

What Form of Privacy Regulation is Effective?

01 Introduction

The mass transit of personal information is a global phenomenon. While companies on both sides of the Atlantic aggregate, compile, link, sell, and exchange personal data, broad differences exist among how the various national governments formulate and implement the privacy policies and practices regulating this flow of personal data. Discrepancies in the definitions and philosophies behind “privacy” have resulted in diverse and inconsistent legislation protecting the online privacy of individuals. Following difficulties early on in creating a resolute policy, the European Union (EU) enacted the European Union Data Protection Directive (EU Directive) imposing significant regulatory controls over personal data collection, use, processing, and transfer guarding what can essentially be viewed as an inherit right to privacy. Conversely, the fear of an overly powerful government in the United States resulted in fragmented policy where regulation is often enacted as a response to specific public privacy anxieties. Ultimately, the commonality is the desire for the fair and equitable use of information though fundamental questions persist on the effectiveness of the various forms of privacy regulation.

02 Approach: European Union Centralized Legislation Need

The European approach to information privacy is premised on the belief that protecting personal data and individual privacy is a fundamental right where preventative measures protect citizens from privacy abuse. The foundation for their privacy law is traced to Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms where the right to privacy involving “private and family life, his home and his correspondence” was recognized. [1]

The importance attached to data protection against privacy abuse has been cited as historically motivated in twentieth century European history. The need for protecting personal information cited as a safeguard against personal data abuses that could be used to further efforts of population control similar to those exerted by the Nazi in World War II. [2] This has resulted in centralized public policy protecting personal information enforced by comprehensive administrative legislation.

Goals

The objective of the centralized legislation of the EU is the endorsement of dignity, autonomy, and self-determination. Most markedly, the EU Directive was set in place to guarantee the rights and freedom of the individual involving the processing of their personal information and their privacy right. It is widely considered the “most important international development in data protection in the last decade.” [4] Broadly, the Directive has two principle objectives: (1) protecting information privacy by Member States of the European Union and (2) preventing the restrictions on the free flow of personal information among EU Member States, for economic reasons. [3] Essentially, the goal was to establish a clear and comprehensive regulatory framework requiring a minimum standard for protecting privacy across the EU ensuring a high level of individual protection from privacy abuse in all Member States while also serving to increase the flow within the EU.

Informed Philosophies

The European scheme of data protection recognizes a fundamental right to data privacy. Within this concept, a just and free society exists when individuals can interact with self-determination and dignity. The right of the individual to his or her information hence becomes crucial in sustain this autonomy. As is the European tradition of the state playing an active role in protecting its citizens from abuse and social harm [3], the state is allowed to intercede between organizations and individuals to uphold parity and preserve the fundamental right through prophylactic protection

encompassing (1) norms for personal data aggregation and processing, (2) avenues for reviewing the information of an individual by the individual, (3) special protections for sensitive data (such as ethnicity, political alignment, and religion), (4) and the enforcement and oversight of the systems of protection.

Example

In 1998, Mrs. Lindquist created a website for parishioners awaiting confirmation. The website included the names, telephone numbers, hobbies, and various facts regarding this individual (including a foot injury in one case). Lindquist had not informed the parishioners about the website and had not obtained consent. Under the EU Directive, a Swedish prosecutor charged Lindquist with a criminal violation of Swedish privacy law. [7] Even after appeal, the Court of Justice determined that the Directive covers the publishing of personal information on websites and a fine was imposed on Lindquist. However, the case also clarified that EU-based websites don't automatically violate the international data transfer part of the Directive by merely posting information online and that affirmative action to transfer data is necessary before that transfer restriction comes into play. Had this not been so clarified, it may have entirely curtailed the web presence of many EU companies.

Advantages & Promise

The digital landscape changed and centralized legislation is one response. Today, more personal information is collected for numerous, very often legitimate, purposes. However, the potential for abuse of personal information has greatly increased. The EU Directive is comprehensive, broad legislation that enforces strict standards to protect personal. By providing a uniform baseline standard, the legislation succeeds in protecting data to ensure privacy and protect individuals from harm. The benefit is two-fold as all the nations in the European Union are now of greater standardization promoting the more efficient and safer exchange of data in the EU. The promise is thus that people will remain secure, safeguard against privacy abuses are in place, and

standardization permits the easier flow of information within the EU. The promise of centralized legislation is the preservation of the Internet as a safe place to communicate, play, and to do business.

Costs & Risk

The Directive poses strict limitations on the collection and use of personal data; however, there are distinct reasons supporting the freest possible flow of information including that of personal information. Arguably, the free collection and use of personal data may be to the benefit of businesses and consumers alike. Consumers benefit when companies can better target their advertising to their personal interests and background (reducing search costs) and companies benefit as targeted marketing improves their e-commerce return. Also, improving advertising effectiveness means more significant web services can be made available without charge.

Furthermore, costs of compliance can have the potential for vastly negative effects. If the EU Directive on Data and Privacy were enacted in the United States, consumers would lose time and money saving practices. According to the Financial Services Coordinating Council, losses could amount to over \$16 billion worth of current financial services. [11] The study, done in conjunction with Ernst and Young, assumes that the financial services would require “opt-in” policies and that less than 10 percent of consumers would allow their personal data to be used by the often unacknowledged intermediary institutions used in electronic transactions. “US consumers have come to rely on the savings and conveniences that result from information sharing by financial firms. These conveniences are being threatened by proposals on the federal and state level to adopt laws patterned on the EU directive,” says Jim Pitts, executive director of the FSCC’s Privacy Project. [11] The same can already be said for many EU companies (explored below). Lastly, the centralized legislation of the EU carries the great risk of its law excluding businesses from exchanging personal data with outside companies. To protect against businesses using nations outside Europe to store data and circumvent the EU Directive, Article 25 provides

limitations on the negotiations European companies can have in such exchanges. This, however, creates a discouraging barrier to sharing information with European partners. Though somewhat eased by the recent “safe harbor” compromise, abiding by EU mandates still persists as an economic disincentive in dealing with European businesses. In a global economy only accelerated by the Internet, restrictions on the flow of personal information hurt the effectiveness of doing business.

Documented Results

A survey of Britain’s top 200 consumer companies found that most were breaking the law banning the use of e-mail for sending unsolicited marketing offer to non-customers which fails to comply with the EU Directive and its requirement that firms can only send unsolicited sales emails to non-customers if they have opted to receive them. [12] Essentially, by limiting the freest flow of information many business practices (including offered services utilizing undisclosed third parties and means of attracting new customers) are ruled illegal to the economic detriment of the EU. Strict comprehensive legislation with strict rules on the flow of information cannot offer the flexibility necessary for addressing every use of personal data including those uses that benefit the consumer. The end result is restrictive and disadvantageous for those under the policy. This is moreover exemplified in problems arising from globalization. Effectively, when companies in other nations can offer consumers better targeted ads, improved services, and have better techniques to attract consumers, policy legislation like that of the EU Directive puts the companies and economies of nations under it at a competitive disadvantage in the global marketplace, especially important when factoring in the increasing role of the Internet in commercial transactions.

Enforceability

The Directive specifically mentions various mechanisms to be used in implementation of the stated privacy objectives. Significantly, it enforces that each Member State enacts legislation to

address and fully implemented the four information privacy principles mentioned above. Moreover, it requires the establishment of one or more public authorities to oversee the enforcement of the personal data protections, including that each should “act with complete independence,” have investigative powers, and have “effective powers of intervention,” and the power for court action where national legislation implementing the directive is obstructed. [3] Additionally, the Directive allows for the individual rights of enforcement and requires citizens be granted the right to pursue a judicial remedy for the breach of a Member State’s national law regarding information privacy and the right to recover compensatory damages. [3] Lastly, the Directive creates supra-national administrative supervision of Member States which is distributed between the EU Commission, a Committee of representatives of the EU Member States, and an advisory working party of the national data protection authorities.

Overall Implication for Privacy Protection and Data Sharing

Privacy is a trade-off. Strict, centralized legislation results in more notices and forms, increased prices, fewer services for free, and reduced convenience. Generally, laws regulating privacy are often burdensome and have the societal effect of chilling innovation and the creating of beneficial collective goods. But, legislation like the EU Directive does allow for standardization and the resolute preservation of the individual’s right of privacy. The result of this being that the nations under EU can that much more efficiently operate while citizens can additionally trust European business facilitating greater electronic commerce. Furthermore, privacy can be seen as innately valuable and a crux for the free society. Taking measures to safeguard against abuse is a precaution against human abuses. Overall, measuring the true effectiveness of this form of legislation is riddled with uncertainty about the metric upon which the right to privacy is to be measured. In the effectiveness of centralized legislation in achieving its stated goals, it clearly catalyzes a comprehensive framework requiring a minimum, enforced standard for protecting privacy. However, information flows in subtle and nuanced ways and enforcing privacy

essentially restricts the free information flow. While standardization promotes data exchange within the EU, it creates potential obstructions to data sharing in the global market. Between this and the stifling of many digital business practices, the economic outcome likely places EU companies at a disadvantage. On the other hand, privacy as a core cultural and social value is catalyzed.

03 Approach: United States Sectorial Legislation

Need

Contrary to European cultural values yet similarly derived from historic motivations, Americans tend to have more trust for the private sector and place their confidence in the free market to protect personal privacy while instead fearing privacy invasion from the government. Starting in the early 1970s, awareness over large amounts of personal information being aggregated by the government about individuals prompted growing public concern over privacy protection. This eventually led Congress to enact legislation to protect individual privacy and to guarantee access to collected data through the Privacy Act of 1974 and the Freedom of Information Act. However, while both provide comprehensive protection against public sector threats, they do not apply to the private sector. In a report from Privacy Study Commission resolved that participatory data protection schemes and self-monitoring were appropriate for the US companies. Privacy legislation in the U.S. has resulted in a decentralized approach to personal information protection in the private sector. Thus, privacy legislation in the private sector comes from industry-specific laws and guidelines that develop when need arises as the result of a problem.

Goals

The marketplace for personal information and web services is big business. It is the goal of American privacy legislation to leave the market unimpeded by legislation while upholding quite specific – often technology-specific – privacy protections. As long as the objective of preserving

the privacy of citizens against government intrusions is maintained, most other privacy concerns are left to the market to value privacy.

Informed Philosophies

Even though privacy is not explicitly protected under Constitution, Americans have traditionally considered privacy a valued right which the Supreme Court has stated is among the “penumbra” of rights as implied. Through the Privacy Act, the “fair information principles” were established focusing on the government’s use of personal data; however, even without legislation or enforcement mandating that the private sector adheres to these guidelines, they nonetheless have become the benchmark by which privacy advocates evaluate private sector data collection. Essentially, most privacy legislation is of the philosophy that citizens principally need protection from the government while maintaining, as stated by the Federal Trade Commission, that “self-regulation (in the private sector) is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology.” [4]

Example

Only in American can a company get in trouble for sharing data with its government. Discount airline JetBlue learned this the hard way when, in the fall of 2003, a group of passengers jointly filed a class action lawsuit against the company claiming breach of contract, invasion of privacy and fraudulent misrepresentation. "In the wake of the Sept. 11 attacks, and as New York's hometown airline, all of us at JetBlue were very anxious to support our government's efforts to improve security," later apologized David Neeleman, JetBlue CEO. Similar airlines are facing identical lawsuits. With the fear from 911 fading, Americans return again to their suspicion of the government. At such public outcry concerning insecure personal information or the perceived threat from an invasive government, private sector data protection has often brought about specific statutes including the Fair Credit Reporting Act, Cable Communication Policy Act, and

Video Privacy Protection Act among others.

Advantages & Promise

The promise of US sectorial legislation is that the marketplace will protect privacy as fair information practices regarding personal information is of value to customers. In effect, industry will protect privacy in its desire to gain consumer confidence and to maximize profit. The advantages from market-driven protection without restrictive government interference provides are that great flexibility is achieved for dynamically developing technologies. This encourages both innovation and the free flow of information.

Costs & Risk

In the United States alone last year over 10 million individual were the victims of identity theft and thousands on new privacy-related bills were introduced in state legislatures and Congress concerning the issue. The demand is present for a federal comprehensive approach to establish a minimum data protection baseline standard in the fight to better protect consumers and business from such staggering losses. Additionally, many recent surveys have indicated a raising concern and distrust on behalf of U.S. consumers over using the Internet for commerce. The rampant exploitation of personal data and many a public information protection failure are hurting the U.S. Economy through the cost of fraudulent transactions and losses due to a perceived disincentive not to use the Internet for commerce. Furthermore, the complex, patchwork state of current federal and state laws involving data and privacy compliance lacks consistency. Its complexities are confusing for businesses and consumers alike and makes doing business across different areas of the country an entangled, often contradictory affair where activities legal on in one jurisdiction may be illegal in the next. Huge costs are associated with legal compliance which is disadvantageous for businesses, especially in electronic commerce, and these incurred costs are often passed onto the consumers. The lack of a comprehensive legislative framework not only

hurts security and is costly, but it also impairs the consumer's understanding and control about how their personal information is being used.

Documented Results

Hundred of lawsuits have been filed against companies alleging violated privacy rights regarding the use or sharing of personal data. "The latest figure is \$125 million recovered in lawsuits from companies," says Alan Westin, Professor of Public Law & Government Emeritus at Columbia. [15] The complexity and proliferation of American law regarding privacy protection is placing a huge burden in the operations of business with a national or global reach. "We have scores, maybe thousands, of laws in the United States on the federal and state level, as well as millions of contracts and as many if not more information or administrative requirements on letters from government services," emotes Alan Goldberg, former president of the National Health Lawyers Association. To quantify this, a study by the IBM and the Ponemon Institute found that some US companies spend more than \$22 million annually on privacy. Moreover, the great cost of addressing privacy in the United States does not attribute to improving security. In fact, the lack of mandated data protection standards may be making things worse. The FTC Commission reports that increasing identity theft in American has amounted to a totaled \$5 billion loss for consumers and an additional \$48 billion loss for financial institutions and retailers. [15] In a recent example, ChoicePoint, a data broker, lost \$11.4 million through the first half of 2005 after its system was breached by hackers releasing personal data. The media actively jumped on the story and combined with the many other similar stories, a sense of insecurity prevails in consumers where fear exists that databases containing their personal information may be breached when they did not even know the company had this information which they have no control over. According to the Identity Theft Resource Center, identity theft costs the individual an average of 600 hours to clear his name. [6] Privacy protection in the United States works on the system of problem and response where in this case, following the lead of California's Security

Breach Information Act (SB 1386) requiring customer notification when their information is compromised or lost, more than 30 additional states have adopted like disclosure laws.

Enforceability

Categorically, these principles today operate through statutes, constitutional protections, and common-law remedies. The Privacy Act of 1974 established the tenets for fair information practices: transparency, individual participation, scope limitation, relevancy, and internal use limitations, no external disclosure without consent, reasonable protective security, and record keeper accountability. However, the law provided no assessments and no administrative process to control personal information use and most decisions about “routine use” were left to the agencies. Vagueness, political pressure, and a lack of oversight and enforcement vastly diminished the impact of the Privacy Act which subsequently failed in protecting personal records from significant computerized manipulation, distribution, and matching. Furthermore, a number of constitutional case examples showcase the absence of any clear right of information privacy in the constitution. While privacy interests against some forms of government intrusion are clearly attained, the Court repeatedly attests that the Constitution offers no protection against the access or use of personal information by private parties. Hence, with no constitutional basis, it is doubtful the Supreme Court will ever uphold any general notion of a constitutional right to privacy. Within common-law remedies, the commonly recognized privacy torts are: intrusion upon an individual’s seclusion or solitude, public disclosure of private facts, placing an individual in a false light highly offensive to a reasonable person, and the un-permitted use for private commercial gain of a person’s identity. It is questionable; however, how well privacy torts cover the manipulation, use, and disclosure of personal information as the scope of any provided relief does not meet the overall objectives of the code of fair information practices. In the context of modern information technologies, these privacy torts are a band aid on the shotgun wound as the commercial exchange and manipulation of personal data exists beyond the reach of present tort

law. Common law shall most likely prove ineffective in responding against the broad threats against personal information. Privacy threats from the both the government and the private sectors have increased while these records are playing a more important role in the lives of individuals. Thus arises the need for legislation to enact a code for fair information principles. However, if we are to learn from the past, the cornerstone of privacy law is establishing independent oversight and enforcement. [14]

Overall Implication for Privacy Protection and Data Sharing

The benefit of sectorial legislation is to increase data sharing permitting improved services, better advertising, innovation, and increased data flow. The trade-off is the lack of recognizing privacy as an individual right in addition to overall weaker protections and substantial costs derived from legal complexity. The effectiveness of U.S. legislation is questionable when fragmented and narrowly targeted laws cause as much trouble in compliance as they do in permitting the free flow of information. Moreover, this legislation may likely not achieve its goals in the private sector because marketplace protections fail when data brokers value personal information more than consumers do making exploitation profitable.

04 Approach: Self-Regulation

Need

The need for self-regulation arises from the lack of an enforcement mechanism for protecting personal information and privacy. Many US companies, for example, realized a lack of regulation was the chief concern of EU officials and companies in matters regarding electronic commerce and the exchange of data. In response, government agencies and corporate officials voluntarily began participating in business-backed programs in self-regulation practices. Today many self-regulation schemes exist. The most popular perhaps taking the form of a third party which grants its “seal of approval” to websites that comply with industry standards and presents a “fair” privacy policy.

Goals

These aforementioned seals of approval can be revoked when a website violates its proclaimed privacy policy. The goal of self-regulation is to allow for industries and companies to demonstrate a willingness and ability to hold themselves accountable for violations of their own privacy policies. Legislative clout was given to support this ideal when the FTC bolstered the enforcement of Section 5(a) of the Federal Trade Commission Act which prohibits unfair and deceptive company privacy policies.

Informed Philosophies

Self-regulation functions at a broad industry level through the associations of websites. It allows companies to be flexible with their particular privacy policies under the philosophy this promotes an efficient approach to addressing privacy issues. This allows the oversight of websites but maintains the ability of industry experts and privacy specialists to tailor requirements. Seal programs, industry guidelines, professional associations, safe harbors and all represent implementations of self-regulation.

Example Case

Lacking a clear legal privacy framework, the E-Loan positioned itself as a company with a more than average sensitivity to privacy concerns. E-Loan, like many others in the industry, outsources some of its backend data processing to India. Uniquely though, E-Loan gives its customers the option to control whether or not their loan application data goes offshore. Customers concerned about Indian privacy protections can check a box marking the individual's application for processing within the United States. This philosophy of openness over how customer data is processed is in fact apparent throughout their website and online application process. "Beyond legal requirements, privacy is an expectation of our customers," states an industry member, "If we say we meet the requirements of the law, many customers would tell us that's not good enough."

We approach it from a customer-first standpoint." Effectively, E-Loan offering its customers options over how their data is handled is the decision to make privacy a point of competitive differentiation. [13]

Advantage and Promise

The example of E-Loan showcases that the act of being upfront and clear in explaining a privacy policy can ease public concerns over personal data. Even though individuals using E-loan had the opportunity to opt out of data outsourcing; however, over 80 percent choose to opt in. [13]

Essentially, the punch line is that if a company clearly informs people what they are going to do with personal information, and abide by those statements, that the company essentially gains efficiency and customer trust. The promise is that brand value can be created through the honest representation of practices through their privacy policy. President Clinton advocated such for the United States private sector practices in his 1997 "Directive on E-commerce" pronouncing: "For electronic commerce to flourish, the private sector must lead. Therefore, the Federal Government should encourage industry self-regulation wherever appropriate and support private sector efforts to develop technology and practices that facilitate the growth of and success of the Internet." The advantage of various self-regulation schemes is that it promotes efficiency in addressing new privacy issues, allowing companies to customize their policy to their own practices, and self-regulation promotes the honest presentation of personal information handling to consumers. This is economically beneficial as companies are not subjected to unnecessary, non-adaptive legislative restrictions and also societally beneficial as it upholds privacy as a valued public interest.

Cost & Risk

Self-regulation schemes often involve business-backed third parties which are of a direct financial cost to its participants. Much more concerning, however, are the other problems of self-regulation: lack of participation and lack of meaningful enforcement. In terms of seal programs,

the two most popular ones (TRUSTe and BBBOnline) have only a combined 1,050 participants. [3] In a 1999 study, only 20 of the leading 100 electronic commerce sites participated in either of these two programs. [3] Essentially, self-regulation simply fails to provide a comprehensive solution to privacy. Furthermore, self-regulation often fails to guarantee the quality of stated privacy policies and lacks an effective enforcement mechanism. At most, these programs can revoke a seal producing negative publicity but can exert no direct punishment. Moreover, self-regulation schemes that require a third party are often only as effective as that party's oversight. TRUSTe has failed on multiple accounts to take action against high profile complaint cases. Third parties often lack the investigative means for proper oversight or it is simply not in their interest to provide sufficient oversight as their paying customers are the potential privacy policy offenders. Cost, lack of participation, lack of enforcement, lack of proper investigative powers, and bias all diminish the effectiveness of self-regulation.

Documented Results

Many privacy pioneers see privacy as an opportunity. Procter & Gamble, Hewlet-Packard, and Nationwide Mutual Insurance among others have gone beyond mere legal compliance regarding protecting personal information in the belief that valuing privacy will build the brand and therefore shareholder value. In an attempt to quantify this effect, Peter Cullen, now Microsoft's chief privacy strategist, worked with Royal Bank of Canada to demonstrate that privacy actually contributed seven percent to the institution's overall shareholder value. [13] Moreover, Sandy Hughes, Procter & Gambles chief privacy officer, says research indicates that half of the customers that visit a website and read the privacy policy will leave the website if they do not like the statement—"Having consumer trust is good business for us. Our whole privacy program is built on that. If we just want to satisfy the letter of law, we'd have a different program. But we see it as a competitive advantage." [13]

Enforceability

Many self-regulation programs lack the means, and sometimes the incentive, to provide meaningful enforcement. While some of the major programs have a violation claim investigative process and offer conflict resolution, little redress is available in the event of a violation. Negative publicity is often the only consequence.

Overall Implication for Privacy Protection and Data Sharing

Self-regulation seemingly offers an efficient solution to addressing privacy concerns; however, the comprehensive fair information practices purported by many self-regulation schemes are meaningless if participants are not held to their agreement. The trade-off is flexibility versus enforceability. The effectiveness of self-regulation in achieving its goals is unlikely when lack of accountability and bias undermine necessary and proper oversight. Self-regulation alone is likely insufficient in protecting privacy interests.

05 Conclusion

Whereas the European approach is proactive, the United States approach is reactive. This represents a fundamental difference in perspective on the theoretical right to privacy and has implications for the effectiveness of legislation guided by these foundations. In balancing privacy rights with economic and societal needs, EU centralized legislation succeeds in upholding security, confidence, and privacy as an unassailable right but fails economically by disadvantaging itself through restrictive legislation which undercuts innovation, hinders the flow of information, and also fails in meeting the demands of a global marketplace for data exchange. United States legislation succeeds in protecting itself from government intrusion and encouraging innovation and new web services through minimal, narrowly-defined privacy protection legislation, but fails to assert a baseline standard for protection hurting overall security and exerting great costs to companies and consumers through excessive compliance costs due to the fragmented nature of its sectorial laws. Self-regulation attempts to balance protection with

flexibility by almost entirely fails to be enforceable. Comparatively, the EU centralized legislation is highly enforceable and United States in enforceable against government but lacks the necessary oversight to enforce privacy in the private sector. Essentially, none of these approaches have proven to be practical as either enforceability proves to be a problem or their regulation comes with significant economic or social sacrifices. Additionally, by the EU being so forthright in its declaration of privacy as a right it has favored continued protection and abilities regarding personal identity and personal data in the digital age; however, the opposite is true with the US which shall continually be playing catch up to technological threats where legislation only comes with blatant public concern. Public policy today is determining the architecture of information flow and must protect not only individual privacy but promote the development of new individual, collective, and societal benefits. Enacting legislation over privacy in the digital age means analyzing the trade-offs involved in regulation including both the benefits and the costs. The result cannot be too broad in nature or too narrowly defined, and it must be backed by effective oversight and due enforceability. Privacy legislation must reflect an appreciation for this incredibly complex technological and social phenomenon. In time, through the efforts of the public, lawmakers, business, and regulators, it can be hoped the extremes of today's forms of regulation might be tempered and that with the continued critiquing of the effectiveness of each that eventually a combination of all might best uphold public interest.

06 References.

- [1] Heydrich, Michael (1999), "A Brave New World: Complying with the European Union Directive on Personal Privacy through the Power of Contract," Brook International.
- [2] Samuelson, Pam (2003), "Social Costs of Incoherent Privacy Policies," <http://www.almaden.ibm.com/institute/pdf/2003/PamelaSamuelson.pdf>, IBM Almaden Privacy Institute
- [3] Strauss, Jared, et al (2004), "Policies for Online Privacy in the United States and the European Union," Conference Paper, Duke University.
- [4] Sun, Chuan (2003), "The European Union Privacy Directive and its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective," *Journal of International Law*.
- [5] Long, William, et al (2002), "Personal Data Privacy Protection in an Age of Globalization: the US-EU Safe Harbor Compromise."
- [6] Grupe, Fritz, et al (2003), "Dealing with Data Privacy Protection: An Issue for the 21st Century", *Law, Investigations, and Ethics*, January 2003.
- [7] Loring, Tracie (1999), "An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States", University of Texas School of Law
- [8] Microsoft (2003), "Microsoft addresses the need for comprehensive federal data privacy legislation," <http://www.microsoft.com/presspass/features/2005/nov05/11-03Privacy.msp>
- [9] CDT (2005), "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," http://www.cdt.org/privacy/eudirective/EU_Directive_.html.
- [10] Reidenberg, Joel (2000), "Cyberspace and privacy: a new legal paradigm? Resolving conflicting international data privacy rules in cyberspace," *Stanford Law Review*.
- [11] Johnston, Margret (2001), "Study: EU Privacy directive would cost US consumers," *IT world*, <http://www.itworld.com/Man/2688/IDG010501euprivacy/>
- [12] Gow, David (2005), "Third of top companies break email privacy laws," *The Guardian* (London).
- [13] Millman, Gregory (2004), "Keeping data under lock & key," *Financial Executive*.
- [14] Paragraph derived from my original summary of Robert Gellmans' article "Does Privacy Law Work?"
- [15] Cisco (2005), "Preventing Identity Theft through Privacy Architecture," http://www.cisco.com/web/about/security/intelligence/05_09_Identity-Theft.html