandated technical specifications would inevitably impose too high of a burden on some organizations for some information, but not adequately protect some personal information held by other organizations. And because security measures are constantly changing and improving as technology advances and engineers respond to evolving threats to information security, a one-size-fits-all regime would likely become obsolete.

The Need for Action

Clearly, these are complex issues with significant implications for consumers and for business. Doing nothing may, at first glance, seem an easier path. Should the industry and policymakers fail to act effectively however, organizations will face increasing risks and costs associated with a growing patchwork of inconsistent, overlapping and complex obligations; consumers will feel even more alienated, uncertain and fearful about disclosing personal information; and the promise of information technology as a new vehicle for economic growth will be at risk.

Federal privacy legislation is an important priority for Microsoft, and, we believe, for consumers, for our industry and for policymakers to consider. We look forward to working with all stakeholders to solve this important challenge.

Microsoft and MSN are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table 2.1 Public Opinion Surveys About Government Regulation of Privacy (Progovernment regulation opinion in italic type)

Equifax, 1993
My rights to privacy are adequately protected today by laws and organizational practices. Do you agree strongly, agree somewhat, disagree somewhat or disagree strongly?

Strongly or somewhat agree	40%
Strongly or somewhat disagree	*58%*
Not sure	2%

Privacy & American Business, 1997
(asked of computer users only)
Here are three ways that the government could approach Internet privacy issues. Which one of these three do you think would be best at this stage of Internet development?
A. Government should pass laws now for how personal information can be collected and used on the Internet,
B. Government should recommend privacy standards for the Internet, but not pass laws at this time,
C. Government should let groups develop voluntary privacy standards, but not take any action now unless real problems arise.

Pass laws	*58%*
Recommend privacy standards	24%
Let groups develop voluntary privacy standards	15%

Privacy & American Business, June, 1998
(asked of computer users only)
The Clinton administration has called on industry and public-interest groups to develop effective privacy rules and practices on the Internet now, and has said that government should legislate only if the private sector fails to do this. How do you feel about this position—do you strongly agree, somewhat agree, somewhat disagree, or strongly disagree?

Agree	75%
Disagree	22%

Some observers say that businesses will take up the Clinton administration's challenge to adopt good privacy standards because they know that consumers will not engage in active buying on the Internet unless privacy and security concerns are met. Other observers say that only legislation and legal enforcement will make most businesses observe good privacy policies. Do you think that business incentives will be enough or do you think that legislation will be needed?

Business incentives enough	26%
Legislation will be needed	*68%*

NPR/Kaiser Foundation, 1999
Is this loss of privacy problem with computers or the Internet [asked about in an earlier question] something the government should do something about, or shouldn't the government be involved?

Government should do something about	*65%*
Government should not be involved	34%
Don't know	1%

(continues)

Table 2.1 Continued

Business Week/Harris Interactive, 2000
Q: Here are three ways that the government could approach Internet privacy issues. Which one of these three do you think would be best at this stage of Internet development?

		March 2000	Feb. 1998
A:	*The government should pass laws now for how personal information can be collected and used on the Internet*	*57%*	*53%*
	The government should recommend privacy standards for the Internet, but not pass laws at this time	21%	23%
	The government should let groups develop voluntary privacy standards, but not take any action now unless real problems arise	15%	19%

Pew Internet & American Life Project, April 2, 2001
From what you've seen or read, do you think that existing laws protecting a person's telephone conversations are enough to protect their email and online activities as well, or do new laws need to be written just for the Internet?

Existing laws enough	14%
New laws need to be written	*62%*
Don't know/refused	24%

Markle Foundation, 2000
Q: I'm going to read you a list of problems that some people talk about regarding the Internet. For each one, please tell me whether it would be better to have that problem addressed by the government, by private companies, or by non-profit groups that work on Internet-related issues.

Protecting the privacy of medical information on the Internet.

A:	*Government*	*57%*
	Private companies	18%
	Non-profits	16%

Percentage of adults who say "government should avoid creating new rules for the Internet because it will make the Internet less free and productive" versus "the government should develop rules to protect people when they are on the Internet, even if it requires some regulation of the Internet."

Government should develop rules	*64%*
Government should avoid creating new rules	32%

Percentage of adults who say "businesses and people on the Internet can't be trusted to regulate themselves" versus "I trust businesses and individuals on the Internet to make their own rules and follow them."

Businesses can't be trusted	*58%*
Businesses can be trusted	35%

Q: Now let me read you two short statements, and please tell me which one you favor:

(continues)

Appendix II

Table 2.1 Continued

Statement A: Some people say that companies on the Internet should not be allowed to collect information about where you go and what you buy on the Internet without first getting your explicit permission. They say Internet companies, left on their own, won't do enough to protect privacy, because they stand to gain from collecting and selling such information.

Statement B: Other people say that by collecting information about Internet usage, Internet companies can provide consumers with services better suited to their individual needs. They say that a government ban on collecting such information would limit the speed and growth of the Internet marketplace. Instead, they propose that consumers be given the option to check a box that would keep such information private.

If you had to choose, which would you favor, statement A or statement B?

A:	*Statement A*	*58%*
	Statement B	37%
	Neither (volunteered)	1%
	Don't know/refused	3%

Gallup Poll, June 28, 2001

Do you think the federal government should pass more laws to ensure citizen's privacy online or are the current laws sufficient?

Yes, federal government should pass more laws	*66%*
No, current laws are sufficient	33%
No answer	1%

Harris Poll, 2003

Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

	2003	2001	2000	1999
Somewhat or Strongly Agree	44%	38%	51%	59%
Somewhat or Strongly Disagree	*53%*	*63%*	*47%*	*38%*

Public Interests Projett, 2003

I'll read you a list of things that some people say the government has a responsibility to do. For each, please tell me whether you think it is something that the government should be responsible for, or not. . . . Guaranteeing a right to privacy . . .

Strongly responsible	*66%*
Somewhat responsible	23%
Somewhat not responsible	4%
Strongly not responsible	5%
Don't know/refused	2%

Table 2.2 Cross National Public Opinion Surveys About Privacy Fears

EU

Question:[a] Do you tend to agree or tend to disagree that you should be informed why organizations are gathering your personal data, and if they are sharing it with other organizations?

Tend to agree	91%
Tend to disagree	5%
Don't Know	4%

Canada

Question:[b] I should be asked for my permission before a company uses my personal information to build a profile on me for the purpose of marketing new products and services.

Agree	82%
Disagree	12%
Neither	6%

US

Question:[c] Privacy means different things to different people. I am going to read you a list of different aspects of privacy. Please tell me how important is . . . being in control of who can get information about you—is it extremely important, somewhat important, not very important or not important at all?

Extremely important	79%
Somewhat important	18%
Not very/ not important at all	4%

US

Question:[d] (Let me mention things that some people feel are interfering with personal privacy today. For each one, please tell me whether you think this is a major invasion of privacy, a minor invasion of privacy, or not really an invasion of personal privacy today.) . . . Companies selling information about their customers to other companies.

Major invasion of privacy	77%
Minor invasion of privacy	19%
Not really an invasion of privacy	3%
Not sure	1%

EU

Question:[e] The personal information that could be collected about people when they use these services could be used to send them advertising leaflets, or be sold to shops, insurance companies or given to public bodies. Would you be . . . about this?

Very or quite worried	72%
Not very/ not at all worried	28%

Hong Kong

Question:[f] If an advertiser keeps track of your visits to websites are the risks greater than benefits or the benefits greater than the risks?

Risks greater than benefits	72.4%
Risks about the same as benefits	22.2%
Benefits greater than risks	5.5%

(continues)

Table 2.2 Continued

EU

Question:[g] In light of the fight against international terrorism, do you think that people should agree to have their telephone calls monitored?

No, the right of individuals must always be respected	33%
Yes, if the monitoring only affects those suspected of terrorist activities	40%
Yes, but only if monitoring takes place under supervision of a (NATIONALITY) judge	14%
Yes, everyone should	7%
Don't Know	6%

US

Question:[h] In order to reduce the threat of terrorism, would you be willing or not willing to allow government agencies to monitor the telephone calls and e-mails of ordinary Americans on a regular basis?

Not willing	62%
Willing	33%
Don't know	5%

Canada

Question:[i] I would like to read you a list of initiatives which could be applied to all Canadians—not just newly arrived immigrants or those awaiting citizenship – and I would like you to tell me whether you would support or oppose being personally subjected to these actions. Allowing intelligence and law enforcement agents to monitor your personal private telephone conversations and e-mail without your knowledge.

Oppose	71%
Support	29%

US

Question:[j] Percentage of adults who say "my right to privacy is relatively absolute." versus, "sometimes my right to privacy must be balanced against the needs of society as a whole."

Right to privacy absolute	58%
Right to privacy must be balanced	38%

US

Question:[k] Which of these would you say is the biggest threat to your own personal right to privacy these days? Is it: banks and credit card companies, because they are collecting and selling marketing information about consumers; the federal government, because it can secretly collect information about people's private lives; or law enforcement agencies, because they are using more aggressive tactics against crime like surveillance cameras in public areas?

Banks and credit card companies, because they are collecting and selling marketing information about consumers	57%
The federal government, because it can secretly collect information about people's private lives	29%
Law enforcement agencies, because they are using more aggressive tactics against crime like surveillance cameras in public areas	8%
None of these (volunteered)	4%
Don't know	3%

(continues)

Table 2.2 Continued

EU

Question: Percentage of EU-15 population that trusts groups below to use their personal information "in a way you think appropriate":

The Police	72%
Social Security	69%
Tax Authorities	59%
Local Authorities	58%
National Authorities	55%
Banks and Financial Institutions	55%
Employers	55%
Market and Opinion Research Companies	43%
Insurance Companies	42%
Credit Card Companies	35%
Credit Reference Agencies	31%
Mail Order Companies	21%

US

Question:[l] As you may know, many sites on the Internet feature privacy statements, which describe what kind of information they collect about visitors to their site and how they use this information. How often do you read such privacy statements on sites . . . often, sometimes, hardly ever, or never?

Often	28%
Sometimes	31%
Hardly ever	29%
Never	12%
Don't know/refused	1%

Canada

Question:[m] How often do you read a company's privacy statement on their website before you consider doing transactions electronically with the company? Would you say . . .

Regularly	43%
Occasionally	37%
Never	20%
Don't Know	1%

Sources:

a. Special Eurobarometer 196. September 1–30, 2003. Sample: 16,124 randomly selected individuals throughout the EU. The percentages are for the EU-15. Individual country statistics can be found in the Eurobarometer publication.

b. Ekos, for The Public Interest Advocacy Centre. August, 2001. Sample: 1007 Canadians.

c. Harris Poll. February 12–16, 2003. Sample: 1,010 randomly selected adults.

d. Peter D. Hart Research Associates. March 16–20, 1999. Sample: Telephone survey of 1277 randomly selected adults.

e. Eurobarometer. October 18–November 22, 1996. Sample: 16,246 randomly selected adults throughout the EU. The percentages are for the EU-15. Individual country statistics can be found in the Eurobarometer publication.

f. Hong Kong. 2001 Opinion Survey Personal Data Privacy Ordinance.

g. Special Eurobarometer 196. September 1–30, 2003. Sample: 16,124 randomly selected adults throughout the EU. The percentages are for the EU-15. Individual country statistics can be found in the Eurobarometer publication.

(continues)

Works Cited

[1] Peter Swire. *None of Your Business.* P. 2.
[2] Peter K. Yu. *GigaLaw.com.* "An Introduction to the EU Directive on the Protection of Personal Data." http://www.gigalaw.com/articles/2001-all/yu-2001-07a-all.html.
[3] Peter Swire. *None of Your Business.* P. 2.
[4] Dorothee Heisenberg. *Negotiating Privacy.* P. 27.
[5] "EU Directive." http://www.cdt.org/privacy/eudirective/EU_Directive_.html.
[6] Dorothee Heisenberg. *Negotiating Privacy.* P. 27.
[7] Dorothee Heisenberg. *Negotiating Privacy.* P. 27.
[8] Dorothee Heisenberg. *Negotiating Privacy.* P. 27.
[9] Dorothee Heisenberg. *Negotiating Privacy.* P. 27-28.
[10] Legal Encyclopedia information about **Unwritten Law**
West's Encyclopedia of American Law. Copyright © 1998 by The Gale Group, Inc. All rights reserved.
[11] Cybertelecom: Privacy: EU. "EU Privacy Directive." http://www.cybertelecom.org/privacy/eu.htm.
[12] "Safe Harbor Overview." http://www.export.gov/safeharbor/SafeHarborInfo.htm.
[13] Wikipedia contributors, "Directive 95/46/EC on the protection of personal data," *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/w/index.php?title=Directive_95/46/EC_on_the_protection_of_personal_data&oldid=40990191.
[14] Dorothee Heisenberg. *Negotiating Privacy.* P. 83.
[15] Dorothee Heisenberg. *Negotiating Privacy.* P. 87.
[16] http://www.bbbonline.org/
[17] http://www.truste.org/
[18] Andy Oram. "Privacy Tectonics: The Shifting Responsibilities in U.S.-European Data Protection." http://www.praxagora.com/andyo/wr/safe_harbor.html.
[19] Dorothee Heisenberg. *Negotiating Privacy.* P. 86.
[20] Dorothee Heisenberg. *Negotiating Privacy.* P. 88.
[21] Dorothee Heisenberg. *Negotiating Privacy.* P. 92.
[22] Dorothee Heisenberg. *Negotiating Privacy.* P. 92.
[23] Dorothee Heisenberg. *Negotiating Privacy.* P. 93.
[24] Dorothee Heisenberg. *Negotiating Privacy.* P. 93.
[25] Dorothee Heisenberg. *Negotiating Privacy.* P. 33.
[26] Ronald B. Standler. "Privacy Law in the US." http://www.rbs2.com/privacy.htm.
[27] Ronald B. Standler. "Privacy Law in the US." http://www.rbs2.com/privacy.htm.
[28] DeCew, Judith, "Privacy", The Stanford Encyclopedia of Philosophy (Summer 2002 Edition), Edward N. Zalta (ed.), URL = <http://plato.stanford.edu/archives/sum2002/entries/privacy/>.
[29] CDT's Guide to Online Privacy. http://www.cdt.org/privacy/guide/protect/laws.shtml.
[30] Dorothee Heisenberg. *Negotiating Privacy.* P. 33.
[31] Dorothee Heisenberg. *Negotiating Privacy.* P. 33-34.
[32] CDT's Guide to Online Privacy. http://www.cdt.org/privacy/guide/protect/laws.shtml.
[33] Dorothee Heisenberg. *Negotiating Privacy.* P. 34.
[34] CDT's Guide to Online Privacy. http://www.cdt.org/privacy/guide/protect/laws.shtml.
[35] CDT's Guide to Online Privacy. http://www.cdt.org/privacy/guide/protect/laws.shtml.
[36] Dorothee Heisenberg. *Negotiating Privacy.* P. 34.
[37] Dorothee Heisenberg. *Negotiating Privacy.* P. 34.
[38] Solveig Singleton. "Privacy and Human Rights: Comparing the United States to Europe." http://www.cato.org/pubs/wtpapers/991201paper.html
[39] CDT's Guide to Online Privacy. http://www.cdt.org/privacy/guide/protect/laws.shtml.
[40] California Constitution. http://www.leginfo.ca.gov/.const/.article_1.
[41] Wikipedia contributors, "Data privacy," *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/w/index.php?title=Data_privacy&oldid=43280044.
[42] Dorothee Heisenberg. *Negotiating Privacy.* P. 52.
[43] Dorothee Heisenberg. *Negotiating Privacy.* P. 52.

[44] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
[45] Dorothee Heisenberg. *Negotiating Privacy.* P. 52.
[46] Dorothee Heisenberg. *Negotiating Privacy.* P. 52.
[47] Dorothee Heisenberg. *Negotiating Privacy.* P. 53.
[48] "Privacy and Data Protection." http://privacydataprotection.co.uk/news/.
[49] Peter P. Swire and Robert E. Litan. *None of Your Business.* P. 40-41.
[50] Andy Oram. "CANADA VAULTS OVER THE PRIVACY BAR, LEAVING UNITED STATES IN THE DUST." http://www.praxagora.com/andyo/ar/privacy_canada.html.
[51] Wikipedia contributors, "Ira Magaziner," *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/w/index.php?title=Ira_Magaziner&oldid=44682952.
[52] *Shopping.com.* http://www.shopping.com
[53] Bill Gates. "Shaping the Internet Age." http://www.microsoft.com/billgates/shapingtheinternet.asp.
[54] *Google.* http://www.google.com.
[55] *Wikipedia.* http://en.wikipedia.org/wiki/Main_Page.
[56] Bill Gates. "Shaping the Internet Age." http://www.microsoft.com/billgates/shapingtheinternet.asp.
[57] Amazon.com Online Shopping. http://www.amazon.com.
[58] Kim Zetter. "Bad Data Fouls Background Checks." http://www.wired.com/news/privacy/0,1848,66856,00.html.
[59] Peter P. Swire and Robert E. Litan. *None of Your Business.* P. 74.
[60] Peter P. Swire and Robert E. Litan. *None of Your Business.* P. 53.
[61] Peter P. Swire and Robert E. Litan. *None of Your Business.* P. 53.
[62] Denis Kelleher & Karen Murray. *IT Law in the European Union.* P. 284.
[63] Denis Kelleher & Karen Murray. *IT Law in the European Union.* P. 284.
[64] Tom Owad. "Data Mining 101: Finding Subversives with Amazon Wishlists." http://www.applefritter.com/bannedbooks.
[65] Chad King. "Data Mining for Fun and Profit." http://privacyspot.com/?q=node/view/788.
[66] Sam Ott. "Computer Intrusion Disclosures Mandated by New Law." http://www.bankersonline.com/idtheft/so_computerintrusion.html.
[67] Larry Abramson and Maria Godoy. "The Patriot Act: Key Controversies." http://www.npr.org/news/specials/patriotact/patriotactprovisions.html.
[68] "Surveillance Under the USA PATRIOT Act." http://www.aclu.org/safefree/general/17326res20030403.html.
[69] Dorothee Heisenberg. *Negotiating Privacy.* P. 140.
[70] Dorothee Heisenberg. *Negotiating Privacy.* P. 140.
[71] Dorothee Heisenberg. *Negotiating Privacy.* P. 142.
[72] "Fact Sheet: US-EU Passenger Name Record Agreement Signed." http://www.dhs.gov/dhspublic/display?content=3651.
[73] Dorothee Heisenberg. *Negotiating Privacy.* P. 147.
[74] Jo Best. "Europe Passes Tough New Data Retention Laws." http://news.com.com/Europe+passes+tough+new+data+retention+laws/2100-7350_3-5995089.html.
[75] Jo Best. "Europe Passes Tough New Data Retention Laws." http://news.com.com/Europe+passes+tough+new+data+retention+laws/2100-7350_3-5995089.html.
[76] Jo Best. "Europe Passes Tough New Data Retention Laws." http://news.com.com/Europe+passes+tough+new+data+retention+laws/2100-7350_3-5995089.html.
[77] Graeme Wearden and Karen Gomm. "Entertainment Industry 'trying to hijack data retention directive.'" http://news.zdnet.co.uk/business/legal/0,39020651,39238422,00.htm.
[78] Brian Krebs. *Security Fix.* "Microsoft Calls for National Privacy Law." http://blogs.washingtonpost.com/securityfix/2005/11/microsoft_calls.html.
[79] Jo Best. "Europe Passes Tough New Data Retention Laws." http://news.com.com/Europe+passes+tough+new+data+retention+laws/2100-7350_3-5995089.html.
[80] Eric Dash. "Europe Zips Lips; U.S. Sells ZIPs." *The New York Times.* http://www.nytimes.com/2005/08/07/weekinreview/07dash.html?ex=1145332800&en=af93b10ac11a26d5&ei=5070.

[81] "Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?" http://www.bc.edu/bc_org/avp/law/lwsch/journals/bciclr/24_1/07_FMS.htm.
[82] *BBC News*. "EU approves data retention rules." http://news.bbc.co.uk/2/hi/europe/4527840.stm.
[83] Jon Gordon. "Privacy the European Way." *Minnesota Public Radio*. http://news.minnesota.publicradio.org/features/199911/15_newsroom_privacy/01_gordonj_eu/.
[84] Dorothee Heisenberg. *Negotiating Privacy*. P. 8.
[85] Dorothee Heisenberg. *Negotiating Privacy*. P. 37.
[86] CNN.com. "Poll: Most want Congress to make sure Internet safe." http://www.cnn.com/2005/TECH/internet/06/15/internet.safety.ap/.
[87] Dorothee Heisenberg. *Negotiating Privacy*. P. 37-38.
[88] Dorothee Heisenberg. *Negotiating Privacy*. P. 38.
[89] Dorothee Heisenberg. *Negotiating Privacy*. P. 19.
[90] Eric Dash. "Europe Zips Lips; U.S. Sells ZIPs." *The New York Times*. http://www.nytimes.com/2005/08/07/weekinreview/07dash.html?ex=1145332800&en=af93b10ac11a26d5&ei=5070.
[91] Dorothee Heisenberg. *Negotiating Privacy*. P. 81.
[92] Dorothee Heisenberg. *Negotiating Privacy*. P. 81.
[93] Dorothee Heisenberg. *Negotiating Privacy*. P. 81.
[94] Dorothee Heisenberg. *Negotiating Privacy*. P. 10.
[95] Dorothee Heisenberg. *Negotiating Privacy*. P. 62.
[96] Dorothee Heisenberg. *Negotiating Privacy*. P. 63.
[97] Dorothee Heisenberg. *Negotiating Privacy*. P. 63.
[98] CNN.com. "Poll: Most want Congress to make sure Internet safe." http://www.cnn.com/2005/TECH/internet/06/15/internet.safety.ap/.
[99] Kimber Spradlin. "Data Privacy Standards, American Style." http://news.com.com/Data+privacy+standards%2C+American+style/2010-1029_3-5892395.html.
[100] "Microsoft Advocates Comprehensive Federal Privacy Legislation." http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx.
[101] Brad Smith. "Protecting Consumers and the Marketplace:The Need for Federal Privacy Legislation." Letter from Microsoft Corporation.
[102] Sam Ott. "Computer Intrusion Disclosures Mandated by New Law." http://www.bankersonline.com/idtheft/so_computerintrusion.html.

Bibliography

Abramson, Larry, and Maria Godoy. "The Patriot Act: Key Controversies." NPR. 14 Feb. 2006. <http://www.npr.org/news/specials/patriotact/patriotactprovisions.html>.

"Amazon.Com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs, and More." Amazon.Com. <http://www.amazon.com>.

"BBBOnLine, Inc. --Promoting Trust and Confidence on the Internet." BBBOnline. 2003. Better Business Bureau. 15 Dec. 2005 <http://www.bbbonline.org/>.

Beach, Derek. The Dynamics of European Integration: Why and When EU Institutions Matter. New York: Palgrave Macmillan, 2005.

Best, Jo. "Europe Passes Tough New Data Retention Laws." CNET News.Com. 14 Dec. 2005. <http://news.com.com/Europe+passes+tough+new+data+retention+laws/2100-7350_3-5995089.html>.

California. Offficial California Legislative Information. Legislative Council. California Constitution. <http://www.leginfo.ca.gov/.const/.article_1>.

"Cybertelecom: Privacy: EU." Cybertelecom. 26 Apr. 2006. 27 Apr. 2006 <http://www.cybertelecom.org/privacy/eu.htm>.

Dash, Eric. "Europe Zips Lips; U.S. Sells ZIPs." The New York Times. 7 Aug. 2005. <http://www.nytimes.com/2005/08/07/weekinreview/07dash.html?ex=1145332800&en=af93b10ac11a26d5&ei=5070>.

"Data Privacy." Wikipedia. 11 Mar. 2006. <http://en.wikipedia.org/w/index.php?title=Data_privacy&oldid=43280044>.

Decew, Judith. "Privacy." Stanford Encyclopedia of Philosophy. 14 May 2002. Stanford. <http://plato.stanford.edu/archives/sum2002/entries/privacy/>.

"Directive 95/46/EC on the Protection of Personal Data." Wikipedia. 24 Mar. 2006. 28 Mar. 2006 <http://en.wikipedia.org/w/index.php?title=Directive_95/46/EC_on_the_protection_of_personal_data&oldid=40990191>.

"EU Approves Data Retention Rules." BBC NEWS. 14 Dec. 2005. <http://news.bbc.co.uk/2/hi/europe/4527840.stm>.

"EU Directive." Center for Democracy and Technology. 27 Jan. 2006 <http://www.cdt.org/privacy/eudirective/EU_Directive_.html>.

European Commission. Justice and Home Affairs. Data Protection. <http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm>.

"Fact Sheet: US-EU Passenger Name Record Agreement Signed." Department of Homeland Security. <http://www.dhs.gov/dhspublic/display?content=3651>.

Gates, Bill. "Shaping the Internet Age." Bil Gates' Web Site. Dec. 2000. 24 Apr. 2006 <http://www.microsoft.com/billgates/shapingtheinternet.asp>.

Gordon, Jon. "Privacy the European Way." Minnesota Public Radio. Nov. 1999. <http://news.minnesota.publicradio.org/features/199911/15_newsroom_privacy/01_gordonj_eu/.>.

Heisenberg, Dorothee. Negotiating Privacy. Boulder: Lynne Reinner, Inc., 2005.

"http://www.cdt.org/privacy/guide/protect/laws.shtml." CDT's Online Guide to Privacy. Center for Democracy and Technology. <http://www.cdt.org/privacy/guide/protect/laws.shtml.>.

"Ira Magaziner." Wikipedia. 20 Mar. 2006. <http://en.wikipedia.org/w/index.php?title=Ira_Magaziner&oldid=44682952>.

Kelleher, Denis, and Karen Murray. IT Law in the European Union. London: Sweet & Maxwell, 1999.

King, Chad. "Data Mining for Fun and Profit." Privacy Spot. 4 Jan. 2006. <http://privacyspot.com/?q=node/view/788>.

Krebs, Brian. "Microsoft Calls for National Privacy Law." Washingtonpost.Com. 3 Nov. 2005. <http://blogs.washingtonpost.com/securityfix/2005/11/microsoft_calls.html>.

Lodder, Arno R., and Henrik Kaspersen. EDirectives: Guide to European Union Law on E-Commerce. The Hague: Kluwer Law International, 2002.

"Microsoft Advocates Comprehensive Federal Privacy Legislation." Microsoft. 3 Nov. 2005. <http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx>.

"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." Organisation for Economic Co-Operation and Development. OECD. <http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>.

Oram, Andy. "CANADA VAULTS OVER THE PRIVACY BAR, LEAVING UNITED STATES IN THE DUST." Praxagora. 13 Oct. 1998. American Reporter. <http://www.praxagora.com/andyo/ar/privacy_canada.html>.

Oram, Andy. "Privacy Tectonics: the Shifting Responsibilities in U.S.-European Data Protection." Praxagora. Nov.-Dec. 2000. Editor at O'Reilly Media and a member

of Computer Professionals for Social Responsibility. <http://www.praxagora.com/andyo/wr/safe_harbor.html>.

Ott, Sam. "Computer Intrusion Disclosures Mandated by New Law." BankersOnline.Com. 20 Nov. 2002. <http://www.bankersonline.com/idtheft/so_computerintrusion.html>.

Owad, Tom. "Data Mining 101: Finding Subversives with Amazon Wishlists." Applefritter. 4 Jan. 2006. <http://www.applefritter.com/bannedbooks>.

Oxman, Stephen A. "EXEMPTIONS TO THE EUROPEAN UNION PERSONAL DATA PRIVACY DIRECTIVE: WILL THEY SWALLOW THE DIRECTIVE?" Boston College Law School Student Publications. Boston College Law School. <http://www.bc.edu/bc_org/avp/law/lwsch/journals/bciclr/24_1/07_FMS.htm>.

"Poll: Most Want Congress to Make Sure Internet Safe." CNN.Com. 15 June 2005. <http://www.cnn.com/2005/TECH/internet/06/15/internet.safety.ap/>.

"Privacy & Data Protection." Privacy & Data Protection. 28 Apr. 2006 <http://privacydataprotection.co.uk/news/>.

"Safe Harbor Overview." U.S. Department of Commerce. 21 Apr. 2006 <http://www.export.gov/safeharbor/SafeHarborInfo.htm>.

"Shopping.Com - Find, Compare, and Buy Anything in Seconds." Shopping.Com. 27 Apr. 2006. 27 Apr. 2006 <http://www.shopping.com>.

Singleton, Solveig. "Privacy and Human Rights: Comparing the United States to Europe." CATO Institute. 1 Dec. 1999. <http://www.cato.org/pubs/wtpapers/991201paper.html>.

Spradlin, Kimber. "Perspective: Data Privacy Standards, American Style." CNET News.Com. 11 Oct. 2005. <http://news.com.com/Data+privacy+standards%2C+American+style/2010-1029_3-5892395.html>.

Standler, Ronald B. "Privacy Law in the USA." 1997. 12 Mar. 2006 <://www.rbs2.com/privacy.htm>.

Standler, Ronald B. "Privacy Law in the USA." 1997. 12 Mar. 2006 <://www.rbs2.com/privacy.htm>.

"Surveillance Under the USA PATRIOT Act." American Civil Liberties Union. 3 Apr. 2003. <http://www.aclu.org/safefree/general/17326res20030403.html>.

Swire, Peter P., and Robert E. Litan. None of Your Business. Washington, D.C.: Bookings Institution P, 1998.

"TRUSTe - Make Privacy Your Choice." TRUSTe. 15 Dec. 2005 <http://www.truste.org/>.

"Unwritten Law." West's Encyclopedia of American Law. 1998. 12 Apr. 2006. Keyword: Unwritten Law.

Wearden, Graeme, and Karen Gomm. "Entertainment Industry 'Trying to Hijack Data Retention Directive'" ZDNet UK. 24 Nov. 2005. <http://news.zdnet.co.uk/business/legal/0,39020651,39238422,00.htm>.

Yu, Peter K. "GigaLaw.Com: an Introduction to the EU Directive on the Protection of Personal Data." GigaLaw.Com. July-Aug. 2001. Benjamin N. Cardozo School of Law. 14 Apr. 2006 <http://www.gigalaw.com/articles/2001-all/yu-2001-07a-all.html>.

Zetter, Kim. "Bad Data Fouls Background Checks." Wired News. 14 Mar. 2005.

<http://www.wired.com/news/privacy/0,1848,66856,00.html.>.