

Copyright

By

Thomas J (TJ) Costello

2003

COPYRIGHT 2003

**The Economic Trade-offs of Privacy:
Exploring the Interaction of Economics and Privacy
in the Formulation of Privacy Policy**

By

Thomas J (TJ) Costello, B.S.

Professional Report

Presented to the Faculty of the Graduate School
of the University of Texas at Austin
In Partial Fulfillment of the Requirements
for the Degree of

Master of Public Affairs

The University of Texas at Austin

2003

Acknowledgments

Over the past two years at the Lyndon B. Johnson School of Public Affairs, I have had the honor of studying with some of the most fascinating and learned people I have yet encountered. This goes for professors and colleagues who entered the LBJ School with me in August of 2001 as well as many who came before and after. Over these two years I have had the opportunity to study a wide variety of topics and learn a great deal about policy, public affairs, and the United States in general. As Professor Kenneth Apfel (former Commissioner of the Social Security Administration 1997-2001) once said to me, “TJ, you are the ultimate generalist.” When I relayed this anecdote to Professor Elspeth Rostow, she simply smiled, in a way that only she can, and seemed to say, “Professor Apfel is quite wise.”

Deciding upon a topic for this Professional Report was difficult. At first I wanted to include things I learned from my career (strategic planner, analyst, educator, ADR specialist); the many courses I took at the LBJ School; my understanding of economics (from Ithaca College and beyond); and the everyday bits of information I picked up from the many fascinating people I have met.

In the fall of 2002 I worked with Professor Philip Doty at the School of Information here at UT. In his class “Federal Information Policy”, we studied many aspects of privacy. I began to wonder about some of the arguments for and against privacy policy and how these arguments play out from an economic vantage point. This curiosity is what led to this report.

In the numerous Professional Reports written by my predecessors at the LBJ School, each writer acknowledged certain people, thanked others, and dedicated their reports to an important individual(s) in their life. As mentioned earlier I have had the honor of meeting and working with a large variety of people. From New Rochelle to Ithaca, to Princeton, to New York City, to Austin each person I have come in contact with has had an impact on my decision to be a part of something special: the LBJ Community. Looking back, there are certain people who had an influence on me, but also impressed me with the impact they made on others. They are Mr. Thomas J. Costello Sr., the young ladies I coached in central New Jersey 1993-2001, and Sara Lovering – LBJ School '02.

My LBJ experience has been a rewarding one but would not have been so without the help and support of so many. To Dean Edwin Dorn, Marilyn Duncan, Dr. Philip Doty, and of course Professor Elspeth Rostow; plus Emily Finnan (always there) and Erica Swanholm (from day one to day last), and so many others I say thank you for everything.

TJC

**The Economic Trade-offs of Privacy: Exploring the Interaction of Economics
and Privacy in the Formulation of Privacy Policy**

By

T J Costello, M.P.Aff.

The Lyndon B. Johnson School of Public Affairs at
the University of Texas at Austin, 2003

Supervising Committee: Dr. Philip Doty; Dr. Kenneth Flamm; Admiral Bobby Inman

What do a civil suit, buying a book, reserving a hotel room over the internet, and assessed property values have in common? Each of these unrelated concerns has privacy and economic implications. This report shows that privacy discussion often takes place utilizing economic terminology, yet the economic trade-offs are absent from the formulation of the final privacy policy. With privacy policy being developed in both the public and private sectors, all of society is affected by its changes and implementation. This report takes four of the countless aspects of privacy (confidentiality in mediation, Section 215 of the USA PATRIOT Act, “un-privacy” and the internet, and “semi-public” information) and illustrates how understanding privacy policy from an economic perspective is important, and moreover, that adopting economic policies that maximize privacy (and vice versa) is a strategy that works.

Table of Contents

Chapter 1. Purpose	1
Chapter 2. Searching for Privacy	4
Definitions of Privacy	5
Chapter 3. Structure	7
Chapter 4. Pre-litigation Mediation	10
Privacy in Pre-litigation Mediation	11
Important Stakeholder Groups.....	13
Costs	13
Benefits	14
Conclusion	16
Summary Matrix (Chapter 4).....	20
Chapter 5. “Un-privacy” and the Internet.....	21
Un-privacy of the Internet	22
Important Stakeholder Groups.....	23
Costs	23
Benefits	24
Conclusion	25
Matrix (Summary for Chapter 5).....	27
Chapter 6. USA PATRIOT Act, Section 215	28
Privacy and Section 215	29
Important Stakeholder Groups.....	30
Costs	30
Benefits	31
Conclusion	32
Summary Matrix (Chapter 6).....	36

Chapter 7. “Semi-public” Information.....	37
Privacy and Semi-public Information.....	40
Important Stakeholder Groups.....	40
Costs	41
Benefits.....	41
Conclusion.....	42
Equalization Model.....	43
Matrix (Summary for Chapter 7).....	47
Chapter 8. Conclusion.....	48
Appendix A. Defining Terms: What is Privacy?.....	50
Appendix B. Defining Terms: Mediation.....	53
Appendix C. USA PATRIOT Act Section 215.....	55
Appendix D. The Privacy Policy Matrix.....	57
Personal Correspondence.....	59
References.....	61
VITA.....	69

Chapter 1. Purpose

In reviewing the literature on privacy, this researcher found a great deal of material about the subject, much of it utilizing economic terms. In view of this phenomenon, it was decided that an examination of privacy from an economic perspective might prove interesting. However, little research was available specifically on the effect of economics on privacy. If privacy is thought of in economic terms (cost, supply, and demand), how do economics and privacy interact? This report will attempt to give insight into this economics/privacy interaction and strive to answer the question of how privacy conflicts and policy are affected by or affect economics and what trade-offs arise from that interaction.

With the legal structure of privacy comparable to a patchwork quilt (Gellman, 1998, p. 193), decision makers need to recognize how these many privacy contexts can benefit consumers, businesses, and the overall economy and how privacy policy can directly interfere with and affect those benefits (Cate, 2001, xv). As mentioned, privacy is often discussed in economic terms (retention, cost, scarcity, value, opportunity), yet economics is rarely part of the privacy policy debate. Alessandro Acquisti points out, "Economics is about allocating scarce resources among competing uses. Economics is about trade-offs." He continues to point out that even if a privacy concern is not measured by monetary criteria, "most [privacy discussions] do raise trade-offs - and economics can be used to analyze those" (2002, p. 2). This report will show how economics and privacy policy interact and will demonstrate that the interaction between privacy and economics is essential to formulating good privacy policy. The report will illustrate how:

- Privacy and economic concerns are highly interwoven.
- Both economics and privacy can be reliant on each other's effectiveness for a privacy policy to be beneficial.
- Economic reasoning can be incorporated into new privacy policy to help maintain privacy as intended by past policies.
- Economics occasionally plays an important secondary role in privacy policy.
- Policy changes or enhancements might be employed to reinforce the interaction between privacy and economics.

Personal privacy concerns are comprised of such issues as credit reports, privacy within one's home, search and seizure, telemarketers, psychological testing and video surveillance. Research, including literature reviews, analytical interpretation, and personal correspondence, reaffirmed the initial determination that privacy concerns and the policy surrounding those concerns are often described in economic terms and that very little analysis of privacy from an economic perspective exists. Richard A. Posner's essay, "The Economics of Privacy" discusses how there is a dearth of economic analysis of privacy and argues the "extension of the economic study of information to the privacy of information [is] overdue" (1981b, p. 408). The lack of analysis raises the question, how could privacy be examined using economic theories, outcomes, methods, and criteria?

Economic theory of supply and demand, cost benefit analysis, opportunity cost, and transaction cost all play into privacy policy. Hal R. Varian, Dean of the School of Information Management and Systems at the University of California at Berkeley, begins his white paper *Economic Aspects of Personal Privacy* by stating, “The advent of low cost technology for manipulating and communicating information has raised significant concerns about personal privacy” (1996, p. 2). Posner describes privacy legislation as redistributive and inefficient (1981b, p. 408). Samarajiva writes how the change in the world’s economy from “mass-production to mass-customization” is creating a substantial need for detailed information on consumers (1998, p. 277).

Privacy is an extremely broad and cumbersome topic. Since Warren and Brandeis wrote “The Right to Privacy” in 1890, numerous definitions have been introduced to help explain, clarify, or institute privacy as a policy. Yet no agreement has been reached on what privacy means or encompasses. As the United States and the world economies have become more complicated and reliant on computers, privacy concerns have grown. Chief Justice William Rehnquist has written:

Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks... These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business [transactions and conversations] (Liptak, 2002, ¶ 2).

With digital technology making privacy concerns more complicated, economic factors have an even stronger affect on privacy policy and the interpretation of that policy. As digital technology evolves, privacy is being compromised by databases, loyalty clubs, federal acts, and general business practices.

Economic and privacy policy are created both through the public and private sectors, making privacy a governmental, business, and individual concern. Even with governments’ power to infringe on one’s privacy, it is interesting to note that people seem more willing to accept government intrusion but reluctant to consent to commercial ones. Liptak observes, “Government’s power is enormous and often wielded in secret, while consumers retain substantial control over their commercial information” (¶ 19). Yet Goss points out that businesses take advantage of consumers through a “systematic accumulation of individual and aggregate data about persons, sometimes by devious means,” which Goss states is equivalent to “consumer espionage” (1995, p. 175).

This report reviews and analyzes four specific privacy issues.¹ These are Section 215 of the USA PATRIOT Act; “semi-public” information; confidentiality in

¹ The topics chosen for review, while offering a strong representation of privacy concerns, do not encompass all aspects of privacy, nor is every economic concept or theory integrated into this analysis. The many other facets of privacy not included in this report were omitted due to space constraints.

mediation; and “un-privacy” and the internet.² These privacy policies were chosen for their broad policy coverage and their relationship to economic criteria. The objective of this report is to look at the four above-mentioned aspects of privacy and examine how they interact with economic criteria. This report will show that, when it comes to privacy policy, the economic impacts are real and should be recognized and considered in formulating that policy.

² As reported in the New York Times on December 29, 2002, the word “internet” typically uses a capital “i”. However Joseph Turow, professor at the Annenberg School for Communication at the University of Pennsylvania, noted that it is time for the word “Internet” to become “internet.” Steven Jones, professor at the University of Illinois at Chicago pointed out that throughout history new technology has been capitalized until integrated into society; it then loses the capitalization. Additionally, many words regarding the online world have already made the transition to lowercase, and in fact the word “internet” is starting to be used without capitalization (Schwartz, 2002a). This report will follow Torow and Jones’ lead and use all lowercase when referring to the internet.

Chapter 2. Searching for Privacy

Privacy is a controversial subject, if for no other reason than there is no one definition for the term “privacy.” With privacy being so broad a concept, this chapter is intended to give better context to its application from an economic viewpoint.

The Debate over Privacy

“The right to be left alone” - these six simple words have been the center of discussion for over one hundred years. Warren and Brandeis stated in their article “The Right to Privacy” (*Harvard Law Review*, 1890) that “Political, social, and economic changes entail the recognition of new rights... Gradually the scope of the legal rights broadened, and now the right to life means the right to enjoy life – the right to be left alone” (1890, ¶ 1). The authors also suggest that every individual has the right to determine whether or not to withhold private information and thoughts from public scrutiny. Assuming this right to withhold information exists, when a company like DoubleClick offers a service that tracks a person’s usage of the internet in order to target specific advertisements to specific customers (Knapp, 2003, p. 3), is this strategy an invasion of privacy, or simply a good business model?

A nearly universal agreement regarding privacy is how difficult privacy is to define. Walter M. Carlson is quoted as saying “there are more questions than there are answers on the matter of an individual’s privacy and its socially acceptable protection from misuse” (Doty, 2001, p. 124). Privacy has different meanings to different people, having been described as everything from control over personal information to unfettered personal reproductive rights to limits on government intrusion. The United States Constitution does little to define privacy (Mitra, 2001, p. 4). While some privacy advocates argue that amendments to the Constitution, such as the Bill of Rights, try to address privacy it could be argued that the amendments, with their purposeful vagueness, broaden the definition (Mitra, p. 5). Table 2.1 offers a good illustration of how broad privacy can be. In the United States, the term “privacy” might include any protection of information, physical person, personal space, or even access to one’s belongings.

The fact that there is very little consensus about the definition of privacy has caused all levels of government, from Congress to state legislatures, as well as the press and the public, to be, as James Harper testified to Congress³, “less able to find solutions to the many

³ James Harper, Editor, Pricacilla.org., presented this statement to the U.S. Congress, House Subcommittee on Commercial and Administrative Law Federal Agency protection of Privacy Act: Hearing. In being questioned by Congressman Watt of North Carolina, Harper later defined privacy as “a subjective condition people enjoy when they first have legal power to control how information is shared, and, second, exercise that power consistent with their values and interests.” (2002, p. 34) Harper’s prepared statement can be found in Appendix A.

problems and legitimate concerns that popularly fall under the heading of ‘privacy’” (U.S. Congress, 2002, p. 22).

Table 2.1

Privacy Examples

“Privacy”	Example
Protection of information related to individual attributes.	Name; age; financial status; medical and educational history; taste in food, clothing, and entertainment
Protection of information about transactions	Retail purchases and Web site browsing; especially purchases through telephone or computer
Protection of information related to social and other relationships, especially intimate relationships	Marital and parental status; group membership; religious and political affiliation; and identities of correspondents
Protection of physical isolation	Limitation of physical intrusion and searches by the government and its agents as well as by searches by commercial action
Prohibition of access to the physical self	Unwanted touching and the forced giving of fingerprints, and of blood, tissue, or DNA samples
Prohibition of access to one’s attention	Limitation of intrusion into awareness such as calls from telemarketers and targeted as well as broadly aimed advertisements
Protection of information related to physical location and activity	
Freedom to act	To be politically active and to live an erotic life and make reproductive decisions largely free from social and governmental scrutiny.

Source: Philip Doty, 2001, p. 125

Privacy has been called “a totally overused and poorly understood term” (Liptak, 2002, ¶ 11). Arthur Miller, in *The Assault on Privacy*, offers his own definition pertaining to public records: “Each individual is entitled to exercise reasonable control over what information about him is collected by government; its use; how it will be safeguarded; and when, to whom, and for what purpose it will be disclosed” (Texas Advisory Commission, 1977, p. 11).

Definitions of Privacy

Every report, paper, article, or book about privacy or aspects of privacy has a section on privacy definitions and notes how there is no clear definition. As has been illustrated, privacy is a term that covers an astonishingly large number of definitions and components of life.

The definition by Warren and Brandeis that privacy is “the right to be left alone” has been noted continuously as a benchmark (Alderman & Kennedy, 1995). In discussing an

economic view of privacy however, going beyond Warren and Brandies is necessary. Varian, for instance, states that privacy is the “right not to be annoyed” (1996, p. 3). Varian’s definition could be considered a summary of Samarajiva’s definition, which is “the capability to explicitly or implicitly negotiate boundary conditions of social relations” (1998, p. 283). While Varian and Samarajiva both look at privacy as a social interaction that should be defined on one’s own terms, Richard Posner argues that privacy can be very selective and manipulative (1981a, p. 234).

This report will show that privacy in economic terms is more than being left alone. In commerce, reduction in privacy provides opportunity for others to collect and store information about a customer or client. The power to control selective disclosures of information about oneself is the “conceptual core of privacy” (Texas Advisory Commission, p. 11). To be selective about one’s disclosure of privacy and avoid being annoyed is what Posner means by his assertions that most people “want to manipulate the world around them by selective disclosure of facts about themselves” (1981a, p. 234). Varian argues that, “I don’t really care if someone has my phone number as long as they do not call me during dinner” (1996, p. 3). The fundamental fact is that, while people want greater privacy, they do not recognize that it involves economic trade-offs.

COPYRIGHT 2003

Chapter 3. Structure

This chapter is designed to give the reader a better understanding of the report as a whole and introduce the four privacy policy case studies chosen for review. These four topics (confidentiality in mediation, personal privacy associated with the internet, privacy of public information, and a person's right to privacy against law enforcement's need for information) emphasize the variety, importance, and inconsistency of the interaction between privacy and economics. A great deal has been written on privacy as a concept and privacy as a right, but, as mentioned, little has been written about how economic concerns can be utilized to protect privacy and vice versa. Privacy and economics do influence each other and these next four chapters will elucidate this interaction.

By demonstrating how privacy and economics can, do, and could interact, it is easier to conceptualize rational arguments about existing and future privacy policy. In exploring economic reasoning as a part of privacy policy formulation, privacy concerns discussed in this report are done so from an economic vantage point. For instance, this report does not attempt to discuss whether Section 215 of the USA PATRIOT Act is good legislation or not. Rather, by looking at Section 215 from an economic standpoint, this report recommends that provisions such as the sunset clause in the Act be maintained to allow Congressional oversight of the costs associated with this policy.

Four Case Studies

Chapter 4, Pre-litigation Mediation: Privacy in the form of confidentiality is shown to be imperative for the success of mediation. This chapter will demonstrate how confidentiality plays an important role in pre-litigation mediation; illustrate the various cost savings associated with the mediation process; and introduce pre-litigation mediation as the best alternative to filing a lawsuit.

The cost of mediation is considered independently of confidentiality. When the savings from using mediation over litigation are added up, confidentiality is not included in the equation. Similarly, when the confidentiality of mediation is considered, there is no dollar figure attached. In the case of pre-litigation mediation, there is a balance between confidentiality and costs, where a change in privacy causes the economic aspects of mediation to become skewed. In the end, the use of pre-litigation mediation will be advocated, and the reinforcement of confidentiality laws for mediators will be recommended.

Chapter 5, Un-privacy and the Internet: In internet commerce, privacy concerns are clearly entwined with economics. Internet commerce, to be efficient, needs customers willing to give up a certain amount of privacy. Businesses utilizing the internet are at a distinct disadvantage when customer relations are considered; the "online shopkeeper" never meets the customer. To make up for this disadvantage, internet businesses imbed cookies into computers, track e-mail addresses, require registration to access information, and so on. Additionally, to offer more privacy to customers (i.e., reduce unwanted e-mails and advertisements) internet commerce needs to obtain more information on consumers. To maximize privacy yet allow for this economic reality, it will be suggested that clear and easily

understood “opt out” measures be incorporated into e-business practices such as Web site design.

Chapter 6, Section 215 of the USA PATRIOT Act: In 2001 the USA PATRIOT Act was signed into law. Section 215 of this Act focuses on law enforcement’s information gathering against suspected terrorists and has received criticism under the premise that civil liberties are being reduced. Critics claim that Section 215 is causing irreparable harm to information providers by allowing the confiscation of a customer’s records. In this case, economic considerations play a secondary and indirect role but are clearly part of the privacy argument. For the USA PATRIOT Act, financial oversight of law enforcement’s utilization of the Act and respect for the embedded sunset clauses must be championed.

Chapter 7, “Semi-public” Information: This chapter builds upon the fact that greater quantities of information are being stored by governmental agencies. Some of this information is and has been available to the general public. With the advent of the internet and other electronic media, information that was public but had limited access (semi-public) is now more readily available. Incorporating economic measures, such as direct costs and opportunity costs, to ensure limited access to information held by public entities is one way to protect the limited amount of privacy that is retained with semi-public documents.

Overall, these four distinct and separate privacy issues and their economic costs and benefits will offer a solid base for examining other privacy policy issues in the future.

Interpreting the Four Cases

The four privacy policy concerns outlined above will be introduced and analyzed so as to better define their distinct aspect of privacy, the economic impact and concerns associated with the policy, and any questions associated with the development or implementation. Each chapter will introduce the issue being discussed. Relevant historical background concerning each privacy policy’s development will be included, offering a better understanding of why this issue was chosen for examination as well as an idea of the economic factors that surround the specific privacy policy.

Privacy Component: Every privacy policy decision is based on a perception of privacy lost or privacy gained. The specific privacy component justifying the policy will be introduced as will the context in which this privacy concern has been incorporated into policy.

Important Stakeholder Groups: Persons and groups most immediately affected by the specific privacy issue will be identified. These stakeholders might include individuals, private businesses, federal government, local government, and law enforcement.

Costs: Each privacy policy has its own direct, opportunity, transaction and indirect costs. Specific economic and social costs associated with this particular aspect of privacy and how the various players might be affected will be examined

Benefits: Once the costs have been examined, are there any benefits from this privacy policy? This section will look at the specific economic and social benefits associated with the specific policy. What has been gained directly and indirectly?

Conclusion: Each of the cases will end with a conclusion reviewing the costs, benefits and challenges facing society with regard to maintaining or formulating privacy policy. Also introduced and discussed are policy changes that might enhance the current economic and privacy interaction. Each chapter's conclusion will be followed by a matrix designed to offer a summary of the chapter's main points.

The Privacy Policy Matrix (Appendix D)

Appendix D is a matrix summary of the cases discussed in this report. This matrix offers a means to compare privacy policies and their economic implications.

Copyright 2003

Chapter 4. Pre-litigation Mediation

While the idea of mediation as a privacy policy may seem odd, the implementation of mediation to resolve a dispute offers privacy protection that most other dispute resolution methods do not. It is precisely because of the privacy associated with mediation that an economic benefit exists. However, unlike many other privacy issues, mediation relies on a balance between privacy and economics. If, for example, the economic costs associated with mediation change significantly, the privacy gained through the mediation process could prove irrelevant.

In the United States, the Constitution guarantees one's right to a trial. That right, however, can be waived through contract or separate agreement. Over time, the legal community has struggled with the fact that the courts have become adversarial, not conducive to preserving relationships, potentially very costly, and open to public review. This struggle has led to the increased use of alternative dispute resolution (ADR).

ADR is "a method for out-of-court resolution of conflict through the interventions of third parties" (American Arbitration Association [AAA]-Consumer Due Process, 1998, p. 8). ADR options include, but are not limited to, mediation, arbitration, mini-trials, and partnering. Of the ADR methods, mediation offers the most flexibility and greatest benefit for privacy retention and cost savings.

Mediation⁴ has been described by the American Arbitration Association (AAA) and the courts as a process in which a non-aligned (neutral) third party (mediator) facilitates communication between disputants and assists disputing parties in reaching a mutually acceptable resolution to their dispute (AAA-Guide, 2000, p. 3; Stong, 2002, p. 5). In mediation, the mediator does not have the authority to make a binding decision. The goal of mediation is for a mediator, utilizing skills such as facilitation, confidential individual conferences with the parties, and cost valuation, to get the parties involved to agree to a binding resolution.

Mediation as a method of resolving disputes is gaining more respect and use.⁵ In fact, mediation has become the fastest growing form of ADR (Stamato, 2000; Personal Correspondence, Claire Gutekunst, December 4, 2002).

Pre-litigation mediation is one of the three main mediation methods; the other two are court-mandated mediation and post-filing mediation.⁶ Of the three, pre-litigation mediation is

⁴ For a comprehensive definition of mediation, see Appendix B.

⁵ For example, the Equal Employment Opportunity Commission's use of mediation cut its backlog of pending cases from 111,451 in 1995 to just over 52,000 in 1999 (Stamato, p. 29).

⁶ Court-mandated mediation is implemented by a trial judge after a case has been filed. Mediators are typically court-chosen or recommended. Post-filing mediation takes place after a case has been filed and the parties agree

the most productive, offering the greatest amount of privacy (i.e. confidentiality) as well as opportunity cost and other economic benefits.⁷

Privacy in Pre-litigation Mediation

Privacy in a pre-litigation mediation comes in two forms. The first is the privacy retained by not filing court papers. When a lawsuit is filed with the courts, the dispute becomes a matter of public record. The second form is the confidentiality of the mediation process.

A dispute heard in pre-litigation mediation has not been filed with the courts, thus information about the dispute is not public. The privacy retained by not having the case in the public eye can be important especially when claimants do not want their identities disclosed and/or a business wants to avoid unnecessary scrutiny. If the potential exists for all phases of a trial and evidence presented to be available to the public, privacy is a strong incentive for disputing parties to enter the mediation process early in a legal dispute.

Confidentiality⁸ is one of the greatest benefits of mediation, and this benefit is intensified through the use of pre-litigation mediation. In mediation, discussions can be held where both sides can feel comfortable revealing information to the mediator. Confidentiality in mediation is essential to allow the parties to candidly and thoroughly discuss all possible avenues of settlement (Sharp, 1998, ¶ 4). The knowledge that an informal, honest, and confidential discussion can take place with the mediator adds to the speed and success of mediation (Stamato, 2000, p. 38).

A strong confidentiality component within the mediation process has been criticized by some lawmakers and consumer advocacy groups (Maharaj, 2000; Berman, 2000). The courts, however, have recognized the importance of confidentiality during mediation. The Court of Appeals for the Second Circuit reasoned that if the parties:

[C]annot rely on confidential treatment of everything that transpires during these [mediation] sessions, then counsel of necessity will feel constrained to conduct themselves in a cautious, tight-lipped, non-committal manner more suitable to poker players in a high stakes game than adversaries attempting to arrive at a just solution of a civil dispute (Sharp, ¶ 1).

to utilize an outside mediation service while the case is making its way through the legal system. Pre-litigation mediation occurs before any papers have been filed with a court.

⁷ Economic savings might include opportunity costs associated with time spent in a deposition, client relationships saved, retained employees, and lower direct payments to attorneys.

⁸ Confidentiality is defined as privacy within the legal system. In other words, one's privacy during a lawsuit or other legal proceeding is based on the amount of confidentiality that exists.

On July 9, 2001, the Supreme Court of California reaffirmed the confidentiality of all mediation communications when it ruled on *Foxgate Homeowners' Association v. Bramalea California, Inc.* (No. S087319 (Cal. July 9, 2001))(Madison, 2001). This decision upheld sweeping protection for the confidentiality of mediation. In doing so, however, the court recognized that a mediator's independent role "is also of paramount importance and should not be compromised" (Madison, p. 11). Conrad notes that "guarantees of confidentiality facilitate an atmosphere of fairness and trust between the parties and the mediator, which is essential to an effective mediation" (1998, p. 46).⁹

In the State of Texas, confidentiality plays a major role in mediation. The Texas ADR Procedures Act, Chapter 154, Civil Practice and Remedies Code Sections 154:053(b) and 154.073, strongly protects the confidentiality of mediation (Fagan, 2002). Additionally, Texas addresses confidentiality in mediation in the Texas Governmental Dispute Resolution Act of 1997. Section 2008.054 of this Act states that confidentiality of certain records and communications applies "to the communications, records, conduct, and demeanor of the impartial third party and the parties" (Texas SB 694, 1997). This legislation helps ensure the frank exchange of information between the parties and the mediator.

Parties might be less willing to discuss embarrassing or problematic situations with a mediator if either party believes information revealed during a mediation will become public knowledge either voluntarily or through a court order. With confidentiality protected by a mediator, parties are able to utilize the mediator's talents fully. Olivella pointed out, "If we ever have information that we do not want the other side to know, but we want the mediator to know it exists, we simply tell him not to divulge it" (Personal Correspondence, 2003). With enhanced confidentiality protections for communication within mediation, an increased use of the mediation process is likely to result (Stong, 2002, p. 6).

Confidentiality is not just a matter of a mediator or parties divulging information or keeping information out of the courts. Mediation is a private process (Stong, p. 5) designed to foster a more open and amicable setting, to which Stamato reminds us, it helps "individuals achieve better and more lasting resolutions of value to themselves, and to assist corporations in meeting and protecting their interests as well" (p. 29). A business participating in the mediation process usually does not wish to discuss its internal problems in an open forum, nor is there a wish to encounter the stress, embarrassment and impersonal features of the courts.

⁹ Conrad continues by noting that the flow of information will be enhanced when parties are assured that what is discussed in mediation will remain confidential and will not be used later against the parties. In *NLRB v Macaluso*, the 9th Circuit Court noted that "parties involved in mediation sessions must have the confidence that information disclosed will not subsequently be divulged, voluntarily or by compulsion... The complete exclusion of mediator testimony is necessary to the preservation of an effective system of labor mediation."

Important Stakeholder Groups

Courts: Potentially all civil matters can enter the court system.¹⁰ Pre-litigation mediation offers the courts a means of having non-criminal cases resolved before they enter an already overburdened court system. Courts are overburdened by their caseloads and are actually encouraging parties to enter mediation when a case is filed (Keating, 1995, ¶ 26; Lande, 1998, p. 22). The reduction of cases and the potential for an amicable decision has led the courts to look with favor on pre-litigation mediation, and they have worked to preserve the integrity and confidentiality of the mediation process.

Private Business: Many of the civil cases that enter the courts involve corporations and private businesses. Corporations can utilize pre-litigation mediation for all non-criminal disputes including contractual and employment disputes. Businesses have the most to gain from the confidentiality of mediation and the potential cost savings associated with the process.

Individuals: The use of pre-litigation mediation by individuals has become more common especially with the growing popularity of employment ADR programs. Additionally, pre-litigation mediation is gaining popularity for divorce settlements and other civil problems (such as neighbor-against-neighbor disputes). While the confidentiality within the mediation process could have a potential negative effect on society and the general public's access to information, on an individual basis the confidentiality of mediation allows for a positive, more creative, less time consuming, and mutually agreed upon resolution.

Costs

The societal costs of pre-litigation mediation must be considered. When a lawsuit is filed with the courts, the dispute becomes a matter of public record and is available to the press, corporate analysts or any other member of the public who might be following court matters. While it can be argued that public record of a lawsuit can be embarrassing, create questions, and potentially hurt future or current relationships, without a public record there is no public discussion about the cause of the lawsuit nor is there discussion over what the outcome might be. This discussion can be important in cases involving questionable business practices. It can be argued that, if a business is allowed to utilize a legal mechanism to avoid public scrutiny, privacy and confidentiality work against the public interest. In September 2000, a controversial article in the *Los Angeles Times* written by Davan Maharaj pointed out numerous companies who have "secretly" settled product liability cases in mediation thus denying the public the right to know about corporate practices and product defects (2000). Maharaj implies that the confidentiality of mediation was the principal reason for this lack of information. The point made in this article is correct; the American people do have a right to know about such complaints (Berman, 2000, ¶ 6).

¹⁰ The court system offers no real ADR option for criminal matters. In some very rare situations, however, the use of Restorative Justice Processes takes place for juvenile and young adult offenders (Flemming, Personnel Correspondence, July 11, 2003).

Another cost is the fact that mediation is reliant upon the good will of the concerned parties. As mediator Michael Shane has pointed out, “The end result is totally up to the parties involved” (1997). As Flemming puts it, “empirical evidence has shown that [some] parties tend to have an ‘overconfidence bias’ as to their side of the case”; he later states that it is also possible for a party’s expectations to be unknowingly low (Personal Correspondence, July 11, 2003). The lack of discovery and depositions in mediation may prove a disadvantage to the mediation process and the parties.

The mediator has no power to impose an outcome on disputing parties. Mediation in any form is not binding on any party unless all parties agree to a specific settlement. One’s right to a trial by court is not waived by agreeing to mediate. Either party may end the mediation process at any time. If any of the parties enter into mediation without a reasonable expectation of settlement, the cost of a pre-litigation mediation could include the time spent preparing and attending the mediation, any cost associated with the mediation (e.g., mediators’ fees, lawyers’ fees, opportunity cost), and in the end the case would simply go to the courts anyway. If a mediation is to be successful, the parties must come together with an understanding of the problems each side faces. Shane points out that if parties do cooperate, “a plethora of ideas can exist to find a resolution [and] a mediation settlement is almost guaranteed” (1997).

Benefits

Pre-litigation mediation has two very important benefits, economic cost reductions and confidentiality. From an economic standpoint, mediation, if conducted prior to filing a formal lawsuit, is a cost-effective form of dispute resolution. Pre-litigation mediation reduces direct costs and indirect costs, saves time, and more than likely helps retain relationships. With regards to confidentiality, as discussed earlier, pre-litigation mediation offers opportunities to utilize a third party mediator’s skills to come to a binding agreement. Confidential information and private situations can be shared and discussed during the process without fear of public disclosure or scrutiny. If pre-litigation mediation fails to bring about an agreement, the mediation process can lead to a case being settled independently before a formal filing. If the case is filed with the courts, the confidentiality of the mediator and the mediation process, having been affirmed by the courts, disallows any discussion of matters discovered during the mediation.

Because of these benefits, mediation has grown as a method of choice to resolve disputes. The growth in mediation is especially evident in matters that can be resolved before a lawsuit is filed, including employment ADR, business-to-business agreements, and many other civil disagreements. The benefits of pre-litigation mediation have been recognized by governmental authorities. For instance, the state of North Carolina has taken advantage of the comparatively quicker resolution time and the confidentiality of pre-litigation mediation by authorizing pre-litigation mediation in the case of farm nuisance disputes and for Y2K disputes (North Carolina, 2000, p. 7).

Legal costs for businesses, governmental institutions and individuals alike have the potential of being burdensome. These costs include direct legal fees, lost labor hours,

destroyed relationships and partnerships, and time lost in the legal process of depositions and court delays. “The costs that are saved by mediation flow from avoidance of costly litigation. Mediation at the courthouse steps doesn't save anywhere near as much because the bulk of the costs have been incurred by that time” (Personal Correspondence, Olivella, 2003).

Resolving a dispute early does not just save direct costs. Because mediation is informal, it preserves long-standing relationships. Pre-litigation mediation's success can be seen in employee retention and in the maintaining of business and personal relationships. For instance, a long-term employee can work through a mediator to achieve an amicable solution to a dispute with his employer, or a business might use mediation to settle a problem with a valued customer. In each case, parties may have been doing business with each other for years. Neither party wants to dissolve the relationship. The result of a successful mediation is an agreement that both parties believe to be fair.

The indirect savings from an amicable resolution through mediation are invaluable. For example, in schools, the potential of lawsuits being filed against teachers adds to the stress shown to be a cause to teachers leaving the profession (Bradley, et al., 2001). “When there is a situation where a parent's feelings need to be heard and a teacher's rebuttal is [essential], confidentiality of the neutral is of the utmost importance. The use of [mediation] for disputes is a real and viable option” (Personal Correspondence, Jack Elrod, March 31, 2002). Mediation can bring schools and parents closer together and help construct positive relationships. It often results in educators and parents reaching an agreement that pleases both parties and helps each party gain a deeper understanding of the other's views — at a fraction of what the overall cost would have been if this dispute were not resolved amicably (Council for Exceptional Children, 1996, ¶3). The parents have to decide if solving a problem amicably is their goal.

Pre-litigation mediation as a means of resolving employment disputes has gained popularity since the United States Supreme Court decided that a mandatory arbitration clause does not preclude the Equal Employment Opportunity Commission (EEOC) from filing a suit against an employer (*EEOC v. Waffle House, Inc*, 2002). Mandatory arbitration clauses were popular in the early 1990's as a way to discourage lawsuits. The thought, at that time, was that if a lawsuit did arise the dispute would at least stay out of the courts.

The new approach is to keep an internal dispute from getting to a point where a suit even needs to be filed — to resolve a problem at its earliest stage. Utilizing a professional mediator to review all the information provided and work with the parties should, in the end, help the parties agree on an amicable and sometimes creative solution. Pre-litigation mediation has proven very successful in employment disputes, since these cases typically involve valued employees who are not looking to

establish blame but rather to resolve a situation and to be heard.¹¹ Mediation can be used to resolve the problem, retain an employee, and avoid having an internal problem escalate to a point where one of the parties believes his only recourse is filing a lawsuit. With costs associated with hiring employees (opportunity costs, training costs, lost time) so high, employment mediation programs are being utilized by many organizations including, UBS PaineWebber, Brown and Root, AAA, and Starwood.

Conclusion

This chapter has illustrated how privacy (confidentiality) can be used as a cost savings vehicle in resolving a dispute. Mediation, in particular pre-litigation mediation, is uniformly recognized as the best opportunity to resolve a dispute (Stong, 2002, p. 5; Olivella, 2003; Glenn, 1993, p. 36). Mediation is an alternative to litigation that “not only saves disputants time and money, but also permits them to work together to settle disputes and remain amicable afterward” (Conrad, pp. 58-59). This amicable outcome is what drives mediation. As Keating has said, “Mediation preserves the privacy of the disputants' concerns during the continuing dispute. If the mediation occurs prior to recourse to the courts, the conflict need never be subjected to public scrutiny at all” (1995, ¶ 19).

With regard to privacy within mediation, the protection of confidentiality is of utmost concern. Confidentiality, which has been challenged by some, is the key to continued use and success of pre-litigation mediation. As shown earlier, the courts in California and the legislature in Texas are examples of how policy professionals can reinforce confidentiality within the mediation process. Other states and the federal government need to reinforce the confidentiality of mediators and of the mediation process through legislation of their own.

Additionally, to answer the critics who say privacy associated with pre-litigation mediation denies the public the right to know, the answer is not the mediation process; rather it again lies with stronger legislation about product disclosure and corporate responsibility. Stronger legislation such as requiring businesses to report complaints against them will help relieve this controversy, not a weaker mediation process (Berman, 2000).

Most legal experts agree that legal costs can be reduced substantially if a problem can be resolved early. In litigation there can be significant direct costs associated with a dispute, including costs associated with attorneys and court costs. Additionally there are indirect costs

¹¹ Employment mediation might follow this typical path. An employee is having a disagreement with her manager. Nothing illegal has taken place, but the employee feels uncomfortable with the manager's attentiveness. The manager has been asked to stop but disregards the request. The employee asks to implement the company's mediation program. The employee wants to keep her job; the company wants to retain both employees; all parties want to keep this incident from reaching the courts, letting this private dispute become public, and incurring unnecessary legal costs. The manager has had a sparkling record with the company. The mediator asks for three-party mediation (employee, manager, corporate decision maker). The flexibility and confidentiality of the mediation process allows the mediator to facilitate an agreement allowing for a mutually agreed upon binding decision.

such as an employee's time, loss of an employee, loss of a customer, loss of a business relationship, or just a loss of faith between parties.

If both parties' goals are to resolve the dispute quickly and avoid high legal costs, mediation provides a means of achieving those goals. "The issue is not whether individual litigants can achieve cost savings by using ADR in specific disputes — the answer to that question is almost certainly yes" (Hensler 1994, ¶ 2).

Jack Elrod, General Counsel for the Dallas (Texas) Independent School District (DISD) believes there are a sizable number of disputes within the DISD that should and could be resolved at an earlier stage than they are. "There is too much litigation and too many lawyers making too much money off of school districts," stated Elrod. "I see hundreds of thousands of dollars going out every couple of months that could be used for teachers and in the schools" (2002).

Table 4.1 illustrates how pre-litigation mediation can reduce litigation costs. Glenn (1993) provides the numbers based on a fictitious case between an accountant and his client. The accountant has mishandled a corporate tax return. He is trying to rectify the situation as fast as possible and is comparing the cost of mediating the case or allowing it to go to litigation. The assumption is that damages will be the same with either option.

Table 4.1

Example of Mediation Savings

Stages of Dispute Resolution	Lawsuit filed in Court	Mediation
Initial consultation	\$3,500	\$3,500
Discovery	\$25,000	\$1,000
Experts before trial	\$5,000	\$3,000
Depositions before trial	\$8,000	\$0
Trial preparation	\$10,000	\$0
Settlement discussions	\$5,000	\$5,000
Trial (three days)	\$15,000	\$0
Post trial (no appeal)	\$2,500	\$0
Cost of disruption to company	\$40,000	\$5,000
Total Resolution Costs	\$114,000	\$17,500

Source: Glenn, 1993, p. 37

The Law Firm of Katz, Kutter, Alderman & Bryant formed a practice area specifically designed to manage pre-litigation mediation cases.¹² According to Mike Olivella, who chairs this section of the firm:

Statistically, one of our clients has documented a reduction in costs amounting to over 70% when comparing claims handled prior to pre-litigation mediation as compared to claims handled in the traditional method. A side benefit is the documented reduction in the amounts paid to resolve the claims, which also exceeds 70%. In the way of hard numbers, prior to 1991, this client spent \$115,000 on average, per claim, on attorney's fees, costs, expenses, verdicts and settlements. Between 1992 and 2000, the average spent by the client to handle the same type and number of claims dropped to approximately \$35,000. That meant \$80,000 less was spent over a 9 year period and almost 1,000 claims were handled during that time frame. If you do the math, the company saved \$80 Million over that time frame (2003).

Numerous businesses, governmental bodies, as well as the courts, have utilized or offered positive opinions about mediation, especially pre-litigation mediation. Each describes the various economic benefits as a reason for their use and positive opinions of mediation, but they also claim confidentiality as the linchpin to mediation's success. Without the free and open discussion encouraged in mediation, there would be no reason to mediate disputes, and the option to resolve disputes in a non-adversarial, solution-finding manner would disappear.¹³

Pre-litigation mediation's opportunity costs need to be as low as possible for claimants. Many pre-litigation mediations revolve around having both parties willing to utilize the confidential aspect of mediation. For instance, in employment mediation, when an employer absorbs the initial costs of mediation, the employee is much more willing to accept the mediation process and is more comfortable discussing the situation surrounding the dispute and accepting the final agreement. If one of the main goals of pre-litigation mediation is retaining relationships, making the process as simple and cost effective for employees, clients, and customers will make achieving that goal more likely.

Organizations such as the American Institute of Architects have suggested that their members include mediation clauses in all contracts. Other industry and trade associations need to encourage their members to incorporate pre-litigation mediation clauses in their

¹² Katz, Kutter, Alderman & Bryant claims to have created and implemented the first national Pre-Litigation Mediation Program in the U. S. in 1991 as a means of cost reduction in claims handling.

¹³ While Keating (1995) describes mediation as a solution-finding method for resolving disputes, the effectiveness of finding that solution is based on the quality of the mediator and the willingness of the parties to resolve the dispute. The success of a pre-litigation mediation is based on the balance between cost and confidentiality. If the confidentiality of mediation weakens too far, the cost would have to drop to a point where the effectiveness of pre-litigation mediation would be diminished and rendered ineffective.

contracts. Organizations should keep the clauses simple, and emphasize privacy and confidentiality. The clauses need to be “customer friendly,” and provide equal participation in choosing the venue and the mediator.

It is clear that pre-litigation mediation saves costs, direct and otherwise. Also clear is how mediation offers privacy protection. In this case, economic factors and privacy concerns work side by side. The confidentiality has no direct cost and legal savings are not due directly to enhanced confidentiality. Yet mediation would not be successful without both confidentiality and cost savings.

This chapter has shown how economics (lower costs, retained relationships, etc.) and privacy (confidentiality and lack of public disclosure) can be reliant on each other to be effective yet be independent in development. The next chapter looks at the economics trade-offs associated with “un-privacy” and the internet.

COPYRIGHT 2003

Summary Matrix (Chapter 4)

Case Study: Pre-litigation Mediation				
	Stakeholder 1	Stakeholder 2	Stakeholder 3	Stakeholder 4
	Defendant (Individuals or Businesses)	Plaintiff (Individuals or Businesses)	The Court System	Society
Privacy Component				
No public disclosure (court papers)	Privacy gained Ability to depose opposition is lost.	Privacy gained Ability to depose opposition is lost.	No effect	Loses knowledge of case development
Confidentiality of mediation	Personal privacy gained.	Personal privacy gained.	No effect	Loses knowledge of case development
Costs	Cost of mediation Lack of knowledge about other parties' past	Cost of mediation Lack of knowledge about other parties' past	- none -	Loss of information Lack of knowledge about past improprieties and business practices
Benefits	Potential for lower legal costs Privacy	Potential for lower legal costs Privacy	Reduces caseload	Less legal expenditures could translate to lower product costs.
Recommendations				
Strengthen confidentiality	Increases privacy Mediation becomes more effective	Increases privacy Mediation becomes more effective	Encourages mediation Helps to reduce caseload	Knowledge of case outcome even less likely
Encourage the use of pre-litigation mediation	Relationship retention, lower legal costs, other economic savings	Relationship retention, lower legal costs, other economic savings	Helps to reduce caseload	Potential for fewer lawsuits going to court Loss of knowledge on contributing issues

Chapter 5. “Un-privacy” and the Internet

Privacy and the internet is one of the most debated privacy topics of today. The internet has been considered the backbone of the new “global economy.” It embodies a technology that while accepted by society is understood by relatively few and therefore causes concern — even fear — regarding its privacy implications.

Kenney et al. define internet commerce as the sale and purchase of products and services over the internet, an industry worth over \$1 trillion (1999, p. 533). The rise of internet commerce has had many positive commercial effects; it has also brought some negative consequences. According to the Center for Democracy and Technology (CDT), “Every day, millions of people receive dozens of unsolicited commercial emails (UCE), known popularly as ‘spam’” (2003, p. 1). Spam is a direct result of information being obtained from internet users (either knowingly or unknowingly) and is considered the “junk mail” of the internet. Once an e-mail address is obtained by a commercial enterprise (primarily or secondarily), a user is potentially subject to spam. Brightmail Inc., an anti-spam software vendor, reports that 41% of e-mail in 2003 will be considered “spam,” up from only 8% in 2001. Brightmail estimates that the average internet user will receive 2,500 spam e-mails in 2003 (Siegel, 2003, ¶ 4). “Some users see spam as a minor annoyance, while others are so overwhelmed with spam that they are forced to switch e-mail addresses” (Center for Democracy and Technology [CDT], p. 1).

Over the course of the last ten years, the internet has become a primary source of information gathering. What is less known is that the internet as a commercial enterprise requires consumers to be willing to give up their privacy. By giving up privacy, they allow businesses to target products and advertising to specific potential customers which as a byproduct may help to reduce the volume of unwanted information and spam (Rubin and Lenard, 2002, p. 11).

Value proposition is a concept frequently used by businesses to characterize “the combination of end-result benefits and price to a prospective customer in purchasing a particular product” (Kenney, p. 533). A customer has the option of choosing the product that offers the best value (the best combination of benefits and price). That value may come from a particular product or from a competing product or even no product at all. Since internet commerce is not a product that one purchases but a means to purchase products, the concept of value proposition becomes the “net value of the benefits and cost of both a product and processes of finding, ordering, and receiving it” (Keeney, 1999, p. 533). When one takes into account the privacy (lack of privacy or “un-privacy”) associated with the internet, one could argue that Keeney stops short of a complete definition of value proposition with regard to internet commerce. Internet commerce includes not just “finding, ordering, and receiving the good or service,” but understanding what amount of privacy is being given up during the transaction.

The internet seems to offer endless opportunity for information gathering and commerce. Commercial and non-profit organizations collect information about users who access their materials through their Web sites. These organizations may collect this

information for any number of reasons, including to raise funds, to track users for demographic studies, “to discover more about users so that they will be able to tailor or improve their offerings; to survey for research or polling purposes consumer preferences, attitudes, or habits; [or] to offer products or services to those most likely to be interested in them” (Smith, 1996, ¶ 13). When a user enters a Web site, that users’ actions can be followed and documented. Many of these users understand that internet use can be tracked, but is allowing an online merchant to have one’s address along with the potential to sell that information worth the convenience of shopping online? The internet relies on that answer being yes.

Un-privacy of the Internet

“While there is widespread agreement that digital technologies pose serious threats to privacy” (Doty, 2001, p. 179), Consumer Alert, a non-profit consumer group, points out that “just about every interaction with a person face to face or through technical means involves some loss of anonymity” (Smith, ¶ 7). The internet thrives on users’ divulging personal information (either willingly or inadvertently) and their willingness to allow information to be gathered about them. The information divulged could be an e-mail address, a log-on name (to track users of a Web site), or even a credit card number. All this information is then readily available to be used by the holder to improve its own enterprise or be sold to a third party.

“The real tension in the current privacy debate isn’t between consumers and businesses, but rather between consumers’ desire for greater privacy and their desire for the many benefits that flow from readily available personal information [targeted information]” (Online Privacy Alliance, 2003, ¶ 3). “The right not to be annoyed” and the “right to be left alone” as definitions of privacy feed into this conundrum, since consumers want to be targeted yet they do not feel as though they are being targeted adequately (Keeney; Acquisti et al., 2003; Goss, 1995; Siegel, 2003).

In our daily lives numerous choices are made. If a product or a place is disliked, it is avoided or ignored. Currently, the phone book does not keep track of how many times you search for a pizza parlor or a sporting goods store. The local shopping mall does not keep data on which shop windows you peeked into at Christmas. The mailman does not log all mail he delivers. But the internet does. When someone logs on to the internet, she is subject to having all her choices tracked electronically.

To receive all the benefits of internet commerce, consumers must tolerate personal information about themselves being collected and maintained. Yet even though consumers have tolerated these practices, they have done so with the understanding that the information will be used selectively and that they will not be inundated by such annoyances as spam. When spam instead increases, some consumers react by divulging even more information again with the hopes of becoming better targeted. They have already divulged private information, such as e-mail addresses, browsing preferences, and purchasing tendencies, and they are prepared to divulge more. On the other hand, privacy is such a concern of internet consumers that, according numerous sources such as the Electronic Privacy Information Center, each year “privacy fears” result in billions of dollars in sales lost (Acquisti, 2002, p.

1). Are those fears warranted, or is giving up some privacy simply a cost of doing business over the internet?

Important Stakeholder Groups

Individuals: Individuals who use the internet concerns are the most likely group to be affected by privacy concerns. It is an individual's choice to provide information to businesses, it is his choice to allow imbedded programs (cookies) to remain on his computer, and he who decides if he wants to opt-in or opt-out of an internet business' database. It is also the individual who gets the "spam," gets the targeted advertisements, and has personal information sold to third parties.

Private Business: Private business is reliant on individuals' either being willing to divulge information or being naïve about the internet so the business can collect and retain as much information as possible. An organization involved in internet commerce needs their customers to accept un-privacy in order for the business to target advertising and products, and to have a reliable data base to sell to other businesses. Businesses looking at the long-term also find that it is in their best interest to meet their customers' requests; which frequently has been to have information removed from data bases.

Costs

Businesses have always found ways to use private and personal information provided by customers. Keeney measures privacy with regard to internet commerce as "the number of lists your name is added to without your approval or the number of data banks obtaining unauthorized information about you" (1999, p. 538). Information about consumers maintained by a business is supposedly from a specific consumer using a specific computer. In actuality the information is gained from a specific computer or a specific registration name that may be used by a single or multiple users (Rubin and Lenard, 2002, p 16). The specific usage habits reflected by one "computer" could actually be the habits of multiple individuals.

So how reliable is the information accumulated by internet businesses? With advertising being such a large source of revenue for Web sites, it is very important that the information collected be acceptable so targeted messages can be sent or advertisements can be inserted. Rubin and Lenard talk about how consumer profiles are developed by internet advertisers by "tracking an individual's online activities and applying database technology and statistical models that yield demographic and interest profiles" (p. 16). As one person's information gets on more lists, the possibility of her being annoyed increases, as does the possibility of her being improperly targeted. Recently, government pressure has given consumers more control over their own information (Siegel, 2003; Goss, 1995, p. 178). Unfortunately, while businesses are giving their customers control, it is being done reluctantly and in many cases the process is made as difficult as possible. "In fact, [in numerous cases] many companies all but frustrate their customers' attempts to exercise that control" (Schwartz, 2002b, ¶1).

In “Guarding Privacy: Tricky Task for Consumers,” Schwartz offers examples of how customers have to go through time-consuming and tedious steps traversing a Web site to find where they can express their desires to not have their information stored, used or sold (2002b). Organizations conducting business over the internet, while offering their customers the option of keeping information “private,” are counting on the process being so burdensome, that for many, controlling information about oneself will not be worth the trouble or frustration.

Benefits

The growth of the internet has offered consumers an additional option to make purchases or to simply gather information. The problem is businesses have no clear idea who is considering the purchase. When one goes to a physical store, a merchant can study the customer’s demeanor, ask questions, direct him to products and simply offer good service. The internet does not offer the same flexibility of knowing a customer. So internet merchants need an alternative means of targeting and directing customers. This need to target customers is one of the main reasons business utilize internet tracking systems.

Chris Wolf, one of the country's leading practitioners in internet and high tech law and in internet privacy, remarked that commercial use of the internet is reliant on relaxed privacy concerns. The internet relies on cookies and “other general data that if they did not exist would make the speed of utilizing the internet much slower” (Personal Correspondence, December 11, 2002). The benefits of better information outweigh the costs by protecting the efficiency of internet commerce. Regulation on information gathering would impose unnecessary costs (Rubin and Lenard, 2002, p. 80). Balancing the information needs of internet commerce with the privacy interests sought by consumers has posed questions for internet businesses but is proving beneficial to both parties.

The ability to communicate electronically has led to a major reduction in the cost of information. With that reduced cost, a greater amount of information has become available to stimulate and drive the economy, in particular through internet commerce (Rubin and Lenard, xiv). Samarajiva has written that the “emerging economy places great weight on relationships - within the production chain, and between producers and customers. Reliance on one-time transactions is superseded by ongoing relationships” (1998, p. 279). The nature of internet commerce is such that, internet businesses must be able to gather information about their customers.

Many internet businesses make it difficult for consumers to choose not to have their information included in databases or to avoid being tracked. In fact, the Federal Trade Commission reports that many internet businesses utilize hidden means to obtain or distribute information (Federal Trade Commission, 2000). According to the Center for Democracy and Technology, even while these hidden measures are used, the majority of businesses will remove a customer’s information upon request (CDT, 2003). Once a user has taken the time and effort to remove his contact information, businesses consistently respect the user’s request. While there are some exceptions, “for the majority of Web sites we encountered no difficulty and found that ‘opt-outs’ were respected” (CDT, p. 11). The incentive for

maintaining good relations with customers and potential customers and to make removal easy is proving to be good business practice leading to greater appreciation and utilization of those businesses. Rubin and Lenard point out that there are numerous examples of the “market disciplining firms that have violated consumers’ preferences with respect to privacy” including: AOL canceling plans to sell its subscribers telephone numbers and RealNetworks changing software found to be information collecting (2002, p. 42-43).

Conclusion

Internet commerce relies on un-privacy, or the release of information by the user of services. Responsible companies have a real interest in meeting their customers’ needs, especially when a legitimate company’s goal is to exist and be profitable on a long-term basis. These “responsible” organizations are extremely sensitive to their customers’ concerns about privacy and information use (Smith, 2003, ¶ 25), but in the end internet businesses need their customers to willingly allow the use of their information. Diffie and Landau note:

The capacity to build databases and feed them the details of every credit-card transaction exists, and the result is an excruciatingly detailed portrait of the shopping, traveling, and trysting habits of hundreds of millions of people. Yet, since such databases are an essential component of today’s commerce... it seems realistic to accept them. The best we can do is regulate their use in a way that protects individual privacy (1999, p. 239).

As society becomes more computerized, privacy is becoming harder to safeguard. And as Singletary observes, “things are only going to get worse as private business and government agencies build bigger databases that store more information on consumers” (2002, ¶ 12). He further observes that the fact that the internet economy thrives on un-privacy ought to be of concern. “We should be concerned about how easy it is to gain access to our personal data. Today, our financial information is passed around like a bad cold” (¶ 4). As stated previously, many internet businesses utilize hidden measures to collect and distribute personal information, but when a customer requests, most respect their customers’ wishes.

If Not Opt-In Then at Least Opt-Out

The idea that databases and such can be “regulated in a way that protects individual privacy” and allow a business to focus on the long-term raises an interesting policy dilemma. The most desirable option from a consumer’s point of view would be the “opt-in” measure (equivalent to being asked to have personal information included in a database), deciding before the fact if personal information can be collected and held by a business. As noted earlier, internet commerce relies on information in order to thrive. Making information difficult to obtain will generally limit the success of internet commerce. While opt-in measures are the best for privacy protection and assisting with one’s “right to be left alone,” opt-in measures constrain internet businesses’ need for information. With opt-in, only information customers are willing to divulge is available to these businesses. Rubin and Lenard report that consumers are less willing to provide information through opt-in thus “reduce[ing] the amount of information available to the economy” (2002, p.72). Furthermore,

as Cate suggests, a recent court decision has implied that governments forcing a business to require “opt-in” measures through legislation may be unconstitutional (2001, p. 39).

Recognizing the needs of internet businesses, opt-in is not a viable option. The use of an easily accessible “opt-out” measure (asking for the removal of one’s personal information from a database) would prove to be beneficial for all parties. Many businesses are providing an option to “opt-out” grudgingly since providing such an option on a Web site or on a data collection site goes against internet commerce’s desire to retain information. Many businesses have offered the opt-out option in fine print or after a litany of Web pages and searches. While it is true that “fine print opt-out measures” are used, they are not the best alternative (Goss, 1995; Liptak, 2002). Using hidden opt-out measures does not allow customers to achieve an understanding of the relevant facts and risks (informed consent) associated with the choice of disclosing or not disclosing information (Goss, p. 179). Easily recognized opt-out measures offer the opportunity for businesses to be customer friendly and still allow them to obtain a sizable amount of information. Since much information given in conventional commercial transactions is done so voluntarily, providing an opportunity for a customer to opt out of providing information does not put the e-commerce business at a disadvantage. As Alderman and Kennedy put it, “You cannot opt out of the digital world, but you may be able to opt out of a piece of it” (1995, p. 328). Legislation mandating easily recognized opt-out measures would help businesses that utilize internet commerce to gain the trust of users and still allow responsible businesses manage information enabling them to prosper. It can be argued that easily recognized opt-out measures allow information to be collected first thus giving more power to businesses and undermining consumers’ privacy. Rubin and Lenard argue that easily accessible opt-out choices benefit both business and consumers. Businesses can get information but consumers still have the “initial property right” allowing them to choose to opt-out or simply avoiding the business altogether (p. 74).

Buyers who are worried about disclosing too much information over the internet can take defensive measures. One can use aliases, avoid Web sites that do not guarantee anonymity, and install blocking software (Smith, 2003, ¶ 9). “In short, with today’s technology, sellers can post prices, observe choices, and condition future prices on observed behavior. But buyers can also hide the fact that they bought previously” (Acquisti and Varian, 2002, p. 3).

Interestingly enough, the internet is being used more each year for transactions and purchases, and in some cases internet businesses are doing more business than conventional stores (Keeney 1999; Acquisti and Varian). While consumers’ willingness to engage in business exchanges online has been influenced by concerns about the privacy of personal information, more consumers are utilizing the internet, confident that information about their financial transactions is secure or at least under their control (Conference Board, 2003, ¶ 5).

Privacy and internet commerce is so integrated that to conduct business through the internet requires the disclosure of personal information. While information is provided in all commercial transactions, internet commerce provides a means for businesses to collect information about consumers’ preferences, to target products, or send spam. The next chapter

covers a Section 215 of the USA PATRIOT Act, a complicated privacy dilemma brought about by the terrorist attacks of September 11, 2001.

Matrix (Summary for Chapter 5)

Case Study: “Un-privacy” and the Internet			
	Stakeholder 1	Stakeholder 2	Stakeholder 3
	Individuals	Private Businesses	Society
Privacy Component			
Disclosing personal information	Give up privacy	Gain knowledge of customer	New economic opportunities and conveniences
Costs	Possibility of being annoyed	Annoyed customers could do business elsewhere	Frustrating procedures to keep personal information private
Benefits	Success of internet commerce means more options for goods and services Un-privacy allows for better targeted information and less spam	Economical target marketing and product inventory	Fewer unwanted goods and services
Recommendations			
Highly visible opt-out measure	Increases personal privacy Reduces amount of undesired use of information by businesses	Reduces amount of information available on specific customers Helps establish good customer relations	Potential for unneeded goods and services

Chapter 6. USA PATRIOT Act, Section 215

The terrorist attacks on September 11, 2001¹⁴ will long be discussed. In the aftermath of the attacks, the 2001 USA PATRIOT Act was passed by Congress and signed into law by President George W. Bush.¹⁵ The USA PATRIOT Act is a result of the public safety and national security concerns that arose after the attacks, and has had substantial privacy concerns associated with it. This chapter specifically looks at one section of the Act, Section 215 and illustrates how one's perceived privacy can be fragile. The privacy concerns associated with Section 215 have been amplified by the fears associated with a terror threat and the resulting legislation. These short-term economic implications associated with these concerns may be peripheral, however, in the long-run Section 215 could present economic consequences if not monitored carefully.

The economic impact of the attacks, regardless of the state of the economy of New York or even the United States at the time, has been large (Bernstein, 2003; New York City Partnership, 2001; The Economist.com, 2002). What made the terrorist attacks so frustrating to United States authorities is that there were opportunities for these attacks to have been prevented during their planning.

The United States government has vowed to stop such an attack from occurring again. Riding a sense of disbelief and renewed patriotism, the lawmakers in Washington took the first step in the months following September 11th. Congress' answer, at the prodding of President George W. Bush's administration, was the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, better known as the USA PATRIOT Act (PL 107-56, 115 Stat 272 (2001)). "The Act strengthens an array of existing law enforcement statutes... and adopts many new counter terrorism measures... however, the Act is not a model of legislative clarity" (Kenney et al., 2001, p. 1)

¹⁴ On September 11, 2001 a group of terrorists residing within the borders of the United States, caused death and destruction not seen by the contiguous 48 states in almost 150 years. In the end, 3,000 people were reported or confirmed dead, millions of square feet of office space lay in ruins, four airplanes were obliterated, and symbols of American strength were partially (the Pentagon) or fully (the World Trade Center) destroyed.

¹⁵ The USA PATRIOT Act was passed by Congress without any debate. The Act was considered one in a long line of legislation that U.S. presidents have attempted to get through Congress giving more power to the executive branch of government. It has been argued during a Symposium on Information and the War on Terrorism (April 11-12, 2003) at the LBJ School of Public Affairs that the USA PATRIOT Act is more concerned about investigating suspects than protecting citizens. The terror attacks scared America and many citizens are willing to give up rights especially rights to privacy as a need to keep the economic and societal disasters of September 11 from occurring again. Many argue that the Act is a breach of the Constitution and only time will prove these protesters right or misled. This chapter does not discuss all the privacy concerns but rather how economic factors could be included or discounted from the specific privacy arguments.

When the USA PATRIOT Act was signed, just six weeks after the September 11th attacks, members of Congress and all of Washington D.C. had just been affected by an anthrax scare and were warned of more terror attacks. Congress was fearful of being labeled disloyal (Levy, 2003, ¶ 3); the House passed the bill 357 to 66, while the Senate did the same 99 to 1. Passage of the act was considered prudent by many, while others considered this new weapon against terrorism a capitulation to the Bush Administration (Chang, 2001). In either case, the USA PATRIOT Act was passed with little debate.

Among the provisions of the Act that have stood out as controversial is Title II Section 215 of the Act (see Appendix C). While Section 215 seems innocent enough, the controversy surrounding Section 215 is understandable especially due to the vagueness and breadth with which the section is written. For example, subsection 501(a)(1) gives the Federal Bureau of Investigation (F.B.I.) authority to retrieve any records that might be connected to a terrorist investigation. In essence the F.B.I. can review business records of people under suspicion, including the borrowing or purchase of books and the use of the internet at libraries and bookstores (Murphy, 2003, ¶ 8). Many have considered Section 215 to be an intrusion into their privacy by the government and an economic strain on establishments such as libraries and bookstores.

Privacy and Section 215

Title II Section 215 Subsection 501 (a)(1) of the Act reads that an agent:

[M]ay make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

Additionally, Section 215 “Overrides state confidentiality laws protecting library records” (American Library Association, p. 1) “Even before the ink on the president’s signature had dried, the F.B.I. began to take full advantage of the new search-and-seizure provisions” (O’Meara, 2001, ¶11). Libraries are required to disclose their circulation records as well as all registration records when law enforcement presents proper documentation.¹⁶ The idea of disclosing such information about patrons has been shunned by such organizations as the American Library Association (ALA) and the American Civil Liberties Union (ACLU), as well as bookstore owners.

¹⁶ According to the official summary of the USA PATRIOT Act, Section 215 “Authorizes the Director of the FBI (or designee) to apply for a court order requiring production of certain business records for foreign intelligence and international terrorism investigations. Requires the Attorney General to report to the House and Senate Intelligence and Judiciary Committees semi-annually” (USA PATRIOT Act of 2001, PL 107-56, 115Stat 272).

The passage of the USA PATRIOT Act happened quickly. Some argue that the Act was hastily put together and that the Act gave the F.B.I. and other intelligence agencies too much authority. Some might argue that, in a war, in particular a war on terrorism, swift investigations are imperative; some liberties have to be sacrificed. The United States Department of Justice (DOJ) asked for Section 215's provision strictly to expedite their investigations. The DOJ argued:

The "business records" section of FISA (50 U.S.C. §§ 1861 and 1862) [which the USA PATRIOT Act modifies] requires a formal pleading to the Court and the signature of a FISA judge (or magistrate). In practice, this makes the authority unavailable for most investigative contexts. The time and difficulty involved in getting such pleadings before the Court usually outweighs the importance of the business records sought (Congressional Research Service [CRS], 2002, p. 22).

While there is legal controversy over the USA PATRIOT Act, there is not nearly as much controversy from the general public. After the attacks, public opposition to greater government surveillance has been muted. "The answer, it appears, is that many people believe the government will invade only someone else's privacy. Privacy for me, they seem to be saying, but not for thee" (Liptak, 2002, ¶ 8).

Important Stakeholder Groups

Government: Section 215 has made it easier for governmental agencies to investigate individuals believed to be a threat to society. More importantly, Section 215 is a tool available to keep another terrorist attack from occurring.

Organizations (such as private, for-profit bookstores and government-supported libraries): Some claim that Section 215 has a direct economic effect on their business by keeping patrons away for fear of disclosure of their purchasing habits. Many bookstores, libraries and such businesses believe Section 215 gives them no choice but to delete customer records as soon as possible.

Individuals: Section 215 probably has the largest direct effect on individuals. Investigations of individuals are easier for law enforcement. Individual's circulation and purchasing records can be examined. Additionally, if an investigation takes place, one is not allowed to reveal this fact and thusly one may not know they are being investigated.

Law Enforcement: Section 215 gives law enforcement agencies, especially federal law enforcement agencies, greater latitude to investigate potential terrorist suspects and do so in secret.

Costs

Based on Section 215, the F.B.I. can request a subpoena if there is no probable cause. "Agents need only convince a judge that their investigation is related to national security or terrorism." There does not need to be proof that a crime has been committed. A judge or

magistrate can be presented with the “evidence,” and a warrant is issued (Marvel, 2002, ¶ 4). The implications of the USA PATRIOT Act were felt immediately. In Illinois, estimates show that, under the stipulations of the Act, law enforcement officials contacted 200 libraries in the months following September 11th (¶ 31).

While the potential for an investigation by law enforcement is a privacy concern and has proven to be contentious for many, an even more controversial area within Section 215 is subsection 501(d). This provision makes it illegal to discuss searches, even with those persons whose records are the subject of the subpoena (Schabner, 2003, ¶ 6). Many have described subsection 501(d) as an attack on the First Amendment to the Constitution (freedom of speech). While it is true that there has to be some sort of criminal activity before the F.B.I. can investigate someone and apply this provision, even Viet Dinh, Assistant Attorney General for Legal Policy, admits there needs to be unease about the loss of some First Amendment rights (Marvel, ¶ 19).

An argument can be made that the consequences of Section 215 need not be measured in terms of direct costs, but rather in the fact that historical data are now being shredded, the freedom to “browse” in a library has been hindered, and that a patron’s circulation records could be scrutinized in secret. Additionally, since its inception, a handful of states and over one hundred cities have found the Act so worrisome that they have adopted resolutions critical of the Act. In each case they have cited the “threat of the FBI rummaging through library and bookstore records” (Clymer, 2003, ¶ 7).

Benefits

Over time, if another September 11th never occurs, the controversy surrounding the USA PATRIOT Act will likely subside; part of the argument will be that the Act worked. As stated earlier, the economic effects from the attacks have been large. “The September 11th attacks killed thousands and irrevocably damaged the lives of thousands more. But the American economy is too large, and resilient, to be thrown off course even by such shocking and tragic events. It is impossible to quantify exactly the effects of the attacks” (The Economist.com, 2002, ¶ 14). To give an example of the attack’s economic impact, the New York City Partnership and Chamber of Commerce gave the following examples in their November 2001 report:

- **JOB LOSSES:** The report estimates that New York has lost 100,000 jobs, but will regain some 20,000 jobs during 2002;
- **TOURISM:** Statewide, the already cooling tourism sector was deeply wounded by the attack, resulting in 46,500 job losses, including 19,700 upstate;
- New York City is expected to lose more than \$4.6 billion in tourism spending through 2003.

Additionally, whether people agree or disagree with Section 215, Congress is charged with monitoring the effects of the section and, in the end, deciding if its renewal is worthwhile or

not. Congress must review the effects if for no other reason than the fact that there is a sunset provision attached to Section 215, as with many of the most controversial provisions of the USA PATRIOT Act. Especially in a crisis, and again with controversial legislation, adding a sunset clause allows Congress to choose whether a section is worth extending or making permanent. In the case of the USA PATRIOT Act, the sunset clauses are perhaps the best known of the Act's safeguards. Under the direction of Section 224 of the Act, many of the law enforcement and foreign intelligence authorities granted by the Act expire December 31, 2005 (CRS, 2002, p.13).

Further, Dinh goes on to reemphasize the fact that Section 215 "does not authorize fishing expeditions." For Section 215 provisions to be used there must be some other evidence linking the person to the crime of terrorism (Marvel, 2002, p. 2).

Conclusion

Section 215 of the USA PATRIOT Act is controversial and raises concerns about privacy. While economic consequences were not considered in the initial public policy debate surrounding Section 215, both economic and privacy concerns have arisen since the passage of the Act. The economic concerns are as glaring as the two towers missing from the New York skyline or as obscure as the cost of signs posted at libraries warning patrons about the Act. The privacy concerns of Section 215 are apparent but are not a cause of great concern in the short term.

While the DOJ admits to limited use of the powers given it by Section 215 (Brown, 2003), the controversy surrounding Section 215's provision allowing review of business records is somewhat perplexing. Librarians and patrons can and do voluntarily report suspicious activity with or without the USA PATRIOT Act. In fact, librarians or bookstore workers have always been required to turn over borrowing, browsing, or purchasing records to the F.B.I. when properly requested. Clymer points out that, while the states and localities that have adopted resolutions against the Act cite library record privacy as a reason, "there is scant, or no, evidence" that the F.B.I. rummages through library and bookstore records (2003, ¶ 7). Librarians are not being required to act as spies or report suspicious activities. There is no new privacy issue and consumers should not be concerned that their privacy is at risk. "Most libraries systematically destroy borrowing records as soon as a book is returned. One way to avoid scrutiny... is to return all borrowed books promptly" (Marvel, ¶ 35). The destroying of records by a librarian is not breaking the law and would be considered illegal only if a subpoena has been issued for those documents (Murphy, 2003, ¶ 16). When purchasing a book, a consumer can avoid a record of a purchase by paying in cash. Likewise, a bookstore owner can avoid record keeping of sales by avoiding credit card or check transactions. As Dr. Philip Doty suggested at a forum on information, records are being destroyed so as to avoid having available what law enforcement might scrutinize. "You can not provide what you do not have" (Personal Correspondence, April 12, 2003).

One must remember that, while the ALA and bookstore owners and the like are all objecting to Section 215, there is no specific clause or wording that specifically targets libraries, stores, or any one entity. Prior to the Act, all states had some sort of subpoena

provision allowing records to be reviewed under specific conditions. Grand juries have always had the power to “issue subpoenas to all manner of businesses, including libraries and bookstores” (Brown, 2003, p. 1). Federal law enforcement officers were allowed to seek a court order for access to certain car rental, storage, and hotel accommodation records. The Justice Department asked that the authority be replaced with permission to issue administrative subpoenas for any tangible item regardless of the business (if any) of the custodian (CRS, 2002, p. 21).

While some may argue that there is no loss of privacy, there is a genuine fear of the USA PATRIOT Act and Section 215 by others who perceive a privacy problem. The costs associated with this perceived fear legitimately raise several policy questions for consideration.

“Millions of dollars have been lost investigating the innocent when this money could be used better to investigate and prosecute the guilty” (Personal Correspondence, Doty, 2003). Whether one believes Doty’s statement regarding law enforcement and the use of provisions in Section 215 is overstated or correct, his point does raise policy concerns. Congress needs to scrutinize Sections 215 if for no other reason than to ensure that the limited resources of law enforcement are being used efficiently. To be prudent, Congress must request independent reports by oversight bodies such as the General Accounting Office (GAO) on a periodic schedule.

Much discussion has been generated about Section 215. Judiciously, either as a safeguard or standard procedure, Congress did incorporate a method for future debate. A sunset clause was incorporated to include many of the more controversial sections of the Act including Section 215 (USA PATRIOT Act, Section 224a). As mentioned, the sunset clause allows the section to expire on December 31, 2005 unless specifically renewed. When asked if Section 215 should cause the concerns that have been generated, Nathan Sales, DOJ – Office of Legal Policy, stated, “You shouldn’t be worried... in fact the USA PATRIOT Act is more protective of civil rights” (Personal Correspondence, April 16, 2003).¹⁷ While Mr. Sales claims concerns are unwarranted, critics of the act strongly disagree with his statement that that civil rights are more protected.

In June of 2002 and May of 2003, the House Judiciary Committee sent a letter to U.S. Attorney General John Ashcroft asking a number of detailed questions regarding the implementation of the USA PATRIOT Act (Sensenbrenner, 2002; 2003). In these letters, among other areas of concern, Chairman James Sensenbrenner wanted to know how many

¹⁷ At a Town Hall Symposium entitled “Unexpected Vulnerabilities of Homeland Security: Civil Liberties vs National Security,” the panel was asked to explain the concern over library use, book purchases, and the like. Nathan Sales, DOJ, answered that one need not be worried and that the power to request the same documents has always been available through a federal Grand Jury. Michael Linz, ACLU, responded that in the past “probable cause was needed, now law enforcement simply certifies to the court” that there seems to be a credible threat. Sales responded: “There is Congressional oversight and secrecy requirements have existed for decades. Investigations depend on secrecy.” To which Linz replied, “Well with Congressional oversight [why should we be worried] (sic).”

subpoenas the Justice Department has issued for bookstores, libraries and newspapers under Section 215. Additionally, the 2002 letter asked if the sunset clause, Section 224, “hampered the DOJ in its efforts against terrorism or any other criminal or intelligence investigation” (Sensenbrenner, 2002, ¶11-12, 19).

Both Sales’ comments and Sensenbrenner’s questions illustrate the importance of debate. With the argument that there was no initial debate concerning the Act, a sunset clause will ensure future deliberation.

The sunset provisions of the USA PATRIOT Act were included to give Congress the opportunity to conduct analysis of the Act. Additionally, sunset provisions are incorporated to allow the adjustment or elimination of a law as deemed necessary by time. Such a time, might be as far off as when the threat from terrorism no longer exists or as soon as Congress and the administration decide to change the law. A sunset provision allows Congress, the Justice Department and lobbyists on all sides of the debate to scrutinize the Act and its effects up to the sunset date. This debate is proper and correct, allowing for analysis from policy, equity, socio-economic, direct and indirect cost, and criminal perspectives. Unfortunately, the sunset measures of the Act are under attack. There has been legislation proposed in Congress, such as the “Domestic Security Enhancement Act of 2003,” that would eliminate sunset provisions (Electronic Frontier Foundation, 2003). Whatever the debate surrounding the USA PATRIOT Act might be, the Linz/Sales conversation illustrated earlier demonstrate that there is controversy surrounding the Act and the section in question. These sunset provisions must not be circumvented but rather they should be reinforced.

Some have asked whether the implications of the USA PATRIOT Act and especially Section 215 will be positive or negative on information services or publicly funded entities. As mentioned previously, there is no clause that specifically mentions information-gathering places (i.e., libraries) in the Act. Could the Act be expanded to have financial ramifications for non-compliance? Yes, but that was the case even before September 11th. Could there be a backlash against libraries because of the Act? Not likely in the short-term, but the long term might alter the way people do business or libraries keep records. In fact, the strategy for libraries is to “keep as little historical information as possible” (Murphy, 2003, ¶ 6).

Are there any economic effects of Section 215? A brief look at the impact of Section 215 shows there is no noticeable short-term economic impact associated with this privacy concern. If more people return books on-time, specifically to avoid law enforcement scrutiny or having a record on file longer than necessary, one might see a reduction in revenue from late fees paid to libraries by patrons. As was suggested, most libraries do not maintain records on books once they have been returned. Also bookstores might see a growth in cash payments so there would be no record of a purchase. In the long-run however, libraries and bookstores will face higher costs associated with training their employees on proper procedures and there is the potential for customers succumb to their fears of Section 215 and just not utilize a bookstore or library.

The economic impact from September 11th can not be diminished nor can the fact that, as of yet, there has been no immediate reduction to privacy. The key is the sunset provisions; when the threat of attack is reduced or privacy is clearly lost, Congress can simply refuse to renew the provisions in the Act. Even if it is proven that there is a reduction in privacy, this

privacy loss is arguably small in comparison to larger need to prevent another terror attack. If another act of terror happens, the privacy reductions perceived in the USA PATRIOT Act could pale in comparison to what may come next.

With the USA PATRIOT Act, in particular Section 215, economic trade-offs with privacy are found in the economic consequences associated with the attacks of September 11th and in the cost to ease the fears of “librarians and bookstore customers”. In the next chapter, privacy of “semi-public” information is analyzed and the responsibility of government agencies to protect a perceived privacy of its constituents is addressed.

COPYRIGHT 2003

Summary Matrix (Chapter 6)

Case Study: Section 215 of the USA PATRIOT Act					
	Stakeholder 1	Stakeholder 2	Stakeholder 3	Stakeholder 4	Stakeholder 5
	Government	Individuals	Law Enforcement	Organizations (private businesses and libraries)	Society
Privacy Component					
Law enforcement's ability to look at use records of individuals	Gain knowledge	Access to information unchanged Potential loss of privacy in criminal proceedings	No change	No Change	Perceived loss of privacy
Unlawful to disclose if records are viewed by law enforcement	Gains absolute secrecy	Lack of knowledge of being investigated	Ability to investigate without disclosure	Loss of trust	Perceived loss of privacy
Costs	Trust in government	Perceived loss of privacy Less personal service with the loss of "purchasing" records	Trust	Less data kept on purchasing habits; more cash transactions	Freedom to gather information
Benefits	Lowers risk of terror attack; freedom to investigate terrorists	Security	Fewer restrictions in gathering information on suspects	Security	Reduced likelihood of terrorist attacks
Recommendations					
Maintain and reinforce sunset clause	Allows for debate; law refinement	Allows Debate	Potential to refine law to better meet needs	Allows debate and law refinement	Potential to refine law to better meet needs
Financial oversight	Reduces waste and abuse	Allows debate	Restricts abuse	Allows for debate	Allows debate and restricts abuse

Chapter 7. “Semi-public” Information

Citizens entrust the government to protect them from unwanted intrusion. The privacy concern related to “semi-public” information is derived from that trust. When government collects information, is it obligated to distribute that information freely, to withhold it, or to divulge pieces of information as needed and only under specific circumstances? “Semi-public” information refers to information collected by the government that traditionally has been available only under specific guidelines and circumstances. The benefit of information being “semi-public” is the relative privacy it offers to citizenry. With new technologies available for data storage and dispersion, maintaining the economic and societal stability associated with information being semi-public has raised privacy concerns.

In 1977, the State of Texas looked carefully at the privacy of public records. The Texas Advisory Commission on Intergovernmental Relations wrote, “Privacy and disclosure issues have become important concerns of government at all levels in recent years as government files have expanded and much more information has become accessible through new electronic equipment” (1977, foreword). Today that same concern has been multiplied exponentially as government increasingly conducts its business — the public’s business — electronically.

In 2001, the Office of the Attorney General of Texas issued a report identifying over “700 statutes that deem certain information as private or confidential. These laws not only restrict certain information from being shared but also outline conditions under which information can be disclosed” (Lyndon B. Johnson School of Public Affairs [LBJ-PRP], 2003, p. 6). But even with such laws and restrictions, the State of Texas still sells personal information.

The issues facing Texas are similar to those throughout the nation. Information provided to governmental entities is being stored and released. Every government entity collects information about its constituents, those it regulates and protects, or simply the territory it oversees. This information can be collected through a Constitutional mandate such as the United States Census or from tax collection records maintained at a local level. Regardless of the means of collection or the reason for collecting information, the growth in the practice of collecting data by governmental agencies “raises privacy concerns about what information is collected, how it is used, and who has access to it” (LBJ-PRP, p. 77).

The U.S. Census collects information largely from questionnaires sent out every ten years. The questionnaires help determine population, household information, and, through interpretation of the responses, a reliable estimate of trends and general information about a locality or portion of that locality (census tract). While the Census Bureau does not release

census data on individuals, census tracts and census blocks can be so specific as to easily determine an individual's personal data within that tract or block.¹⁸

The need to collect information has led to better targeting of services by governmental agencies, and to a business tactic known as geodemographics. Geodemographics¹⁹ is the targeting of individuals or groups based upon where they live (demographics) and their societal tendencies of those being targeted (psychographics). According to Goss, geodemographics is possible only because of the "administrative geographies of the U.S. Bureau of the Census, Postal Service, and various media monopolies, and the increasing complementarity in function between public and private bureaucracies" (1995, p. 194).

Individuals are often surprised to learn exactly how many databases their names are in, and that "many details of an individual's life, activities, and personal

¹⁸ For instance Block 4005, Block Group 4, Census Tract 9611, Hill County, Texas is reported by the Census Bureau to have a population of two (2) in one (1) household; both people are classified as "white"; 1 male 67-69 years old and 1 female age 65-66.

¹⁹ Geodemographics is described by Jon Goss as an information technology that enables marketers to predict behavioral responses of consumers based on statistical models of identity and residential location. It is also used by retailers for site locations and media planning, non-profits for fund raising, and political campaigns. Geodemographics is based on a detailed knowledge of consumers' behavior obtained through systematic surveillance of social life, the elaboration of reductionist models of consumers' identity, and the inference of unobserved behavior from residential location.

characteristics can be found scattered throughout the files of governmental agencies” (LBJ-PRP, p. 77). Examples of personal information available from public records are in Table 7.1.

As discussed earlier in this report, Miller’s point that each individual is entitled to reasonable control over information collection and use by government is evident in the trust ensured to public officials. The public believes that information about them will be used in their best interests and the best interests of society (Mitra, 2001, p. 8); this belief is the backbone of information accessibility.

Table 7.1

Potential Sources of Personal Information from Public Records

Source	Information
Driver’s license	Address, sex, height, weight, date of birth, Social Security number, vision correction, selected medical conditions
Other licenses	Selected occupations (such as medical, professional, insurance agent) and hobbies (hunting, fishing, boating, aviation)
Vital statistics (birth, death, marriage records)	Social Security number, information about parents, spouses, and children
Property title	Size of home, address, price, physical description, mortgage
Property tax records	Assessed home value, address
Voter registration and history	Address, date of birth, political party affiliation, voting frequency
Court records	Details of criminal, civil, divorce, and bankruptcy proceedings

Source: LBJ-PRP, 2003, p. 78

Some records required by the government might be personally embarrassing. As long as the only way to access this information was to visit “the local courthouse, [the information] remained hidden from larger public view... [Now] these once obscure records can be accessed from anywhere in the world” (Hammitt, 2002, ¶ 3). With new technologies and the growth of computer use, governments are forced to reconsider what constitutes a public record. This reconsideration is due, in part, to the fact that the widespread dissemination of records can now occur much more easily (Hammitt). Varian provides one example:

My understanding was that housing assessments were meant to be available on a "need to know" basis so that homeowners could compare their assessments to others to judge whether they were being fairly assessed. There wasn't any intent (or good argument for) making these assessments publicly available via a broadcast medium (Personal Correspondence, June 30, 2003).

In other words, just because someone's tax assessment can be obtained by waiting in line at a county clerk's office, should digital technology, like the internet, be utilized to make obtaining that information easier?

Privacy and Semi-public Information

In the past, information was *de facto* private or semi-public since "mass information on paper was difficult to compile and manipulate" (Mitra, 2001, p. 8). If specific information was desired, it had to be requested, identified, and searched for through warehouses or filing cabinets, and it was obtainable only from a specific location (Mitra; Alderman and Kennedy, 1995, p. 323). One would have to make travel to that location, spend a period of time there, and pay any fee that might be imposed. Similar "semi-public" information might be available in a different jurisdiction at possibly a different cost and most certainly a different location.

Additionally, in the past if documents were not current, they may have been destroyed or made inaccessible through storage. Obsolete information can be misleading, inaccurate or "incriminate out of context," and agencies were able to replace old hard copy documents with new ones. With the advancement of computer technology, that safety net of having older or "non-recent vintage" documents either inaccessible or destroyed is gone (Alderman and Kennedy, p. 324; DeCew, 1997, p. 150).

Important Stakeholder Groups

Local Governments: Local governments concerned with semi-public information can be as small as the local fire district to as large as a state government agency. Each governmental entity collects or has collected information provided by their constituents that might have been accessible in the past but only on a limited basis or in a controlled manner. Local governments face a conundrum between protecting a perceived privacy right associated with semi-public information and the lower overhead costs and ease of accessibility associated with advanced electronic data storage.

Individuals: Semi-public information directly and indirectly affects individuals. An individual may want to know what his neighbor's property assessment is, for instance, so he can better assess the value of his own property. Yet that same individual will fight the disclosure of his assessment (Liptak's point of "privacy for me but not for thee"). While a business may compel customers to divulge information in order to receive a good or service, if a government compels its constituents to divulge information to receive services, there is no choice other than to live elsewhere. Additionally, individuals previously had the assurance that, while their information might be available, there was control over its distribution.

Costs

With governments readily collecting information about their constituents, some would say it is in society's best interest to have this information readily available for review and analysis. Some information gathered by governments is used extensively. Information having "widespread use" and being widely disseminated should be provided for free (Varian, 2003). However there is a large pool of information gathered by government that is not widely disseminated (e.g. personal information such as birth certificates; obscure information; information with security ramifications) that currently has an expense associated with its acquisition.

There is a fixed cost associated with semi-public information that can be reduced through the utilization of new data storage technologies. Government could reduce the cost associated with data storage and retrieval, but is there an obligation for government to incur a certain amount of cost to maintain their constituents' privacy? As Cate points out, regulating privacy should generate greater benefit than cost and privacy laws should not generate any "cost that does not achieve commensurate increases in privacy protection" (2001, p. 52).

Benefits

A Nation Online, a report issued by the Department of Commerce, estimates that two million additional Americans join the ranks of internet users each month (U.S. Department of Commerce et al., 2002, p.91). It is true that, more people use the internet each day, but *A Nation Online* also refers to the fact that many Americans do not have access to the internet. Even if access to the internet is available, it may be outside of one's home (at work, at a public library) or the technology available may not permit a user to utilize all the tools the internet offers. This inequality is well documented and has resulted in what has been called a digital divide (Chapman, 2001; Department of Commerce, et al.). Even if the internet is available, there are many different ways to gain internet access including cable modem, dial-up, wireless, and other methods which offer different capabilities and transmission speeds. Further, limitations in technology can cause some computers to be incompatible with certain programs or information downloaded off the internet. Varian has described how public records are becoming less private as the internet becomes more integrated in society (1996). He addresses public information availability by pointing out that, while records have always been available from public agencies, certain records have not always been easy to obtain. Varian writes:

Information that was previously deemed useful to be publicly available under the old transactions technology, may now be deemed to be *too* available... The information could be made available in digital form, but at a price that reflected the transactions costs implicit in acquiring the information using the old technology (1996, pp. 9-10).

Varian implies that semi-public information can have a desired level of privacy preserved by equalizing the costs of obtaining information. Under the assumption that public information is available in a number of forms (i.e., in person or through the internet), the transaction cost

of obtaining information electronically should, according to Varian, be equal to obtaining the information through more conventional or historical method.

Conclusion

Governmental agencies will continue to collect personal information about citizens within and beyond their jurisdictions. There is little argument that information is collected by governmental agencies. What is of concern is what is done with the information once it is collected, especially as the internet makes information collection easier. Hammitt points out that a difficult balance between electronic access and the concerns for personal information protection will have to be maintained by governments (2002).

The Texas Advisory Commission on Intergovernmental Relations in its 1977 report *Privacy and Public Records* made several suggestions for maintaining the balance between the privacy of constituents and information availability. Today as governments are faced with a new “difficult balance”, these suggestions could still easily be applied:

In many cases it appears that a better procedure could be adopted to:

- ensure that only necessary information is compiled,
- inform subjects of the purpose for collecting specific information,
- purge files that are no longer needed,
- allow record subjects to inspect their files and if necessary correct inaccurate or incomplete information,
- provide better security for confidential files, and
- protect private information in computerized data banks (1977, p. xiv).

In the internet-dominated world, much information is readily available at the touch of a button. Information that was once obtained for a price is now available with little or no cost. This ease of access combined with lack of cost has lowered the level of privacy that once existed. Varian suggests that this aspect of privacy could be regained through economic means. For example, if it originally took one hour to wait for a tax payment report and there was driving involved in getting to the information, then a fee could be charged to those obtaining this information through the internet that represents the costs associated with the original means of obtaining the information. While situations related to privacy include “uncertainties and information asymmetries,” allowing for the “marginal [efficiency] of information regardless of where it ends up being used is reasonable to maintain stability” (Acquisti, Personal correspondence, June 4, 2003).

Costs associated with acquiring “semi-public” information might include opportunity costs for staff to obtain a requested record, transit time (mail), opportunity costs associated with time waiting in line, or travel expenses getting to the location and parking. While all transaction costs associated with “semi-public” information may not easily be determined, “one could come up with a reasonable number...; there is no compelling reason why information (such as housing assessments) could not involve modest user fees” as a cost for accessing semi-public information via non-traditional methods (Personal Correspondence,

Varian, 2003). Using Varian's approach, governmental agencies could utilize an equalization model until that time that the information in question has "widespread use" or is reasonably accessible to all constituents by non-traditional methods.

Equalization Model

Equalizing transaction costs benefits society in that information historically "semi-public" can remain semi-public and avoid idle or unwarranted use. To paraphrase Rubin and Lenard, if information provided by constituents is suddenly not being accurately used or transmitted according to their expectations, regulation of the market is reasonable from an economic standpoint (2002, xiv).

The societal and personal values to both open government and privacy precipitate the need to find a workable balance between the two. The issue is of special importance because unlike [commercial transactions], citizens are compelled to disclose information to the government in order to receive governmental services, licenses, and benefits (Mitra, 2001, p. 9).

Taking Varian's equalization theory at face value, a governmental agency would be able to offer access to information through different options to a broader constituency, but still keep that information semi-public.

Continuing with the example that one is trying to obtain semi-public information such as the tax assessment on a piece of property, the total cost of going to the county tax assessor's office would be considered equal to the cost of obtaining the information over the internet. Certain pieces of information, while available to the public, are still private in nature. Privacy as "the right to be left alone or not be annoyed" means that while public information should be available, if the information was intended to be semi-public, it should remain semi-public and ensure that privacy is not decreased.

The equalization model, $(C + SX + Y) - SZ = E$, is designed specifically to give a local government the flexibility to determine a fair and reasonable charge to obtain "semi-public" information. The equalization model is not meant as a revenue generator for governments, for Varian points out that measuring the incremental cost of providing "semi-public" information is very hard to measure (2003). This model offers a means for providing a balance between access and privacy concerns. Also, the variables incorporated into the model allow for local interpretation.

C = Fixed or actual cost of receiving the information

There is always a fixed or specified cost to obtaining information. This cost "C" might be a fee assessed to process the request. If the fixed cost of obtaining the information is equal to C, then C must include all fees and mandated charges imposed to fulfill a request.

X = Time specifically associated with the established method of obtaining the information

Obtaining information always takes time. The amount of time can vary depending on traffic, how far one travels, or simply time to process a request. A calculation of time might include a mean amount of time to reach the destination from the generally accepted coverage boundary for the location in question. There should also be consideration for a typical wait for information to be processed, but only time that has a clear opportunity cost.

S = Value of time

The value of time needs to be determined. With the disparity of salaries other time related costs, there needs to be a specific rate attributed to time that is not too high yet not too low. The value of time needs to be comprehensive and consider the different values individuals place on time. A reasonable amount (and one that Varian uses in his argument) would be \$25.00 per hour.

Y = Fixed costs associated with obtaining the information (not required but more than likely incurred, i.e., parking, mass transit, and the like)

It is possible that there are specific costs attributed to obtaining information, e.g., postage, parking, tolls, or mass transit, that are unavoidable to the point of being mandatory. Whatever the variable costs, they should be included in the formula only if they are almost certain and reasonable for the most common means of obtaining the information.

Z = Time specifically associated in receiving the information electronically

As with gathering “semi-public” information from the more established methods (clerk’s office), gathering information electronically takes time. The amount of time can vary depending on which means is utilized (i.e., cable modem or phone line). The calculation of time should include a mean amount of time to reach a Web site and time to access the information.

E = Cost of obtaining information through digital technologies

The cost of information from new digital technologies (e.g., the internet) would be calculated as E.

$$(C + S*X + Y) - S*Z = E$$

Taking all the factors described above, the formula $(C + SX + Y) - SZ = E$ is composed. This formula takes into account costs of gathering information.

An Example of How the Formula Might Work

Person A is interested in determining the tax assessments on one property. To do so, he decides to go to the county tax assessor’s office. The office is downtown and can be accessed only by car. There is a toll bridge to enter the downtown area. He gets into his car

and pays a \$1.00 toll to cross the bridge, pays \$2.00 to park at a meter (there is no other option). He takes the elevator to the third floor office of the Assessor, waits 5 minutes for his turn. There he fills out two forms and pays a \$5.00 processing fee. After obtaining five pages of information, he needs to make copies at \$0.10 each. He leaves and gets into his car. Approximately one hour has transpired from the time he put the money in the meter to the time he got back into his car. All the times and amounts spent are reasonable.

Person B seeks the same information but has access to a computer with a cable modem. She logs on and goes straight to the Assessor's Web page. She scrolls down, finds the proper forms, and fills them out online. In three minutes the information appears on her screen, and she prints it out. The total amount of time used (from entering Web site to printing) is 10 minutes. Assume these times are reasonable.

Table 7.2 displays the variables associated with the Equalization Model, under the assumption that time is worth \$25.00 per hour (\$0.42 per minute). Table 7.3 illustrates the formula associated with the Equalization Model.

Table 7.2

Equalization Model - Variables

Variable	Cost	Reason
C - (Fixed costs)	\$5.00	Processing fee
S - (Value of time)	\$0.42 per minute	
X - (Time to acquire using conventional means)	60 minutes	Time from paying meter to leaving
Y - (Variable costs)	\$1.00	Toll
	\$2.00	Parking
	\$0.50	Copies
Z - (Time to acquire with new technology)	10 minutes	Time from entering Web site to printing

The equalization model would be:

Table 7.3

Equalization Model - Formula

$$(C + SX + Y) - SZ = E$$

$$(\$5.00 + .42(60) + \$3.50) - .42(10) = E$$

$$\$33.70 - \$4.20 = E$$

$$\$29.50 = E$$

In the above example, the cost of acquiring the information over the internet would be \$29.50. This payment would equalize the gathering of information by the two means. “This sort of charging schedule essentially restores the status quo, provides some funds for local government, and offers an additional choice to individuals. People who didn’t want to pay the [\$29.50] could make the trip to the county records office and access the same information there ‘for free’ (i.e., paying no additional monetary cost)” (Varian, 1996, p. 10).

Is the Equalization Model the Best Alternative?

While a program such as the equalization model might equalize access to semi-private information between forms of acquisition, there are issues that should be addressed. Minimizing cost for public information is a goal worthy of consideration. In the case of semi-private information, until a community is assured that there is equal access to electronic access processes and an educated population, then one group of citizens should not have a distinct advantage over another. Additionally, the costs included in the equalization model are typical for the average constituent of the governmental entity in question. If someone is atypical (lives outside the jurisdiction) then the electronic version would be a convenience provided and an opportunity cost of not having to drive to receive the information would be realized.

Semi-public information is information collected by governmental agencies (e.g., tax assessments); access to this information is limited due to such constraints as office location or hours of operation. The semi-public information described above is what the Equalization Model, $(C + SX + Y) - SZ = E$, is intended for. With the advent of electronic means of accessibility, semi-public information is becoming less private and more public. This model can easily be implemented until access to alternative electronic means is equalized or standardized. The Equalization Model will help assure that the “semi-public” or the private nature of the information in question is maintained by equalizing the cost of access in the short term.

This chapter has illustrated how semi-public information has economic ramifications important to privacy concerns. Costs can be saved if information were made readily available, but the privacy of constituents would be compromised. If information is available at a substantial cost, thus making it somewhat private, does that privacy need to be maintained if the information is now offered through a different mechanism?

Matrix (Summary for Chapter 7)

Case Study: "Semi-public" Information			
	Stakeholder 1	Stakeholder 2	Stakeholder 3
	Local Government	Local constituents	Society outside local area
Privacy Component			
Ability of governments to maintain "semi-public" information	Residency check	Reasonable expectation of privacy	Restriction of information access
Keeping information from being viewed electronically	Tradition, meets constituents' wishes	Continued privacy	Restriction of access
Costs	Storage and manpower	Freedom of information	Lack of ability to optimize access to information or use information casually
Benefits	Control over who gains access to information	Security of information collected through mandate Preserves perceived privacy	Allows for limited access to information
Recommendations			
Texas Advisory Counsel Suggestions	Sets standards for information release	Understanding of how and when information is released	Standardizes records
Equalization Model	Offers a means to preserve a traditional level of privacy while incorporating new digital technologies	Allows access through digital technology (internet) but reduces threat of idle use from unconcerned parties	Makes access more available but at a cost

Chapter 8. Conclusion

This report has shown that privacy discussion often takes place utilizing economic terminology, yet the economic trade-offs are absent from the formulation of the final privacy policy. With privacy policy being developed in both the public and private sectors, all of society is affected by its changes and implementation. Recognizing that privacy covers such a broad area of study, four specific topics within the privacy policy “patchwork quilt” were chosen for analysis. Each of the four privacy policy topics (confidentiality and pre-litigation mediation; Section 215 of the USA PATRIOT Act; un-privacy and the internet; and “semi-public” information) illustrate how economic factors interact with privacy in a variety of ways.

Acquisti points out that “If privacy is a holistic concept, only a holistic approach can provide its adequate protection: economics to identify the information to share and the information to protect; law to signal the directions the market should thereby take; and technology to make those directions viable” (2002, p. 7). While policymakers give the impression they are keeping this holistic view in mind, they actually seem to focus only on law and technology as they determine how privacy policy is shaped. As policymakers formulate privacy policy, there needs to be more focus on the economic trade-offs caused by privacy decisions.

Privacy as a function of economics or economics as a function of privacy seems hard to grasp at first, but, as demonstrated, they can and do work together. Looking at privacy in terms of economic trade-offs helps illustrate that privacy policy and economic factors interact in important ways. This report has shown the economic questions surrounding pre-litigation mediation to be different from those of internet commerce. One uses economic factors to help ensure privacy, and the other uses un-privacy to ensure the economic success of e-commerce. This report has also shown how privacy in the context of law enforcement’s access to library records, as in Section 215, is different from confidentiality in mediation. Each of these privacy policies affects its relevant stakeholders differently, and both have distinct economic consequences. For instance, chapter four shows that, while costs and confidentiality work independently in pre-litigation mediation, in this case there is a precarious balance that exists between privacy and economics. If either confidentiality or cost became less effective the entire mediation process might be damaged.

Clymer claims, “Privacy is an issue of fears – often, but not always rational fears” (2003, ¶ 21). Culnan adds that these fears appear when the public perceives a threat from new information technology “with enhanced capabilities for surveillance, storage, retrieval, and communication of personal information” (1993, p. 343). “Semi-public” information and Section 215 of the USA PATRIOT Act demonstrate how privacy fears can arise from enhanced data collection and retrieval. The economic consequences of Section 215, while arguably not significant, are a concern of the general population. If economic consequences associated with information retrieval (whether real or perceived) were considered during policy formulation, the debate about Section 215 may not have been avoided but perhaps the section would have been more palatable and less frightening economically for the bookstore

owner, a library system, and/or the users of these establishments. Similarly, the equalization model in chapter seven offers an economic means of addressing privacy concerns by lowering the perception of idle use of information not historically accessible.

Samarajiva notes, “Public attitudes are affected by laws and regulatory processes as well as by corporate practices” (1998, p. 302). Policymakers and privacy advocates need to better inform the general public about the economic consequences of having or not having privacy protection. Rubin and Lenard point out that “it is easy for individuals to say they want more of a particular good (e.g., privacy) when not being made aware of potential costs” (p. 49). If costs and benefits of a privacy policy are understood, the economic trade-offs associated with a particular privacy concern will seem less burdensome (internet); more worthwhile (mediation); less controversial (Section 215); or more viable (“semi-public” information). Clearly, understanding privacy policy from an economic perspective is important, and moreover a strategy that works. Looking at privacy through an economic lens and understanding the privacy implications of economic decisions in the end is good public policymaking.

The four privacy policies discussed in this report can be improved or strengthened by looking at the trade-offs brought about by interaction of privacy and economics. In each of these four cases, however, a lack of understanding of the issues or an unwillingness to implement privacy policies effectively will have economic consequences. This report has demonstrated that, when it comes to privacy policy, the economic impacts are real and should be recognized and considered in formulating that policy.

Appendix A. Defining Terms: What is Privacy?

Prepared Statement of Jim Harper, Editor of Privacilla.org Hearing on H.R. 4561, the "Federal Agency Protection of Privacy Act" U.S. House of Representatives Committee on the Judiciary Subcommittee on Commercial and Administrative Law.

Source: U. S. Congress. House Subcommittee on Commercial and Administrative Law
Federal Agency protection of Privacy Act: Hearing, 2002, p.21

May 1, 2002

(EXCERPT)

Chairman Barr, Mr. Watt, and Members of the Subcommittee:

It is a great pleasure to appear before you to discuss H.R. 4561, the "Federal Agency Protection of Privacy Act." I am Jim Harper, the Editor of Privacilla.org, a Web-based think-tank devoted exclusively to privacy. I am also an Adjunct Fellow at the Progress & Freedom Foundation and the Founder and Principal of Information Age lobbying and consulting firm PolicyCounsel.Com.

Privacy is one of the most complex and difficult public policy issues confronting Congress and legislatures across the country today. I am pleased to lend what knowledge I have to your consideration of this legislation.....

The Judiciary Committee is the committee of American law and legal institutions. There is no better place to define and give structure to terms such as our focus today: privacy. By digging deeply into privacy as a legal concept, you as congressional leaders can dramatically improve the quality of many public policy debates, and the outcomes Congress produces for the American people.

Left undefined, the word "privacy" has become far too much of a stalking horse for all variety of ideological and special interest groups. Indeed, a coterie of activist organizations - including Privacilla - thrives because there is not an agreed to and limited definition for the word "privacy" in current debate. Moreover, the lack of definition has rendered Congress, state legislatures, the press, and the public less able to find solutions to the many problems and legitimate concerns that popularly fall under the heading of "privacy."

For example, identity fraud is widely perceived as a "privacy" problem. But it is better understood as a group of crimes that thrive on the use of personal identification and financial information. Because of this widespread misperception, the crimes that constitute identity fraud go poorly enforced while Congress considers banning many uses of Social Security Numbers in the name of "privacy." Limiting SSN use would likely stifle many benefits that consumers and the economy enjoy without effectively reducing this serious crime problem.

Similarly, unwanted commercial e-mail, or "spam," is an intrusion into electronic communications and a serious annoyance that is often labeled as a "privacy" problem. Spam exists in large part because e-mail marketers know little or nothing about the interests of potential customers. It is difficult to reconcile spam - e-mails broadcast to unknown people nearly at random - with the heart of the privacy concept, which is too much personal information being available too widely.

At Privacilla, we have a working definition of privacy that we believe should form the basis of policy discussions on the topic: Privacy is a subjective condition that individuals enjoy when two factors are in place — legal ability to control information about oneself, and exercise of that control consistent with one's interests and values.

Privacy is a personal, subjective condition. It is a state of affairs individuals enjoy based on sharing or retention of information about themselves consistent with their own preferences. These preferences are a product of such things as culture, upbringing, and experience. Because privacy is subjective, one person cannot decide for another what his or her sense of privacy should be. You can not tell me, either by giving your opinion or by passing a law, that my privacy is protected when I think it is not.

The first factor above goes to the existence of choice — the legal power to control the release of information. A person who wishes to maintain privacy in the appearance of his or her body, for example, may put on clothes and be relatively certain that no one will remove that clothing without permission. Few laws require people to remove their clothing and, thanks to the concept of "battery" in state tort and criminal law, private actors may be punished for touching our clothing in any way that interferes with bodily privacy. Our choices to hide or reveal information about the appearance of our bodies are protected by law.

Likewise, a person who wants to prevent others from gaining knowledge of his or her purchasing patterns may pay in cash and regularly change the stores at which he or she shops. He or she may also arrange by contract to have personal information maintained in confidence. Various legal protections, such as the law of contracts, give us autonomy and choice that we use to protect privacy.

The second factor is exercising that control of information consistent with our values. This is difficult in many commercial marketplaces. Many consumers are unaware of how the Information Economy works, and the fact that they are a part of it. Many industries are monolithic in their information practices. Arguably, they fail to fully inform consumers about what happens with personal information, and they offer consumers few alternatives. This is arguable, however. It may be that only a tiny, but vocal minority of consumers and activists actually wants to study commercial information practices and exercise choice among different options. If a significant number of consumers do, they are a market waiting to be served.

As policy-makers, we should not presuppose that a certain amount or type of privacy serves consumers' interests in the marketplace, and Privacilla's definition of privacy does not do this. Advocates who claim to know what consumers want in terms of privacy prove their ignorance by making the claim.

Consumers may rationally determine that they are safe from harmful uses of information when dealing with certain companies and leave it at that. The fact that hundreds or even thousands of mundane facts about themselves are in the hands of businesses may be a matter of indifference to reasonable people. Aware, empowered, and responsible consumers can demand of businesses what options they want in terms of information sharing or withholding. They can also demand, if they prefer, lower prices, customized service, combined offerings, and so on.

Unless Congress and state legislators are going to guess at consumers' true preferences and impose them from the top down, only consumer education will deliver privacy on the terms consumers want it in the commercial world. Governments cannot protect privacy directly; they can only foster or destroy people's ability to protect their own privacy.

Copyright 2003

Appendix B. Defining Terms: Mediation

Source: The State of North Dakota – Office of Administrative Hearings offers this comprehensive definition of mediation and its uses. Source: the North Dakota – Office of Administrative Hearings.

Mediation is the most popular form of ADR, in which a third-party neutral, a mediator, guides the interaction of the participants. A mediator will:

- Maximize communication between the parties, ensuring all parties are treated with dignity and respect.
- Identify the interests behind the positions the parties have taken in the dispute.
- Meet with all parties in one group and/or talk to each party individually and move back and forth between the tables if that is helpful. Information shared with the mediator in these sessions will not be relayed to the other party unless the mediator is given specific permission to do so.
- Assist parties in the generation and evaluation of options which may resolve the dispute to the satisfaction of all parties.
- Assist in writing any agreement which may remain confidential unless otherwise required by law.



Communications are confidential.

- Communications in a mediation or between the parties and the mediator are confidential. Each party can give the mediator confidential information knowing that the mediator will not share that information with anyone else unless the party gives permission to do so. Sharing information in a mediation does not, however, protect information if it is otherwise discoverable in litigation, or public information as required by law.



Participants have the ultimate control over the outcome.

- Parties, who have the most knowledge about the dispute, can fashion an agreement to resolve it.
- Parties may create solutions satisfactory to all parties that may not be available through a formal legal or administrative process.
- The mediator cannot force the parties to reach any agreement.

- The mediator cannot enter any orders in any pending case related to the mediation.
- Participants do not give up any right they have to litigation or a hearing by participating in a mediation.



Mediation often works because the process allows the parties to:

- Express their feelings and interests.
- Be heard in a confidential process.
- Identify what is really important to them.
- Get feedback from a neutral outsider about the dispute.
- Formulate options for resolving the dispute and evaluate the pros and cons of each option.
- Have absolute control over whether agreement is reached.



Mediation is particularly appropriate when:

- The parties have an ongoing relationship.
- The consequences of not resolving the dispute are negative, i.e., expensive, time consuming, risky, or otherwise unsatisfactory.
- There is a wide range of potential resolutions to the dispute.



Mediation is probably not appropriate when:

- An agency needs a legal interpretation by a judicial body to guide future actions.
- An agency is seeking to establish an important precedent.

Appendix C. USA PATRIOT Act Section 215

H.R.3162

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Enrolled as Agreed to or Passed by Both House and Senate)

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall--

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the U. S.

(b) Each application under this section--

(1) shall be made to--

(A) a judge of the court established by section 103(a); or

(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

`(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

`(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

`(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

`(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

`(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

`SEC. 502. CONGRESSIONAL OVERSIGHT.

`(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.

`(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period--

`(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and

`(2) the total number of such orders either granted, modified, or denied.

Appendix D. The Privacy Policy Matrix

Comparison of Case Studies

	Chapter 4: Privacy in pre-litigation mediation	Chapter 5: “Un-privacy” and the internet	Chapter 6: Privacy and Section 215	Chapter 7: Privacy and semi-public information
Privacy Component	No public disclosure (court papers) Confidentiality of mediation	Disclosing personal information	Law enforcement’s ability to look at use records of individuals Unlawful to disclose if records are viewed by law enforcement	Ability of governments to maintain “semi-public” information Keeping information from being viewed electronically
Stakeholders	Courts Private business Individuals	Individuals Private business	Government Individuals Law enforcement Organizations (i.e. private business; public libraries)	Local Government Individuals
Costs	Loss of knowledge about parties involved	Frustrating procedures to keep personal information private	Trust of government and law enforcement	Lack of ability to optimize access to information or use information casually Storage and manpower
Benefits	Lower legal costs Privacy Reduced number of cases in court system	Targeted marketing Fewer unwanted goods, services, and “spam”	Reduced likelihood of terrorist attacks Freedom to investigate terrorists by law enforcement	Security of information collected through mandate Preserves a traditional level of privacy
Policy Recommendations	Strengthen confidentiality Encourage the use of pre-litigation mediation	Highly visible opt-out measures	Maintain and reinforce sunset clause Financial oversight	Texas Advisory Counsel Suggestions Equalization Model

Privacy Concerns of Stakeholders

	Individuals	Court System / Law Enforcement	Government / Local Government	Organizations (i.e. private business and public libraries)	Society
Pre-litigation Mediation	Privacy gained Relationships retained Potential for lower legal costs Loss of knowledge of other parties' past	Case load reduced	-- NA --	Privacy gained Relationships retained Potential for lower legal costs Loss of knowledge of other parties' past	Lack of knowledge about past improprieties and business practices Less legal expenditures
“Un-privacy” and the Internet	Loss of privacy Better targeted information, goods and services	-- NA --	-- NA --	Gains knowledge of customer Economical business practice	Frustrating procedures to keep personal information private New economic opportunities and conveniences
Section 215 of the USA PATRIOT Act	Perceived loss of privacy Access to information is unchanged Security	Fewer restrictions on gathering information on suspects Loss of trust	Gains secrecy and knowledge Loss of trust Increased national security	Loss of trust Less data on customers Increased security	Loss of privacy Increased security
“Semi-public” Information	Reasonable expectation of privacy	-- NA --	Conflict over preserving traditional level of privacy and cost savings from digital technology	-- NA --	Restriction of information access

Personal Correspondence

Throughout the course of writing this report, a number of interviews, letters, e-mails, discussions, and workshops were utilized. Below is a list of those whose expertise is incorporated in this report either directly or indirectly. Their time and assistance is greatly appreciated.

- Acquisti, Alessandro, Assistant Professor, Carnegie Mellon University, Pittsburgh, PA through the School of Information and Systems at the University of California at Berkeley, Berkeley, CA and (June 4, 2003)
- Brown, Laura, Chief Librarian, American Arbitration Association, New York (December 27, 2002)
- Chapman, Gary, Participating Faculty and Lecturer, Director, 21st Century Project, Lyndon B. Johnson School of Public Affairs, University of Texas at Austin, (April 12, 2002)
- Doty, Philip, Professor, School of Information, University of Texas at Texas (Fall 2002 and Spring 2003)
- Elrod, Jack, General Counsel, Dallas Independent School District (March 31, 2002).
- Flamm, Kenneth, Dean Rusk Chair in International Affairs, Lyndon B. Johnson School of Public Affairs, University of Texas at Austin (Spring 2003)
- Flemming, John, Mediator, Galton, Cunningham & Bourgeois, P.L.L.C., Austin, TX (July 11, 2003)
- Gutekunst, Claire, Partner, Proskauer Rose LLP., New York (December 2002)
- Linz, Michael, American Civil Liberties Union, Austin, TX (April 16, 2003)
- Meade, Robert, Vice President, American Arbitration Association (Spring 2001 and January 2003)
- Olivella, Mike, Department Chair – Alternative Dispute Resolution and Mediation Advocacy, Katz, Kutter, Alderman & Bryant, P.A., Tallahassee, Florida (January 23, 2003)

- Sales, Nathan A., Office of Legal Policy, United States Department of Justice, Austin, TX (April 16, 2003)
- Updegrave, Daniel, Vice President for Information Technology, University of Texas at Austin, Austin, TX (March 7, 2003)
- Varian, Hal, Dean – School of Information Management and Systems, University of California at Berkeley, Berkeley, CA (June 30, 2003)
- Wolf, Chris, Partner, Proskauer Rose LLP., Washington, DC. (Dec. 11, 2002)

COPYRIGHT 2003

References

- Acquisti, Alessandro, "Protecting Privacy with Economics: Economic Incentives for Preventive Technologies." PhD. Dissertation, The University of California at Berkeley, 2002, (Draft). Previously presented at the Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, Ubicomp 2002.
- Acquisti, Alessandro, and Hal R. Varian, "Conditioning Prices on Purchase History." Paper to support NSF grant #9979852 - University of California at Berkeley, November 21, 2002.
- Acquisti, Alessandro, Roger Dingledine, and Paul Syverson, "On the Economics of Anonymity." *Financial Cryptography*, 2003, (Draft).
- Alderman, Ellen, and Caroline Kennedy, *The Right to Privacy*, New York: Alfred A. Knopf, (1995).
- American Arbitration Association (AAA), AAA – Dispute Resolution Services Worldwide: Rules and Procedures. Available: <http://www.adr.org/index2.1.jsp?JSPssid=15727&JSPaid=37505>. Accessed: March 21, 2003.
- American Arbitration Association (AAA), *Consumer Due Process Protocol: A Due Process Protocol for Mediation and Arbitration of Consumer Disputes*, New York, May 1998.
- American Arbitration Association (AAA), *Guide to Mediation and Arbitration for Business People*. New York, September 2000.
- American Library Association (ALA), "The USA Patriot Act in the Library." American Library Association, Office for Intellectual Freedom (April 2002), Accessed August 11, 2003 from: http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/Intellectual_Freedom3/Intellectual_Freedom_Issues/usapatriotlibrary.pdf
- Berman, Lee Jay, "Hands Off Mediation Confidentiality." *Mediate.com* (September 2000), Accessed July 24, 2003 from: <http://mediate.com/articles/berman.cfm>.
- Bernstein, James, "NY Fed: Don't Blame 9/11 For All of the City's Woes." *Newsday* (February 27, 2003), p. A39, Accessed March 16, 2003 from Lexis-Nexis Academic Universe: <http://web.lexis->

nexis.com/universe/document?_m=62b0231dbc32b2482cadd27390975579&_docnum=12&wchp=dGLbVtb-ISIAI&_md5=ee9155107d1f8229f9ffd9119dce403e.

Bradley, Allison, TJ Costello, Robin McMillin and Bob Popinsky, "Redefining the Texas Teacher Shortage: Key Issues in Retention and Recruitment of Quality Educators." Policy Briefing Paper – Texas State House of Representatives, Presented to Speaker Pete Laney's Office of Education Affairs, December 2001.

Brown, Jaime E., Letter to the Honorable F. James Sensenbrenner, and Honorable John Conyers, May 13, 2003, The United States Department of Justice, Office of Legislative Affairs, Office of the Assistant Attorney General.

Cate, Fred H., *Privacy in Perspective*, Washington, DC, The AIE Press, (2001).

Center for Democracy and Technology (CDT), "Why Am I Getting All This Spam?: Unsolicited Commercial E-mail Research Six Month Report.", (March 2003), Accessed March 24, 2003 from: <http://www.cdt.org/speech/spam/030319spamreport.pdf>.

Chang, Nancy, "How does USA PATRIOT Act affect Bill of Rights?" *New York Law Journal*, (December 6, 2001), Accessed October 22, 2002 from: http://web.lexis-nexis.com/universe/document?_m=c5486afc4728d586a6ec5229a3d71.

Chapman, Gary, "The Great Digital Divide." *The Texas Monthly* (March 2001), Accessed July 25, 2003 from: <http://www.texasmonthly.com/mag/issues/authors/garychapman.php>.

Clymer, Adam. "In the Fight for Privacy, States Set Off Sparks." *The New York Times – Week in Review* (July 6, 2003), Section 4, p. 1.

Conference Board. Quarterly press release regarding online transactions. (January 2003), Accessed January 4, 2003 from: <http://www.conference-board.org/utilities/press.cfm>.

Congressional Research Service (CRS), CRS Report for Congress – The USA PATRIOT Act – A Legal Analysis, April 15, 2002, Through the CRS Web, Accessed October 20, 2002 from: <http://fpc.state.gov/documents/organization/10092.pdf>.

Conrad, Daniel R., "Confidentiality Protection in Mediation: Methods and Potential Problems in North Dakota." *North Dakota Law Review*, Vol. 74 No. 1 (1998).

Council for Exceptional Children, "Mediation Opens Door to Amicable Dispute Resolution for Schools, Parents and Students", (October 1996), Accessed March 23, 2003 from: http://www.ldonline.org/ld_indepth/legal_legislative/mediation.html.

Culnan, Mary J., "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use." *MIS Quarterly*, The Economics of Privacy, The American Economic Review, Vol. 17, No. 3 September 1993 pp. 341-363. Accessed January 6, 2003 from J-Stor.

DeCew, Judith Wagner, *In Pursuit of Privacy*. Ithaca, New York: Cornell University Press, 1997.

Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, Massachusetts: The MIT press, 1999.

Doty, Philip, "Digital privacy: Toward a new politics and discursive practice." In Martha E. Williams (Ed.), *Annual review of information science and technology*, (Vol. 35, pp. 115-245), Medford, NJ: Information Today (2001).

EEOC v. Waffle House, Inc., U.S. Supreme Court No. 99-1823 (Jan. 15, 2002). Accessed March 22, 2003 from: <http://supct.law.cornell.edu/supct/html/99-1823.ZS.html>.

Elan, Susan, "Library Association head questions Patriot Act estimate." Not In Our Name project (May 23, 2003), Accessed August 11, 2003 from: http://www.notinourname.net/police_state_restrictions/library_asec_questions_est_23_may03.htm

Electronic Frontier Foundation (EFF), EFF Analysis of USA PATRIOT Act (October 31, 2001), Accessed October 20, 2002 from: http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html.

Electronic Frontier Foundation (EFF), EFF Analysis of "PATRIOT II" (January 9, 2003), Accessed July 19, 2003 from: http://www.eff.org/Censorship/Terrorism_militias/patriot-act-II-analysis.php.

Fagan, Wayne I. and Brian D. Shannon, "A Potential Threat to Texas ADR." State Bar of Texas, *A legal Perspective – Alternative Dispute Resolution*, (2002), Accessed March 23, 2003 from: <http://www.texasbar.com/globals/tbj/jan02/ADR.asp>.

Federal Trade Commission (FTC), "Privacy Online: Fair Information Practices in the Electronic Marketplace." May 2000.

- Gaplan, Bryan. "Creeping Privatization: The Present and Potential of Alternative Dispute Resolution." *The Cato Institute, Regulation – The Cato Review of Business and Government* No. 2, 1994, Accessed February 9, 2003 from:
<http://www.cato.org/pubs/regulation/regv17n2/reg17n2-currents.html>.
- Gellman, Robert, "Does Privacy Law Work?" In Philip E. Agre & Marc Rotenberg (Eds.), *Technology and privacy: The new landscape*, 1998. (pp. 193-218). Cambridge, MA: MIT Press, 1998.
- Glenn, Donald, "Easing the Strain of Litigation Cost." *OUTLOOK*, Vol. LXI No. 3 (Fall 1993), p. 34.
- Goss, Jon. "'We Know Who You Are and Where You Live': The Instrumental Rationality of Geodemographic Systems." *Economic Geography*, Vol 71, No. 2. (April 1995), pp. 171-198. Accessed January 7, 2003 from J-stor: <http://links.jstor.org/sici?sici=0013-0095%28199504%2971%3A2%3C171%3A%22KWYAA%3E2.0.CO%3B2-D>.
- Hammitt, Harry. "To Put 'Public Records' on the Web or Not?" *Privacy Journal*, Vol. 29, No. 2, (December 2002).
- Hensler, Deborah R., "Does ADR Really Save Money? The Jury's Still Out." *The RAND Reprint Series*, RAND/RP-327, (Reprinted from *The National Law Journal*), 1994.
- Keating, J. Michael, "Getting Reluctant Parties to Mediate (A Guide for Advocates)." CPR Institute of Dispute Resolution: *Alternatives* (January 1995), Accessed April 13, 2003 from New York State Dispute Resolution Association:
http://www.nysdra.org/articles/article_details.asp?ID=49.
- Keeney, Ralph L., "The Value of Internet Commerce to the Customer." *Management Science*, Vol. 45, No. 4. (April 1999), pp. 533-542. Accessed January 10, 2003 from J-stor:
<http://links.jstor.org/sici?sici=0025-1909%28199904%2945%3A4%3C533%3ATVOICT%3E2.0.CO%3B2-M>.
- Kenney, John J., Joseph M. McLaughlin and Valerie Caproni, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act") Act of 2001." Simpson Thatcher & Bartlett (November 12, 2001), Accessed October 21, 2002 from:
www.simpsonthatcher.com/FSL5CS/memos/memos1025.asp.
- Knapp, Michael C., "E-Commerce: Real Issues and Cases: Updates for Website (February 20, 2003)." Accessed March 18, 2003 from:
http://www.swcollege.com/acct/knapp/first_edition/updates.doc.

Krikorian, Adrienne L., "Litigate or Mediate?: Mediation as an Alternative to Lawsuits." Accessed January 15, 2003 from Mediate.com: <http://www.mediate.com/articles/krikorian.cfm>.

Lande, John, "Failing Faith in Litigation? A Survey of Business Lawyers' and Executives' Opinions." *The Harvard Negotiation Law Review* (Spring 1998).

Lessig, Lawrence, *The Future of Ideas*. New York: Random House (2001).

Levy, Robert A. "The USA Patriot Act: We Deserve Better." The Cato Institute (2003), Accessed February 9, 2003 from: <http://www.cato.org/current/terrorism/pubs/levy-martial-law.html>.

Liptak, Adam. "In the Name of Security, Privacy for Me, Not Thee." *The New York Times – Week in Review* (November 24, 2002), Section 4, p. 1.

Lyndon B. Johnson School of Public Affairs (LBJ-PRP). Privacy Protection in Texas. Policy Research Project Report Series, no. 144. Austin, Texas, 2003.

Madison, James R. "California Supreme Court Upholds Confidentiality in Mediation." *ADR Currents* (September – November 2001), p. 11.

Maharaj, Davan, "Tire Recall Fuels Drive to Bar Secret Settlements." *The Los Angeles Times* (September 10, 2000), p. A-1, Accessed July 26, 2003 from: [http://web2.infotrac.galegroup.com/itw/infomark/141/755/39044538w2/purl=rc1_SP00_0_CJ65120009&dyn=3!dgxrn_"News"_1_0_CJ65120009?sw_aep=txshracd2598](http://web2.infotrac.galegroup.com/itw/infomark/141/755/39044538w2/purl=rc1_SP00_0_CJ65120009&dyn=3!dgxrn_).

Marvel, Bill, "Is the F.B.I. watching what you're reading?" *The Bergen Record* (August 25, 2002), Accessed October 22, 2002 from: http://web.lexis-nexis.com/universe/document?_m=2333591830de7bc36b9614c1908574d.

Mitra, Vanessa. "For the Public's Eyes Only: Who Has the Right to Know?" Professional Report, Lyndon B. Johnson School of Public Affairs, The University of Texas at Austin, May 2001.

Murphy, Dean E., "Some Librarians Use Shredder to Show Opposition to New F.B.I. Powers." *The New York Times* (April 7, 2003), p. A11.

New York City Partnership and Chamber of Commerce. "Working Together to Accelerate New York's Recovery: Economic Impact Analysis of the September 11th Attack on New York City." (November 2001), Accessed March 16, 2003 from <http://www.nycp.org/impactstudy/EconImpactStudy.pdf>.

- North Carolina Ad Hoc Dispute Resolution Task Force. Report of the Ad Hoc Dispute Resolution Task Force (May 22, 2000), Accessed January 15, 2003 from: <http://www.comp.state.nc.us/ncic/pages/taskforce.htm>.
- North Dakota – Office of Administrative Hearings, “Mediation.” Accessed April 13, 2003 from: <http://www.state.nd.us/oah//Mediation.HTM>.
- O’Meara, Kelly Patricia, “Police State, Issues and Alibis.” (2001), Accessed October 21, 2002 from: www.dreamwater.net/art/uncleernie/page26.html
- Online Privacy Alliance, “The Price of Privacy.” Accessed April 8, 2003 from: <http://www.privacyalliance.org/resources/roundup.pdf>.
- Perritt, Henry, H., “Sources of Rights to Access Public Information.” Presented to the *William & Mary Bill of Rights Journal* and the Virginia Council on Information Management, Accessed: March 10, 2003 from: <http://www.courtstuff.com/JCIT/wandm.htm>.
- Posner, Richard A., *The Economics of Justice.*, Cambridge, Massachusetts: Harvard University Press (1981a).
- Posner, Richard A., “The Economics of Privacy.” *The American Economic Review*, Vol. 71, No. 2 (May 1981b), pp. 405-409. Accessed January 6, 2003 from J-stor: <http://links.jstor.org/sici?sici=0002-8282%28198105%2971%3A2%3C405%3ATEOP%3E2.0.CO%3B2-A>.
- Privacy Journal, “Should All Court Papers Be Posted on Web Sites?” *Privacy Journal* (January 2003), p. 3.
- Riba, Elisabeth, “The USA PATRIOT Act: the response and responsibility of library management.” (July 2002), Accessed October 21, 2002 from: www.osmond-riba.org/lis/usapatriot.htm.
- Rubin, Paul H, and Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*, Norwell, Massachusetts: Kluwer Academic Publishers (2002).
- Samarajiva, Rohan. “Interactivity as though privacy mattered.” In Philip E. Agre & Marc Rotenberg (Eds.), *Technology and privacy: The new landscape*, 1998. (pp. 277-309). Cambridge, MA: MIT Press, (1998).
- Schabner, Dean, “Right to Read: Librarians, Booksellers Take on Feds Over Patriot Act Provisions.” ABC News Online (April 24, 2003), Accessed July 19, 2003 from: <http://abcnews.go.com/sections/us/Business/righttoread030424.html>.

Schwartz, John, "Case Sensitive Crusader; Who Owns the Internet? You and i Do." *The New York Times – Week in Review* (December 29, 2002a), Section 4, p. 3.

Schwartz, John. "Guarding Privacy: Tricky Task for Consumers." *The New York Times* (October 17, 2002b), p. A1.

Sensenbrenner, James F, and John Conyers, Letter to the Honorable John D. Ashcroft, June 13, 2002 Accessed October 21, 2002 from:
<http://www.house.gov/judiciary/ashcroft061302.htm>.

Sensenbrenner, James F, and John Conyers, Letter to the Honorable John D. Ashcroft, April 1, 2003 Accessed July 19, 2003 from:
<http://www.house.gov/judiciary/patriot040103.htm>.

Shane, Michael B., "Creating Currency in Mediation", *ADR Currents*, (Spring 1997).

Sharp, Dennis. "The Many Faces of Mediation Confidentiality." *Dispute Resolution Journal* (November 1998), p. 56.

Siegel, Joel, "Fed Up and Hoping to Can the Spam." *The New York Daily News* (April 6, 2003), Accessed April 6, 2003 from:
http://story.news.yahoo.com/news?tmpl=story2&cid=355&ncid=355&e=18&u=/kr/20030406/lo_krnewyork/fed_up_and_hoping_to_can_the_spam.

Singletary, Michelle. "Big Mama Was Right About Financial Privacy." *The Kansas City Star*, Moneywise Section, December 22, 2002, p. G-11.

Singleton Solveig. "How Privacy Regulation Will Chill Commerce." *The Cato Institute* (December 13, 1999), Accessed February 9, 2003 from:
<http://www.cato.org/dailys/12-13-99.html>.

Smith, Francis B., "Consumer Privacy on the Global Information Infrastructure." *Consumer Alert: Comments to the Federal Trade Commission* (June 18, 1996), Accessed April 5, 2003 from <http://www.consumeralert.org/issues/telecom/ftcprivy.htm>.

Stamato, Linda, "Dispute Resolution and the Glass Ceiling: Ending Sexual Discrimination at the Top." *Dispute Resolution Journal*, (February 2000).

Stong, Elizabeth, "The Uniform Mediation Act: An Opportunity to Enhance Confidentiality in Business Mediation." *ADR Currents* (June – August 2002).

- Tedeschi, Bob, "E-Commerce Report; Filling Cracks in E-tailin's Promise to Protect Privacy." *The New York Times* (June 30, 2003), Section C, p. 5.
- Texas Advisory Commission on Intergovernmental Relations. *Privacy and Public Records*, Jack A. Griesenbeck – Chairman, Austin, Texas, February 1977.
- Texas Senate Bill 694, 75th Legislature, Regular Session (1997).
- The Economist.com. "Counting the Cost" from *The Economist Global Agenda* (September 11, 2002), Accessed March 16, 2003 from http://www.economist.com/agenda/displayStory.cfm?story_id=1324045.
- U.S. Congress. House Subcommittee on Commercial and Administrative Law of the Committee on the Judiciary. *Federal Agency protection of Privacy Act: Hearing*. 107th Cong., 2nd session, May 1, 2002.
- U.S. Congress. House Subcommittee on Commercial and Administrative Law of the Committee on the Judiciary. "*Know Your Customer*" Rules: *Privacy in the Hands of Federal Regulators: Hearing*. 107th Cong., 1st session, March 4, 1999.
- U.S. Department of Commerce, Economics and Statistics Administration, National Telecommunications and Information Administration, *A Nation Online: How Americans are Expanding Their Use of the Internet*. February 2002, Washington DC, Accessed July 25, 2003 from: <http://www.ntia.doc.gov/ntiahome/dn/index.html>.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PL 107-56, 115Stat 272 (2001) Accessed October 17, 2002 from: <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR>:
- Varian, Hal R. *Economic Aspects of Personal Privacy*, University of California at Berkeley, December 6, 1996, Accessed January 6, 2003 from <http://www.sims.berkeley.edu/~hal/Papers/privacy/>.
- Warren, Samuel L. and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* (December 15, 1890), Vol. IV, No. 5, Accessed January 6, 2003 from: http://www.lawrence.edu/fac/boardmaw/privacy_brand_warr2.html.

VITA

TJ Costello is originally from New Rochelle, NY and is a 1986 graduate of Ithaca College. At Ithaca, he achieved Honors in Economics while obtaining a Bachelor of Science in Economics-management.

His career has offered him the opportunity to play an important role in strategic development on a local, regional, and international basis. Before moving to Austin to attend the LBJ School of Public Affairs at the University of Texas at Austin, TJ was National Marketing Coordinator for the American Arbitration Association (AAA) in Manhattan. Prior to that, TJ worked for HANWHA International and Ethan Allen Inc. In addition, he has been appointed to the local zoning board as well as several oversight committees in South Brunswick Township, NJ.

For seven years, he coached basketball and softball at various levels (named High School Basketball Coach of the Year in 2000). At the LBJ School, TJ focused on Policy Development along with Crisis Management and Youth Advocacy. He was named Co-Chair of the Seventh Annual Barbara Jordan National Forum on Public Policy and was invited by the Center for Ethical Leadership to be a lecturer at its annual Leadership Conference.

Permanent Address: 2901 Barton Skyway #3410
Austin, TX 78746

This Professional Report was typed by the Author