International Journal of Communication 3 (2009), 169-187 1932-8036/20090169

U.S. and EU Privacy Policy: Comparison of Regulatory Approaches

LAUREN B. MOVIUS
University of Southern California

NATHALIE KRUP
University of Southern California

While the Internet can be viewed as a global network of networks, many elements of Internet law remain delineated by sovereign nations, creating the potential for regulatory conflict and spillover. In particular, national governments have different views on the regulation of private information, and to whom it should be available. Concerns arise about how personal data and identifiers should be handled on the Internet. The U.S. and EU are each other's largest trading partners yet follow vastly different approaches in their respective attempts to regulate personal information and the digital economy. This article explores the cross-border variation in privacy policy in the U.S. and EU and discusses how differences in countries' values, social norms, and interests account for the variance in regulation. Distinct regulatory approaches and priorities between the U.S. and EU profoundly affect numerous industries in both regions. The article analyzes the example of passenger name records in the travel industry as a case study in this privacy policy contrast.

Keywords: Data privacy, privacy policy, EU Data Directive, U.S. Patriot Act, Passenger name record

The digital networked age is characterized by the increasing availability and pervasiveness of electronic communication products and services. These advancements, epitomized by the Internet, can greatly increase the speed and efficiency of transactions to catalyze productivity and economic growth. The U.S. Federal Communications Commission (FCC) states, "The Internet plays an important role in the economy, as an engine for productivity growth and cost saving" (FCC Policy Statement, 2005). Commercial transactions and e-commerce have significantly risen on the Internet. Because much of e-

Lauren Movius: **lmovius@usc.edu**
Nathalie Krup: **NKrup@magid.com**
Date submitted: 2008-09-08

Copyright © 2009 (Lauren Movius & Nathalie Krup). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at http://ijoc.org.

commerce is concerned with the exchange of information, the problem of data protection and privacy comes into play.

With e-commerce, global dataflows via the Internet may appear to dissolve national borders, yet territorially defined jurisdictions and regulations still exist. While the Internet can be viewed as a global network of networks, national governments have different views on the kind of information that should be lawfully available and regulate accordingly (Goldsmith & Wu, 2006). Concerns arise about how personal data, including age, sexual orientation, religion, financial status, medical records, and identifiers like credits cards, driver's licenses, passports, Social Security and bank account numbers should be handled, and by whom. Although explicit definitions of privacy vary according to context, privacy and data protection are typically interpreted in terms of standards for the treatment and dissemination of the aforementioned types of personal information.

The desire to safeguard personal information is not a new phenomenon. However, digital technology affects privacy in new ways by making it easier and cheaper to collect, search, store, aggregate, and market information. As more online transactions are conducted via more networks, new electronic privacy problems have emerged in this networked environment. For example, there has been a recent increase in the use of "cloud" computing, whereby public and private organizations consign their consumer data to third parties for storage and securing. Client information is permanently stored in Internet servers and cached temporarily (Hewitt, 2008), a development which has recently entered public debate in terms of security and privacy concerns (Economist.com, 2008). While the "cloud" is in some ways "the ultimate form of globalization," with data floating freely within, nations seek control through regulation (Economist.com, 2008).

The issue of national sovereignty and control of data protection is exacerbated by the Internet, as personal data easily crosses borders in digital form. There is a tension between the economic space of transborder dataflows and the territorially-based jurisdiction of national regulation of data privacy. Dataflows reside in a network and a "space of flows," not a "space of spaces" (Castells, 2000), whereas state regulation is bound by geography. Certain characteristics of the Internet appear to make this technology borderless, leading libertarian thinkers in the 1990s to suggest that the Internet could not be controlled and would inevitably erode national authority (Barlow, 1996). However, many elements of our geo-political global makeup, especially legal systems, remain delineated in terms of sovereign nations, and nations do indeed regulate the Internet (Goldsmith & Wu, 2007; Wilske & Schiller, 1997; Wu, 1997). This creates an inherent contradiction, exacerbated by the vastly different approaches nations employ in their attempt to regulate the Internet and e-commerce.

Regulatory Spillover

Whereas the European Union has proactively regulated uses of personal data, the United States has refrained from regulation to protect personal data (Fromholz, 2000; Schwartz & Reidenberg, 1996). Regulatory differences become problematic, however, when countries face a cross-border spillover. Regulatory spillover occurs when the impact of regulation is not limited to the originating jurisdiction.

Unilateral national Internet regulations may affect both the Internet activities of users in other jurisdictions as well as the regulatory approach of other nations (Goldsmith, 2000).

Regulatory spillovers and differences in policy create wasteful bureaucracy, confusion, and inefficiencies for countries and companies involved, as well as for the public. Excessive regulatory spillover in the U.S. and EU could disrupt both economies. The potential for harm lies in the fact that the U.S. and the EU enjoy the world's largest bilateral trade relationship. Such trade and investment demonstrate a high degree of interdependence between the two economies. In 2006, the 27 countries in the EU exported EUR269 billion of goods to the U.S., while total U.S. imports amounted to EUR178 billion (EC Directorate General for Trade, 2007). According to the U.S. Trade Representative, transatlantic trade amounts to approximately US$2.15 billion every day, and, jointly, EU and U.S. global trade accounts for almost 40% of international trade (EC Directorate General for Trade, 2007).

Moreover, e-commerce is an increasingly important component of this transatlantic trade and investment, and indeed the global economy. Regulatory spillovers between the U.S. and EU in this digital environment pose challenges to government and private actors on both sides of the Atlantic. Privacy protection on the Internet is one such issue demanding attention. As discussed more thoroughly below, e-commerce naturally involves the collection and exchange of information and can include profiling. The Federal Trade Commission noted that in 2000, 97% of Web sites collected personal identifying information about consumers. The ubiquity of the Internet and collection of electronic data increases the potential for data privacy to be compromised. Clearly this is dependent on the particular definition of privacy.

Conceptions of Privacy

The Universal Declaration of Human Rights Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." However, the legal protection of privacy varies greatly around the world. In many contexts, the concept of privacy has been combined with data protection, which understands privacy in terms of management of personal information. Data privacy is never considered in a vacuum; it "is always considered in a specific social, political, economic, cultural and historical context (Kobrin, 2004, p. 115). Thus, we now compare the conceptions of data privacy in the European and American contexts.

The Right to Privacy: The European Approach

Different privacy norms in the U.S. and EU can be seen as the result of fundamental differences regarding the role of government and the commercial sector. On the whole, the European approach to corporate governance requires close participation between business and government to achieve public tasks. Government is seen as an active partner along with the major industry participants, discussing regulatory and public interest objectives and strategies to attain them. Moreover, European decision makers have tended to see a wider role for the state in addressing social problems. In contrast, U.S. decision makers have typically favored a more laissez-faire approach to corporate governance and emphasize the role of private actors and market forces in ameliorating societal challenges (Farrell, 2003).

Our depictions of these competing approaches are abstractions of complex and dynamic policy sets that are better conceptualized in their entirety as relative points on a spectrum as opposed to polar opposites.

European attempts to regulate privacy also stem from their concept of privacy. Europeans appear to consider privacy a fundamental human right, which the government is responsible for providing to its citizens. The right to privacy is explicitly mentioned in Constitutions of many EU countries, including Germany and Spain, and in the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms. The Treaty to establish a Constitution for Europe explicitly states the necessity to strengthen the protection of fundamental rights in the light of changes in society and technological developments. Article 8 of the European Convention on Human Rights guarantees the right to respect for private and family life, one's home, and correspondence. Historically, data protection is grounded in the attempts of European countries to control improper use of personal data (Flaherty, 1989). Still healing from memories such as the Nazi's Gestapo and the Soviet's KGB, Europeans remain highly sensitized to the collection of personal data files (Bach, 2001).

The European approach is likely to question the ability of free markets, as compared to legislation as an appropriate solution to societal concerns (Fumholtz, 2000). The value of using information to promote consumer commerce is less important in the EU than in the U.S., which has a more consumer driven economy. For example, stores in the U.S. often have extended hours, while EU retailers may face strict limitations on hours of operation (Walker, 2004). Statistics show that the EU has approximately one credit card per four people, while the U.S. has 2.25 credit cards per person; EU savings exceed 10% of disposable income, while average U.S. savings come from current income and may be near zero or negative when financed by borrowing (Bureau of Economic Analysis, 2008). Until the 2007 housing and credit meltdowns, much of America's wealth was invested in housing equity. Currently, a large and growing proportion of Americans have mortgage debt exceeding the value of their property. Again, it is important to note that the EU and the U.S. are both far from monolithic. For example, the UK economy and government regulatory approach, particularly in terms of the examples provided in this paragraph, are closer to the U.S. condition than most EU countries.

The EU Data Directive

The EU Data Protection Direction represents the current focus of privacy discussions in Europe. On Oct. 25th 1998, the EU passed a comprehensive Data Protection Directive that applies to the processing of personal information in electronic and manual files. The Directive sought to harmonize the then 15 member states' laws in providing consistent levels of protections for citizens and ensuring the free flow of personal data within the EU, promotes European-wide commerce, and sets a baseline common level of privacy that not only reinforces the current data protection laws, but also establishes a range of new rights. The Directive assumes the existence of cross-border dataflows and attempts to protect the data privacy rights of Europeans regardless of where data are transferred and processed (Kobrin, 2004). Article 25 of the Directive mandates that member states ensure personal data relating to European citizens is protected when it is exported to, and processed in, countries outside Europe. It states:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection

with adequacy of level of protection

> assessed in the light of all the circumstances surrounding a data transfer operation; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country. (EU Data Directive)

Recognizing the importance of trans-Atlantic e-commerce, and the relative lack of "adequate" privacy protection from the U.S. in particular, the EU included a list of "derogations," or exceptions, under Article 26, by allowing the transfer of data to countries where protection has not been deemed adequate in hopes to cover everyday information transfers, such as passenger travel information. It soon became apparent that U.S.-EU commerce and dataflows would not be assured on the basis of Article 26 exemptions alone, and that the European Commission was not going to accept the existing American self-regulatory regime as adequate. In 1998, negotiations began between David Aaron, the U.S. Under Secretary of Commerce for International Trade, and John Mogg, the European Commission Director-General for Internal Market, which ultimately resulted in the creation of Safe Harbor Agreements (Farrell, 2003). The Safe Harbor Agreement was adopted in May 2000, and requires compliance with seven principles: notice, choice to opt out, notice and choice to opt out when transferring to third parties, access to one's information, protection and security of personal information, data integrity, and enforcement. The U.S.-EU Safe Harbor is a streamlined process for U.S. companies to comply with the EU Directive. U.S. firms handling personal data of EU citizens could voluntarily sign up in order to avoid EU sanctioning. Thus, firms that signed up for the Safe Harbor are considered to be providing "adequate" protection for the data of EU citizens.

Neither side of the Atlantic was impressed by the Safe Harbor Agreements. Europeans believed it could not come close to offering truly adequate levels of protection, while U.S. firms believed implementation and operation would be too costly (Kobrin, 2004). The Safe Harbor negotiations illustrated the "deeply rooted differences in historical experience, cultural values, beliefs about the organization of the polity, economy and society" (Kobrin, 2004, p. 116). Specific problems arose with regard to transparency and enforceability of privacy policies, clarity of onward transfers, and the status of third parties (Dhont, Asinari & Poullet, 2004). These regulatory inconsistencies contribute to organizational inefficiency and the growing regulatory contention between the U.S. and EU over Internet privacy standards (Dhont et al., 2004).

The Right to Privacy: The U.S. Approach

Whereas the right to data privacy is heavily regulated in Europe, data privacy is not highly legislated in the United States. The history of privacy regulations in the U.S. has been one of industry self-regulation and reactive legislation. The U.S. traditionally follows a laissez-faire governance system where markets set industry agenda, and governments intervene only when the private sector fails. In many sectors of the U.S. economy, the role of the government has been to act as a latent rule maker of last resort.

The U.S. Constitution does not contain the word *privacy* and therefore the right to privacy is not guaranteed by the Constitution. The notion of privacy came from American lawyers Samuel Warren and Louis Brandeis' seminal 1890 piece on the right to privacy as a tort action, explicitly defining privacy as "the right to be left alone." This concept of the privacy tort gradually emerged as a part of common law across the U.S. and helped to shape the idea that privacy is a commodity and essentially a tool against the government (Bach, 2001; Privacy International, 2006). Privacy protection through statutory law in the U.S. is not well developed and is characterized as a "patchwork quilt" (Holvast, Madsen & Roth, 1999). Unlike the EU, there is no single overarching privacy law. That is not to say that federal legal cases have neglected the issue of privacy. In 1965, the U.S. Supreme Court judicially recognized an implicit right of the individual to privacy in relation to the government in a case decriminalizing the use of contraceptive devices. This right was more famously relied upon in Roe v. Wade, which legalized first and second trimester abortions.

The first statutory protection of information privacy in the private sector was the Fair Credit Reporting Act of 1970. Other pieces of legislation emerged, responding to specific issues, such as the Video Privacy Protection Act of 1988, which protects data on video rentals; the Cable Television Consumer Protection and Competition Act of 1992, which regulated cable subscribers' name-linked data; and the 1998 Children's Online Privacy Protection Act, which limits the amount of information that can be gathered from children. Fromholz (2000) cites the above regulations as examples of the patchwork nature of U.S. privacy legislation, and notes the difficulty in comparing the network of U.S. laws to EU standards.

The U.S., aware of the importance of privacy protection in order for e-commerce to grow, continues to self-regulate within various industries. This U.S. perspective was encapsulated in the Clinton/Gore 1997 Framework for Global Electronic Commerce, which stressed that the private sector should take a leading role in e-commerce and Internet governance. Thus, the framework encouraged self-regulatory solutions to privacy concerns, and e-commerce was left to self-regulation insofar as was possible. Indeed, most U.S. businesses favor self regulation to government regulation, and companies have sought to regulate themselves through various mechanisms, such as industry codes, organizations such as the Online Privacy Alliance developed in 1998, and third-party privacy seal programs such as BBBOnline and TRUSTe (Fromholz, 2000).

This approach contrasts the EU approach to data privacy. Whereas in the EU, it is the responsibility of the government to protect citizens' right to privacy, in the U.S., markets and self-regulation, and not law, shape information privacy. In the EU, privacy is seen as a fundamental human

right; in the U.S., privacy is seen as a commodity subject to the market and is cast in economic terms (Kobrin, 2004). David Aaron, who negotiated the Safe Harbor, noted that in Europe:

> Privacy protection is an obligation of the state towards its citizens. In America, we believe that privacy is a right that inheres in the individual. We can trade our private information for some benefit. In many instances Europeans cannot. This can have important implications when it comes to e-commerce. (2001)

The U.S. Patriot Act

After the terrorist attacks of Sept. 11, 2001, the U.S. government called for increased surveillance in order to protect against other terrorist attacks. The key initiative which emerged to augment government access to domestic information was the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (U.S. PATRIOT Act). The act was introduced less than a week after the 9/11 attacks, signed by President George W. Bush, and passed into law Oct. 26, 2001. The Act has provisions expanding government investigative authority, including online information. Those provisions implicate constitutional protections of individual liberty, including procedures for interception of information transmitted over the Internet.

The Patriot Act strengthened capabilities in several areas including surveillance, search warrants, detention, restricted access money laundering, information sharing, and criminal penalties. In terms of surveillance, court oversight was reduced for wiretaps, email tracing, and tracking Web surfing. The Patriot Act enabled the FBI to subpoena computer records from ISPs and allowed law enforcement to use roving wiretaps. Under the Patriot Act, law enforcement officials have greater authority to monitor Internet activity, and technological advancements enable U.S. Intelligence Services to access multiple databases for foreign and domestic information, "relating to terrorism." The reorganization of information technology under Title VII entitles top American officials to access every source of information that may "lead to terrorism."

The Act, coupled with new investigative guidelines, has redefined the U.S. approach to personal privacy rights. Under section 215 of the Act, the government may now obtain any and all records with a business records order from the Foreign Intelligence Surveillance Court, which sits in secret and has denied or modified six out of more than 15,000 surveillance orders sought in a quarter century, a mere .004%. From 2006 to 2007 there was a 14% increase in court orders for eavesdropping, with judges approving 4,578 state and federal wiretaps, as compared to 4,015 in 2006 (Administrative Office of the United States Courts). Table 1 provides information on intercept requests each year from 1994 to 2007. While the consequences of expanded capacity for government access to personal information is incredibly far reaching, we focus on the privacy implications of the Patriot Act and subsequent legislation, with respect to passenger information protection.

Table 1. Number of Wiretap Applications, Authorized Intercepts, and Denied Intercepts as Reported in Wiretap Reports for Calendar Years 1994 – 2007. *(Administrative Office of the United States Courts)*

Year	Wiretap Applications	Authorized	Denied
2007	2208	2208	0
2006	1839	1839	0
2005	1774	1773	1
2004	1710	1710	0
2003	1443	1442	0
2002	1359	1358	1
2001	1491	1491	0
2000	1190	1190	0
1999	1350	1350	0
1998	1329	1327	2
1997	1186	1186	0
1996	1150	1149	1
1995	1058	1058	0
1994	1154	1154	0

Privacy Protection Paradigms

There are clear benefits to protecting privacy, but there are related costs as well. Privacy can impose economic and social costs; while privacy may protect some individuals, it may result in costs by preventing others from making fully informed decisions (Fromholz, 2000). As countries attempt to secure privacy protection for their citizens, they move along a privacy continuum defined by two fundamental tensions. The cost of providing privacy protection can be described as a relinquishment of economic efficiency and security. Privacy protection can be conceptualized as a balance in continuous tension with the political and economic spheres. As governments create legislation, they are forced to prioritize amongst issues of privacy, security, and economic efficiency. The stance governments take with respect to these balances influences the workings of the two other. Governments can manipulate the tacit and explicit connections between privacy, economic efficiency, and security to achieve various goals. The economic tensions between privacy protection and economic efficiency and the political tensions between privacy protection and security will be explored in more detail.

The relationship between privacy protection and economic efficiency is manifested in various ways, as explained well by Hal Varian (1996). One tension is that buyers want sellers to know their taste and what product they want, thereby reducing search costs for the appropriate product. However, the buyer does not want the seller to know the maximum price that he is willing to pay for the item. Research suggests that when information about customers' tastes and purchase history is available and shared

among sellers, markets produce efficient outcomes (Acquisti & Varian, 2002; Calzolari & Pavan, 2001). The buyer benefits by targeted services reducing search costs, while the seller benefits from rectifying asymmetric information about buyers' preferences (Acquisti, 2004).

Privacy erosion allows sellers to know more about customers' willingness to pay, and to control arbitrage in which somebody who might face a high price from a seller buys instead from an intermediary at a lower price (Odlyzko, 2003). For instance, adjacent airline seats may be priced at $200 or $2,000, depending on conditions under which tickets were purchased and knowledge concerning the buyer. Odlyzko states, "Privacy intrusion represented by airplane tickets being non-transferable contracts with named individuals enables airlines to practice yield management in the extreme form it has reached" (2003, p. 356). In essence, the constant struggle between the information needs of a commerce driven economy and privacy protection illustrates an example of how this cost/benefit tension is evaluated.

A similar kind of tension is thought to exist between privacy protection and security. The general claim is that democratic societies seek to strike a "balance" between liberty and security, and that citizens must relinquish some degree of personal privacy for the sake of security. After the 9/11 terrorist acts and the "War on Terror," this issue of security versus privacy gained new prominence. Benjamin Franklin's claim that "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety" has been referenced numerously since 9/11 (Neocleous, 2007), echoing its popularity during the American Revolutionary period. Security and privacy are often discussed in a zero-sum paradigm. However, some have questioned the false dichotomy between privacy and security (Cavoukian, 2008; Schneier, 2008) and suggest that giving up privacy does not necessarily result in greater security, and greater security need not require a loss of privacy. The debate is often presented as security versus privacy, yet perhaps the real logic is liberty versus control.

National security tensions, or the balance between individual privacy and the handling of personal information collected by governments or any third party, has garnered much attention recently, especially in connection with the Patriot Act. While the collection of personal information and government databases can provide socially beneficial information about organizations and establishments (Duncan, 2004), tension arises when concerns are raised as to whom this information might be disseminated or how it will be used. Many of the extended powers granted to the U.S. government in the wake of the Patriot Act exemplify this debate and display just how heated the tension between privacy and security can become.

The Paradigm in Practice

The concept of privacy protection, its relative importance versus other social goods, such as security and economic efficiency, the roles of government and other organizations in protecting citizens, and implementing regulation vary dramatically across countries, even those as close as the United States and Europe (Kobrin, 2004). The regulatory disparities can be explained in part because governments impose regulations as a function of unique culture, social norms, political and economic philosophy as well as historical experience, and unique pressures and priorities (Kobrin, 2004). These issues, along with the different concepts of privacy in the U.S. and Europe as discussed above, contribute to distinct governance and regulation aimed at striking the privacy balance at particular points to capture distinct priorities.

The EU Directive exemplifies the privacy versus economic efficiency tension by illustrating Europe's tendency to privilege privacy protection at the expense of data access to information and economic efficiency. Research concludes that in Europe, concern for the protection of the rights of citizens, or data subjects, trumps the economic outcome of the market (Frumholz, 2000; Kobrin, 2004; Reidenberg, 2000). The Directive was conceived as an attempt to secure the fundamental right of privacy in all member states. The EU seemed willing to potentially risk huge economic losses from ceasing dataflows with countries, like the U.S., that did not provide adequate protection to European citizens' information.

Critics of the Directive claimed that the economy would stagnate, and there was an emerging sense that Europe was attempting to erect a trade barrier by keeping U.S. firms out of its lucrative markets for personal information-intensive services (Bach, 2001). Quick to point out potential economic losses caused by increased privacy protection, critics asserted that any firm operating within or receiving information from the EU would have to revise its data-handling processes. Firms would not be able to automate data collection from its customers and would be severely limited in their ability to offer personalized or targeted advertisements. Companies, regardless of location, would need to affirmatively gather consent, known as "opt-in," from all European customers and employees just to include their information in company e-mail or phone directories (Swire & Litan, 1998). Despite these potential costs, which increase as digital capabilities grow, the EU sought to grant individuals rights over their personal data.

The U.S. conceived the Patriot Act with the intent of increasing national security and consequently revoked some degree of privacy protection for its citizens. This level of domestic protection evaporated on September 11, 2001 when two major American cities became targets of acts of terrorism and greatly affected the national psyche. This backdrop virtually ensured that in the balance of security versus privacy, U.S. authorities would err in favor of the former. Additionally, the historically reactive regulatory regime of the U.S., along with the traditional view of privacy as a commodity, made the U.S. a much more fertile ground for the adoption of legislation which favored national security over privacy. Technical and complex changes to surveillance laws, detention regulations, and government guidelines that disregard traditional checks and balances and ultimately increase government secrecy, favor hopes of national security over privacy protection.

However, we must note that the impacts of the events of Sept. 11, 2001 and the Patriot Act brought about corresponding policies in other countries. Lyon (2004) notes two surveillance areas affected in the aftermath of 9/11. The first is how governments have proposed measures to deal with the terrorist threat, such as Smart ID cards and various biometric devices. The second "surveillance consequence of 9/11" is the proliferation in various countries around the world of anti-terrorist legislation, which tend to relax limitations of prior laws on wiretapping. Lyon argues that surveillance is an increasingly globalized phenomenon. Indeed, a shift has taken place in the political and legal landscape of many counties around the world which introduced legislation to aid their ability to fight terrorism following the 9/11 terrorist attacks. Such legislative measures all tend to increase surveillance of communications, intensify data sharing, and increase identification schemes. For example, France passed 13 anti-terrorism measures on Oct. 31, 2001, the United Kingdom passed the Anti-Terrorism, Crime and Security Act on Dec. 15, 2001 —

since replaced by the Prevention of Terrorism Act 2005; Belgium in December 2003 enacted legislation outlawing any action with the purpose of "destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country" (Cohn, 2004); and Canada passed their Anti-Terrorism Act on Dec. 18, 2001. In 2008, the EU has been working on enacting legislation to combat terrorism, but, in contrast to the U.S. Patriot Act, there appear to be checks and balances in place to protect public freedoms and ensure that these freedoms do not pay the price for an increase in public security. Members of the European Parliament insisted on including rules for the processing of persona data, out of concern that "the cure should not be worse than the disease" (EurActiv.com, 2008). Thus, European policy makers have considered the impact of legislation upon civil liberties, a discussion which did not seem to occur with the quick passage of the Patriot Act.

The Travel Industry and Passenger Name Records

This article focuses on conflicting privacy regimes of the U.S. and EU, with a case study of the travel industry to illustrate these contrasts. Distinct regulatory approaches and priorities between the U.S. and EU affect numerous industries in both regions. As the U.S. and EU economies become increasingly linked through trade and the processes of globalization, the impact of conflicting regulatory regimes increases. Regulation and trade disputes occur over issues from the environment to food safety to taxation of e-commerce to privacy concerns. Policy differences are exacerbated not only by the very nature of international travel — an individual physically changing jurisdictions — but also by the contrasting requirements concerning privacy protection of passenger data between the U.S. and EU. It is easy for most to see why medical and financial data are legally recognized as posing certain privacy issues and afforded protection. With travel data, some may argue that such records are simply a category of commercial transaction data. However, many privacy issues regarding travel data are at stake. Specifically, much controversy focuses on the collection and maintenance of Passenger Name Records (PNRs). We will first discuss Passenger Name Records and then analyze governmental regulation, and hence regulatory spillover, and commercial practice in this area.

PNRs include extremely detailed personal information from numerous sources, added through different channels over time. This results in a PNR history, or a traveler profile, which includes: regularly used credit cards; alternate addresses, phone numbers, and emergency contacts; names and other information of family members or business associates who have traveled with the individual; tastes and preferences — e.g., "prefers room on low floor in hotels," "always requests halal meal," "won't fly on the Jewish Sabbath," "uses wheelchair," "prefers not to fly Delta Airlines"; department and project billing and approval codes for corporate travel; and frequent flyer or loyalty customer numbers (Hasbrouck, 2007). Some of the aforementioned categories of information have special protected status in the EU as being sensitive personal data.

Few companies manage their own PNRs. Most major travel companies choose to outsource to a Computerized Reservation System (CRS) of which there are three major global players: Sabre, Amadeus, and Travelport. Individual bookings are either generated on or automatically forwarded to a CRS. That CRS then discloses the relevant PNRs to any company who owns any component of that trip, whether they be car rentals, theaters, cruise ships, airlines, or hotels. Canceling a trip will not erase the PNR since

"copies of the PNRs are 'purged' from live to archival storage systems, and can be retained indefinitely by CRSs, airlines, and travel agencies" (EPIC, 2004).

Governmental Regulation of PNRs

In the aftermath of 9/11, the U.S. Congress enacted legislation that authorized the U.S. Customs and Border Protection to access PNRs, which were originally used for commercial purposes by airlines. Section 7210 of the Intelligence Reform and Terrorism Prevention Act of 2004 states that the U.S. government should screen passengers departing on a flight to the U.S.; Customs and Border Protection uses PNR information as an initial screening tool to follow these Congressional mandates.

After 9/11, the U.S. government and airlines accessed and archived PNRs to investigate the hijackings and to test the ability to identify "suspicious" travelers through PNR profiling (EPIC, 2004). From 2001 to 2003, most of the major U.S.-based airlines and a variety of U.S. government agencies were involved in these investigations, which were conducted in secret, and without notice to, or the consent of, the data subjects (EPIC, 2004). Information later became public through the U.S. Freedom of Information Act (FOIA) requests and lawsuits, Congressional questioning, and investigative journalism. The Privacy International 2006 report argues, "Governments, airlines, and CRSs in other countries were pressured by the U.S. government to cooperate in providing reservation data for these programs, irrespective of national data protection laws against such use without travelers' prior consent."

While PNRs contain extensive categories of passenger information, the most controversial component of the PNR is the Advance Passenger Information System (APIS). Originally designed as a system to expedite immigration processing by allowing destination authorities to start reviewing the passenger manifest while vessels are still in transit, APIS collects, stores, and forwards to governments information about incoming passengers. According to U.S. law, any vessel entering the U.S. by land or sea must disclose the APIS information to the U.S. [Bureau of] Customs and Border Protection. APIS information, which includes passenger name, country of origin, what kind of identification the passenger is using, and the identification number, must be transmitted to the Customs and Border Protection at least 15 minutes before arrival in the U.S.. Consistent with the increased authority granted to CBP, each carrier operating passenger flights in foreign air transportation to or from the U.S. must provide CBP electronic access to PNR and APIS data. In Europe, access to and transfer of PNRs fall under the purview of European Data Protection Law. The aforementioned U.S. government PNR disclosure requirement put in place following 9/11 directly conflicts with the EU Data Directive, as it does not provide European citizens information or transparency on how their personal data is being used or stored. Furthermore, they do not have editorial control or the option to stop the forwarding of their PNRs to different vendors. U.S. data requests also conflict with the principle of Article 6 (1)(b) of the EU Data Directive, which states that the data controller may process personal data only if it is compatible with the original purpose of collecting the data. Airlines collect personal data to deliver a service and not to transfer them to U.S. Customs. Thus, transfer of personal data to the U.S. is not considered a fulfillment of obligations of airlines vis-à-vis their passengers.

Another conflict arises regarding transfer of data to non-EU countries if such countries do not provide an adequate level of data protection. The Department of Homeland Security negotiated with the European Commission for more than a year to obtain an adequacy finding under Article 26, which would allow Customs and Border Protection to access PNR data in a manner consistent with EU privacy laws (Department of Homeland Security, 2003). In May 2004, the European Commission and U.S. government negotiated the 2004 Passenger Name Record Data Transfer Agreement, which provided a safe harbor PNR transfer and found that the passenger data transferred to U.S. authorities enjoys the adequate protection required under the EU Directive for data sent to countries outside the EU. The European Parliament, however, disagreed that passenger data transfer offers adequate protection, and the European Court of Justice invalidated the U.S. EU PNR agreement on May 30, 2006.

With the annulment by the European Court of Justice, a temporary deal was put in place in October 2006, with a long-term agreement reached in June 2007. In the original 2004 agreement, the U.S. had access to 34 data fields, which was reduced to 19 in the 2007 agreement. However, the new agreement lengthened the retention period for PNRs to a minimum of 15 years. This lengthened retention period, as well as several other areas of the new agreement, led the European Data Protection Supervisor to outline areas of "grave concern" in a letter to the EU's Minister of the Interior.

Commercial Use of PNRs and Regulatory Constraints

The tension between privacy and economic efficiency surfaces often and explicitly with respect to PNRs. Travel companies benefit from aggregating large databases of personal information about their passengers. This information, provided by PNRs, allows targeted advertising and cost savings. Moreover, mobile phone, Internet search engine and other emerging technologies have increased the efficacy of targeted advertising.

Consistent with theory, PNR information provides companies an increasing ability to price discriminate. For example, in 2004 a major international cruise company (Interview,[1] Dec. 13, 2004) ran ads the week between Christmas and New Years aimed at summer travelers. By carefully analyzing PNRs and specific bookings by their repeat "loyalty guests," the company discovered the person most likely to book a cruise over the summer is a woman, age 50-70, not employed outside the home, booking for herself and her husband, who is typically a retiree. After extensive research, the company launched commercials running weekday morning from 8-10 a.m. — after their partners have left for work or other activities, but before these women go out for the day — specifically on cable channels that target this demographic. This campaign resulted in the highest conversion rate in company history, or ratio of an ad running and, within an hour, a booking being made.

[1] An employee of a major international cruise line was interviewed by the authors on Oct. 13, 2004 and Dec. 15, 2008. The source had been employed at the company for more than 10 years and reported directly to the Chief Information Officer (CIO), with responsibility for all reservations and CRM software used by most major divisions of the company.

The company also employs Customer Relationship Management (CRM) software which analyses all PNR information. When running alongside a reservation system, the CRM software automatically siphons through the PNR, and will pop up as a window inside the screen showing personal information, loyalty number, and anything else relevant to the current reservation. Because PNRs are typically shared between various parts of a traveler's experience, a cruise line might know that a customer prefers to fly into port a few days before sailing to shop in the local town. A company may then target a "convenience" package to this customer that offers a flight, hotel room, and shopping guide before the cruise at a slightly inflated price.

Clearly, the use of PNRs in this case conflicts with the European privacy approach and systems of handling personal information as required in the EU Directive. Before a passenger or their travel agent can actually print a ticket, even if the reservation has already been made, APIS information must be provided. Minimal information regarding PNRs usage and access to this data is provided to the passenger, because, unlike rights to EU citizens as enforced in the Directive, the U.S. has no comparable privacy law requiring disclosure to passengers of how their travel records are used (Hasbrouck, 2007). Negative passenger perception of privacy infringements may have its costs. "It would be a lie to say that we have not lost any reservations because of this issue. There are European guests that resist giving their personal information and may call into our office to express discontent" (Interview, Dec. 13, 2004). The interviewee acknowledges that travel companies spend significant time and money dealing with privacy advocacy groups in the U.S. and abroad. "Most things that advocacy groups want is not part of U.S. law, so we typically send them a copy of our privacy policy and spend time spinning to them" (Interview, Dec. 13, 2004).

Enforcement of the EU Directive continues to be problematic. In many countries, airlines and travel agents are overseen by distinct government agencies dedicated to that industry. Few of the aviation regulatory agencies have a data protection division. In the U.S., the Department of Transportation has jurisdiction of the enforcement of privacy policies by airlines and travel agencies, but the department has no staff dedicated to data protection and has never brought an action for violation of a privacy policy or of the Safe Harbor arrangement (EPIC, 2004). For the specific company we looked at, the interviewee said that in order to be eligible under Article 26 of the EU Directive, the company simply filled out paperwork stating it would comply. European authorities have never audited the company's records or even requested access to its passenger privacy information.

U.S. enforcement of the Patriot Act and APIS information is much more stringent. At least one APIS-related incident involving a cruise line is well documented. In April 2004, a Celebrity Cruises ship, Galaxy, docked in Charleston, SC, without transmitting its manifest as required. According to a news report, the ship returned to sea for seven hours, stranding about 400 passengers on shore in Charleston (Menchaca, 2004). The Celebrity cruise line was fined $32,500 for the failure, and eventually compensated affected travelers. While enforcement in this case happened only *after* the unannounced passengers had disembarked, this incident certainly demonstrates the U.S. commitment to APIS enforcement. In the face of customer dissatisfaction, publicity, and the cost of the incident, Celebrity seems not to have had another APIS failure since.

In addition to economic costs of PNRs, companies also encounter the security constraints. For the travel company we looked at, all that the cruise line employee could legally disclose was, "[a] handful of passengers, identified by their PNRs to be on the DHS wanted list, have been intercepted under the terms of the Patriot Act." While government rhetoric focuses on the urgent need to collect data for national security, it is difficult to asses the actual effectiveness of such measures, due to the classified nature of these issues.

Conclusion

This article has explored the differences between U.S. and EU approaches to privacy protection. U.S. authorities are increasingly in favor of security, while European policy makers continue to emphasize personal freedoms. This gap is quite representative of the priorities of the governments when mandating the Patriot Act and the Data Directive. In the U.S., security concerns eclipse privacy protection as the government's chief concern. In Europe, maintaining this "fundamental human right" of privacy supports most of their legislation, however overlooked it may be in the U.S. As discussed in this article, variances in privacy legislation stem from fundamental differences in belief systems and cultural values between the U.S. and EU, including the definition of privacy, and underlying cultural differences regarding the role of government and the commercial sector. A widening of this gap could increase the potential for costly trans-Atlantic regulatory spillovers and impede the true potential for seamless digital commerce. Substantiating general claims about the entirety of the global travel industry is obviously not possible using the analysis offered in this article. However, this work does offer a look at how trans-Atlantic regulatory inconstancies affect a major travel firm, and the case study of the Passenger Name Record debate provides an example of the practical implications of distinct regulations in the U.S. and EU.

Stringent enforcement of the Directive by European authorities, at least in the near future, seems unlikely. The EU looked to be conceding this point to the U.S. when the EC ruled that PNRs constitute "adequate protection" of information. However, while this was annulled and new agreements have been reached, the level of enforcement of the new agreement is unclear at the time of this writing. Contributing to the EU's lack of enforcement could be the rigid demands made by the U.S. to disclose passenger information to the CBP. Unlike violating the EU's mandate, if companies fail to provide adequate passenger information to U.S. authorities, they face severe penalties. According to the interviewee, "If companies disclose information in the form of PNRs or APIS, they are breaking European laws, yet if they do not, they are breaking U.S. laws. Because of the vastly differing amount of enforcement and potential penalties, companies tend to favor breaking EU laws" (Interview, Nov. 29, 2004).

With the secrecy surrounding U.S. government operations, it is difficult to judge if revoking some degree of privacy rights has increased national security. Conclusions from the case study are nebulous in this regard, yet do support the argument that the Patriot Act is quite ambivalent in what and who is considered a security threat. The suggestion that the Act is serving to widen the cultural gap between the U.S. and Europe is quite prolific and increasingly likely as European support for U.S. policy wanes. The overall handling by the U.S. of their citizens' privacy suggests that Americans view privacy not as a fundamental right, but rather a commodity that can be bought and sold, granted and revoked to achieve certain ends.

The Passenger Name Record example addresses the tensions of a global information economy and national sovereignties advocating different laws, regulations, and priorities. The consequences of these policy differences have resulted in confusion and frustration by travelers and substantial costs of companies forced to comply with two contrasting sets of regulations at once. The choice of having to break one or another country's law is not an optimal situation. Limited solutions have been posed to rectify the situation. A focus on making the U.S. and EU systems interoperable using interfaces, which do not change the content of any privacy standards but provide a platform for business, seem the most popular approach (Bach, 2001). Even so, there is much work to be done in creating interoperable solutions between two regions with such different priorities and regulatory regimes. Given the volume of world trade between the U.S. and EU, there is a significant need to reconcile different approaches to standards of data and information privacy. As the Internet and e-commerce become increasingly pervasive and significant, these differences must be reconciled for both economies to flourish in the digital age, as well as for citizens' rights to be protected. The passenger name record debate represents one example of the variances of privacy policy between the U.S. and EU, and future research investigating the variances around other forms of commerce and privacy could further advance study of U.S. and EU privacy policy.

References

Aaron, D. L. (2001, March 8). Prepared Witness Testimony. *The EU Data Protection Directive: Implications for the U.S. Privacy Debate.* The House Committee on Energy and Commerce. Washington, D.C.

Acquisti, A. (2004). Privacy and security of personal information. In J. Camp and R. Lewis (Eds.), *The economics of information security* (pp. 179-186). London: Kluwer.

Acquisti, A., & Varian, H. (2002). Conditioning prices on purchase history. *SIMS Working Paper.*

Administrative Office of the United States Courts. (2004). *Wiretap report*. http://www.uscourts.gov/wiretap04/contents.html

Bach, D. (2001). *The new economy: Transatlantic policy comparison, industry and self regulation in the e-conomy*. Berkeley Roundtable on the International Economy (BRIE).

Barlow, J. P. (1996). *A declaration of the independence of cyberspace.* Available at http://www.eff.org/~barlow/Declaration-Final.html

Bureau of Economic Analysis: National Economic Accounts. (2008). *Personal income & outlays.* Accessed Dec. 1, 2008 from www.bea.gov/newsreleases/national/pi/pinewsrelease.htm

Calzolari, G., & Pavan, A. (2001). *Optimal design of privacy policies.* Technical report, Gremaq, University of Toulouse.

Castells, M. (2000). *The rise of the network society*. MA: Blackwell.

Cohn, M. (2004). Spain, U.S. and EU: War on terrorism or war on liberties? *Jurist*. Available at http://jurist.law.pitt.edu/

Department of Homeland Security. (2003). *U.S.-EU passenger name record agreement signed.* Press Release. Available at www.dhs.gov

Dhont, J., Asinari, M., & Poullet, Y. (2004). *Safe harbour decision implementation study.* European Commission, Internal Market DG. Available at http://europa.eu.int/comm/internal_market/privacy/docs/studies/safe-harbour-2004_en.pdf

Duncan, G. (2004, April). *Exploring the tension between privacy and the social benefits of governmental databases*. Paper presented at Security, Technology, and Privacy: Shaping a 21st Century Public Information Policy, Washington, D.C.

EC Directorate General for Trade. Retrieved Aug. 7, 2007 from http://ec.europa.eu/trade/issues/bilateral/countries/index_en.htm

Electronic Privacy Information Center and Privacy International. (2004). *Privacy and human rights: An international survey of privacy laws and developments.* Washington, D.C., London: Electronic Privacy Information Center; Privacy International.

EurActiv.com. (2008, Sept. 24). *EU makes headway on anti-terror law*. Retrieved Dec. 18, 2008 from http://www.euractiv.com

European Union Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, 1995 OJ (L 281).

Economist.com. (2008, Oct. 23). *Computers without borders.* Available at www.economist.com

Farrell, H. (2003). Constructing the international foundations of e-commerce: The EU-U.S. safe harbor arrangement. *International Organization, 57,* 277–306.

Federal Communications Commission. (2005). *Policy Statement*, Adopted Aug. 5, 2005, Released Sept. 23, 2005.

Federal Trade Commission. (2000). *Privacy online, fair information practices in the electronic marketplace.* Washington D.C.

Flaherty, D. H. (1989). *Protecting privacy in surveillance societies.* University of North Carolina Press.

Fromholz, J. M. (2000). The European data privacy directive. *Berkeley Technology Law Journal, 15*, 461-484.

Goldsmith, J. (2000). Unilateral regulation of the Internet: A modest defense. *EJIL, 11*(1), 135-148.

Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world.* New York: Oxford University Press.

Hasbrouck, E. (2007). What's in a Passenger Name Record? *The Practical Nomad.* Available at www.hasbrouck.org/articles/PNR.html

Hewitt, C. (2008). ORGs for scalable, robust, privacy-friendly client cloud computing, *IEEE Internet Computing*, *12*(5), 96-99.

Holvast, J., Madsen, W., & Roth, P. (1999). *The global encyclopaedia of data protection regulation.* London: Kluwer Law International.

Kobrin, S. (2004). Safe harbors are hard to find: The transatlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies, 20*, 111-131.

Lyon, D. (2004). Globalizing surveillance: Comparative and sociological perspectives. *International Sociology, 19*(2), 135–149.

Menchaca, R. (2004, April 8). Ship strands hundreds in Charleston. *Charleston Post and Courier.* Available at www.charleston.net

Neocleous, M. (2007). Security, liberty and the myth of balance: Towards a critique of security politics. *Contemporary Political Theory*, *6,* 131–149.

Odlyzko, A. (2003). *Privacy, economics, and price discrimination on the Internet*. Extended abstract. Digital Technology Center, University of Minnesota.

Privacy International. (2006). *Travel privacy.* Available at www.privacyinternational.org

Reidenberg, J. R. (2000). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review, 52*, 1315-1371.

Schwartz, P., & Reidenberg, J. (1996). *Data privacy law: A Study of United States data protection.* Charlottesville, VA: Michie.

Swire, P., & Litan, R. (1998). Avoiding a showdown over EU privacy laws*. The Brookings Institute*. Available at www.brookings.edu/comm/policybriefs/pb29.htm

United Nations Department of Public Information. *Universal Declaration of Human Rights*, Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948.

Varian, H. (1996). Economic aspects of personal privacy. In *Privacy and Self-Regulation in the Information Age*. National Telecommunications and Information Administration Report.

Walker, M. (2004, Dec. 10). Europeans tight hold on wallets keeps lid on continent's growth. *The Wall Street Journal*. Available at http://online.wsj.com/public/us

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy, *Harvard Law Review, 4*(5), 193-220.

Wilske, S., & Schiller, T. (1997). International jurisdiction in cyberspace: Which states may regulate the Internet? *Federal Communications Law Journal, (50)*1, 117-125.

Wu, T. (1997). Cyberspace sovereignty? The Internet and the international system, *Harvard Journal of Law and Technology, (10)*3, 647-655.