22

AICGS POLICY REPORT

A REASONABLE EXPECTATION OF PRIVACY? DATA PROTECTION IN THE UNITED STATES AND GERMANY

Jim Harper
Axel Spies

AMERICAN INSTITUTE FOR CONTEMPORARY GERMAN STUDIES THE JOHNS HOPKINS UNIVERSITY

AICGS

AMERICAN INSTITUTE
FOR CONTEMPORARY
GERMAN STUDIES

THE JOHNS HOPKINS UNIVERSITY

The American Institute for Contemporary German Studies strengthens the German-American Relationship in an evolving Europe and changing world. The Institute produces objective and original analyses of developments and trends in Germany, Europe, and the United States; creates new transatlantic networks; and facilitates dialogue among the business, political, and academic communities to manage differences and define and promote common interests.

ISBN 0-941441-98-9

ADDITIONAL COPIES:
Additional Copies of this Policy Report are available for $5.00 to cover postage and handling from the American Institute for Contemporary German Studies, 1755 Massachusetts Avenue, NW, Suite 700, Washington, D.C. 20036. Tel: 202/332-9312, Fax 202/265-9531, E-mail: info@aicgs.org Please consult our website for a list of online publications: http://www.aicgs.org

TABLE OF CONTENTS

FOREWORD

In the borderless world of the twenty-first century, global interconnectivity has never been greater. Through the use of millions of computers, billions of e-mails, and a level of personal and product mobility never known before, the amount of information racing around the globe is incalculable. We are being confronted with urgent new questions about the means with which we can control that tidal wave of activity, particularly when it comes to safeguarding the privacy and data of individuals, organizations, corporations, and governments.

Who is in charge of that process in today's interwoven societies? How should one regulate the needs and demands of the various players involved? What freedoms do individuals have, should they have, to control what is known about them under which circumstances and by whom? When does regulating data about individuals hinder rather than help business, government, or researchers? How does the development of technology respond to both the need for privacy and the need for information?

While individual countries are facing such challenges on their own, the implications of cybersecurity and data privacy reach beyond the national framework. Cross-border dialogue is needed to better define the concepts and construct the policies that will enable us to handle these issues.

AICGS is pleased to present two approaches to these problems, from both the German/European perspective and that of the United States. Axel Spies and Jim Harper have collaborated to provide an assessment of the legislative, regulatory, and market demands, along with an outline of the deeper cultural, historical, and institutional factors influencing the debate and how decisions to deal with cybersecurity have developed during the recent past on either side of the Atlantic. They focus in particular on the significance these developments have for doing business in the global marketplace and how the public and private spheres have tried to keep up with the ever quickening pace of technology and demands involving data protection.

As Jim Harper notes, the policy debate on data privacy in the United States began with the Fourth Amendment to the Bill of Rights and has gone all the way to current concerns about the USA-Patriot Act. Over the past three decades, individual protection from public and private intrusion has gradually but increasingly become a major concern in the United States. In Germany, the recent past and the experiences of both the Nazi and *Stasi* periods were a primary influence on the approach to protecting individual privacy since the founding the Federal Republic in 1949. Amidst these unique historical settings, there is a great deal of common concern found in the current debate. In Germany, that debate is now inextricably intertwined with the European Union's policies and practices.

Coming to grips with the challenges facing data privacy remains a challenge for both governments and markets. These two analyses provide astute assessments of the German and American approaches, with suggestions as to how cooperation and coordination on both sides of the Atlantic might benefit the many players involved.

We are grateful to the Heinrich Böll Foundation for its support in publishing this document and to AT&T for its support of the study.

JACKSON JANES
Executive Director
AICGS

ABOUT THE AUTHORS

JIM HARPER is Director of Information Policy Studies at the Cato Institute. As the director, Harper speaks, writes, and advocates on issues at the intersection of business, technology, and public policy. His work focuses on the difficulties of adapting law and policy to the unique problems of the information age. He is a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. Harper received his Bachelor's degree in political science at the University of California, Santa Barbara, where he focused on American politics and the federal courts. At Hastings College of the Law, he served as editor-in-chief of the *Hastings Constitutional Law Quarterly*. In addition to numerous writings and ghost-writings in the trades and popular press, his scholarly articles have appeared in the *Administrative Law Review*, the *Minnesota Law Review*, and the *Hastings Constitutional Law Quarterly*.

AXEL SPIES is a German attorney in the Telecommunications practice of Swidler Berlin LLP, Washington, D.C. Spies advises American and international clients on issues focusing on licensing, competition and interconnection in the European telecommunications markets. He also provides advice in the areas of international data protection, technology licensing and lobbying. Prior to joining Swidler Berlin LLP, Spies worked extensively in the telecommunications sector in Germany, Russia, and France and as a lawyer for the German Embassy in India. He has authored more than twenty articles on various legal issues. Spies is a native speaker of German, and also speaks English, French, and Russian.

01

CHAPTER ONE

DATA PRIVACY/CYBERSECURITY IN GERMANY

AXEL SPIES

"I think there is a world market for about five computers."
– IBM CEO Thomas Watson in 1943.

The Purpose of the Study

In Germany, data protection has several dimensions Not only are distinctions made between private and public entities, but different rules and different agencies also monitor those entities on the federal and state levels. There are both sector specific rules (e.g. for telecommunications) and an omnibus law—the Federal Data Protection Act. In combination, these rules cover nearly every business activity in Germany and grant individuals a variety of mechanisms to protect their personal data. Data protection and data security cannot be separated in Germany, and they both require constant monitoring.

This part of the study focuses on how private entities, in particular U.S. investors, must use and protect personal data in Germany. It also addresses why abiding by these data protection rules creates security, enhances customer confidence, and, in the end, saves companies money.

> *"Security is not a product; it's a process. You can't just add it to a system after the fact."*
> - Bruce Schneider, *Digital Security in a Networked World,* 2000.

PRIVACY AND DATA PROTECTION: DEFINITION AND GERMAN PERSPECTIVES

The term "Data Protection" is the literal translation of the German word *Datenschutz*; although a more accurate characterization would be "protection against the abuse of personal data." In this respect, it is broader than the English word "privacy." The term "privacy" itself is difficult to translate into German ("*Privatheit*," "*Privatsphäre*," "*Privatleben*"), and even a good translation for the English term "cybersecurity" does not exist. In German usage, the terms "data protection" and "data subject" (for the individuals to whom personal data belong) reveal that it is the responsibility of the government to ensure that an individual is protected against the unjustified collection, storage, transfer, or deletion of his/her personal data. In this sense, it is not the "data" itself that is protected, but the individual behind the data. Thus, "data protection" and "data security" (the terms for how to keep the data physically safe) have different connotations in Germany and should not be confused.

German data protection laws cover "personal information." The exact English translation of the German term would be "data related to a person" (*personenbezogene Daten*). This term is interpreted broadly and comprises any information related to an identified or identifiable natural person: name, address, telephone number, e-mail address, social security number, etc. The definition even covers data related to things and only indirectly related to an individual, (e.g., a car's license tag) or data related to a legal entity (e.g., a family name being part of the name of an incorporated legal entity).

There exists a unique class of personal data, or "Sensitive Data," that is protected by special rules

(the German law refers to this category as "special classes of person-related data" that contain the following information: race/ethnic origin; political opinion; religious and political affiliation; affiliation with a trade union; health data; and sexual orientation).

This distinction between sensitive and non-sensitive personal data is based on EU law, with the idea being that sensitive data should not be processed without explicit consent of the individual. The distinction becomes complicated and questionable when sensitive information is implicitly contained in "normal" personal data (for example, buying cigarettes = being a smoker = having a higher risk of cancer).

Unlike the law in some other EU member states (e.g., Denmark, Austria, and Luxembourg), the German Data Protection law does not cover data that pertain only to a legal entity (e.g., a company instead of an individual), such as its number of employees, financial data, and know-how. That data is not protected, whereas an individual's name as part of a company's name would be covered.

The German data protection law covers "data processing," which comprises online or offline operation(s) performed on personal data, and thus goes beyond the collection or transmission or data. Under this term, the "life cycle" of data includes collection/storage, modification, transfer, blocking, and deletion, regardless of the technical means used to process the data. All phases of data processing are defined and interpreted broadly—for instance, a data "transfer" would also cover the disclosure of data to a third person, the sale of the hardware where the data is stored, or posting personal data on a website.

The Roots and Political Context of the Regulation on Data Protection/Cybersecurity

DEVELOPMENTS UP TO THE CENSUS DECISION OF 1983

Data Protection as a concept was not invented in Germany; however, German laws and court decisions have significantly influenced (and promoted) the concept of data protection in Europe. And although its roots can be traced back to the beginning of the nineteenth century, the broader debate on data protection began in the 1960s and evolved into a wide-spread movement that culminated with the adoption of the German Data Protection Act and by the rendering of the famous "Census Decision" of the Federal Constitutional Court by proactive judges in 1983.

The German roots of data protection reach back to 1907, when the German Law on Art and Copyright (*Kunst- und Urheberrechtsgesetz*) was adopted. The term "data protection" itself does not appear in this law; rather, this law stipulated that only a small aspect of data protection would be covered: every individual, whether alive or deceased, had the right to his/her own image. German courts had already elaborated upon this legal concept in a number of earlier cases. in particular in a famous case of a journalist who illegally took a picture of the corpse of Chancellor Bismarck. After 1949, the German courts quickly developed the concept of the "right to one's own image." They invoked the the Basic Law (German Constitution) to determine when photos and other information (e.g. on celebrities) could be used for journalistic and commercial purposes through the use of a more granulated concept.

One other aspect distinguishes Germany from the United States: since the days of the Prussian Empire, Germany has had a network of residential registers (*Melderegister*) that authorities have used for more than a century for various purposes, such as levying taxes, census, military drafts, etc. This system of locally administered *Melderegister* still exists today. Like more than a century ago, German citizens who move to another town and do not file a notification with the *Melderegister* on their change of residency face a hefty fine. Today's *Melderegister* provide data for a variety of governmental tasks (the levy of the much disputed German "broadcast tax" is one example). In addition, the police and other agencies had (and still maintain) their own registers of criminals, hotel guests, registered foreigners, etc. During the Nazi period, many of these registers were centralized and abused to register the race of citizens and allow for war preparations. After the Second World War, the Allies took over the registers and held various censuses to determine the size of the labor force, number of refugees, etc. The Federal Republic of Germany, founded in 1949, relied on the traditional decentralized approach of citizens' local residential

registers to perform various administrative and police tasks.

With the emergence of computer systems, the German population grew increasingly uneasy about "automatic processing of personal data" through these various registers. While there were only fifty-seven computer systems operating in 1957, the number exploded to 7,500 in 1970—most of them operated by public entities and agencies. At first, the debate on how the data processed by these systems should be protected was confined to circles of experts who warned that the government could become an Orwellian "Big Brother" figure, watching over every aspect of life, citing abuses of such registers by the Nazis. The privacy debate in the United States at this time also played an important role for the opponents of far-reaching data processing.

By the end of the 1960s, the debate rapidly entered the political mainstream. In 1968, the Federal Government announced plans to introduce a personal ID for each citizen that would enable the executive branch to categorize and register the data of each citizen nationwide, in some respects similar to the U.S. social security number. The idea behind this concept was the "data should move, not the citizen." The German federal government, while stating that the data would remain safe even if transferred from one authority to another, completely underestimated the fears and concerns of the citizens. The government quickly dropped the plans for a centralized database, but the debate continued. A similar national database, based on national IDs of each citizen, was introduced in East Germany in 1971 and remained a major tool of the Communist Government to control its citizens and allow their Secret Police (*Stasi*) and others to spy on them (this database was ultimately shut down in 1990 following the fall of the Berlin Wall). In West Germany, the concern at this time was focused on the real or perceived dangers arising from processing large amount of data by large computers. Personal computers were practically unknown at this time.

Almost at the same time, the West German Government launched a census against which various citizens filed lawsuits. In June 1969, the German Federal Constitutional Court (*Bundesverfassungsgericht*) rendered the so-called "Micro Census Decision" that determined under which circumstances the federal government could ask citizens to disclose their personal information for statistical purposes. In this decision, the Court laid the groundwork for data protection and established itself as its main driver: "It infringes with the principle of human dignity," the Court ruled,

> … if a human is treated as a mere object … government is not allowed to register an individual's entire personality, even under the anonymity of a statistical survey, and to treat the individual like a thing that is in any respect open for inspection and registration... However, this right is not without limits. A citizen who is a part of a society and interacts with it must accept to a certain extent that the government collects data for necessary statistical purposes, such as for a census, that is a precondition for planning and future government action.

Compared with the "privacy" debate in the United States, the Court's approach is much broader. Although the Basic Law has provisions that guarantee the right of every individual to be secure in their homes and not be subject to unreasonable searches and seizures, etc., the "data protection" concept of the Court went far beyond mere privacy intrusions. The issue was not only that the government would intrude on privacy (by eavesdropping, opening mail) and collect citizens' data, but also that the government would categorize the citizens and connect the data so that the individual would become a "citizen of glass," or a "mere object." This explains why the term "privacy" gave way to the much more expansive term "data protection": data that the government collects from its citizens must be protected against being passed on or being "exploited" for other purposes. In order to ensure that the different agencies abide by the law, in particular the local administration operating the residential registers (*Melderegister*), they are supervised by independent State agencies the "Data Protection Offices." Hence, this is one important reason why the first data protection laws were State laws.

In December 1970, as a result of this debate, the German State of Hessen took the necessary steps regarding the impact of new technologies on privacy and adopted what became the world's first data protection law (*Hessisches Datenschutzgesetz*). The

law was perceived as moving away from self-regulation to a regime under which the government, through independent agencies, decides how information should be protected and what checks and balances should be in place and implemented and enforced.

The Hessen law was a milestone in many respects: (1) it placed the "documents that are produced for the purpose of data processing by machines, all stored data and the results of such processing" of all public state entities and institutions under the supervision of a new independent state authority–the Hessen Data Protection Commissioner; (2) all public state entities were obliged to keep personal data secret so that third parties would not be able to obtain access to them; and (3) individuals (owners of the data) were entitled to inquire as to what information was stored about them and to demand correction if the information was incorrect. The Hessen law had a significant impact on the first federal data protection law worldwide, the 1973 Swedish Privacy Act, and caused a debate in many other states. Also in 1973, another German State, Rhineland/Palatinate, adopted its own Data Protection Law that, for the first time, foresaw damages for no-fault liability if an individual's rights under this law were violated.

It took almost seven years until the German Federal Parliament adopted the Federal Data Protection Act of 1977 (*Bundesdatenschutzgesetz* of 27 January 1977–"BDSG 1977"), which has since been modified several times. The 1977 law already covered data protection in the private and in the public sector and had as its goal protecting data related to a person from "abuse caused by their storage, transfer, modification and deletion" (which is defined as "data processing") to the extent the processing infringes on protected interests of the individuals to whom the data refers. In spite of this broad definition, the scope of the BDSG 1977 was limited, because it did not cover data that were not intended to be transferred to third parties. By 1981, all states of the Federal Republic of Germany had adopted their own State Data Protection Acts.

THE "CENSUS DECISION" OF THE FEDERAL CONSTITUTIONAL COURT

It took another seven years before the German Federal Constitutional Court (the "Court") developed an overarching concept under the Basic Law to protect an individual's data protection rights–the so-called "right to informational self-determination." The Court's ruling, rendered on 15 December 1983–the famous "Census Decision" (*Volkszählungsurteil*)–followed a fierce political debate over a law on a national census. The Census Law caused a public outcry although its scope was relatively limited. Its opponents cited once more George Orwell's *1984* and decried the law as a major step down the road toward a "surveillance state" (*Überwachungsstaat*). There were public demonstrations and rallies, many organized by student organizations, that tried to align the Census Law with the Nazi regime's use of the censuses to track minorities for extermination. Many citizens were concerned that individual census takers would enter their homes, possibly spy on them, share the information with others, and ask questions that they deemed inappropriate. The law was finally brought before the Court, which struck down major provisions of the law as unconstitutional and demanded various modifications by parliament to ensure data protection.

Several aspects of this landmark decision continue to define Germany's approach to data protection on the Federal and the state levels:

(a) "The Right to Information/Self Determination"
The Court found the Census Law unconstitutional because it infringed on what the Court named the "fundamental right to informational self-determination," which derives from the Basic Law, even though the Basic Law does not specifically mention data protection. In order to provide the legal basis for this right, the Court cited several constitutional provisions that support this right, referring, in particular, to the right of human dignity (Art. 1 Para. 1 of the Basic Law). The majority of the judges stated that this Article would be violated if an individual's "entire personality" was registered and catalogued in a way that would treat the individual like an "object" rather

than a human being. In this respect, the right to informational self-determination goes beyond a mere right to privacy, blocking the federal government from observing a person or from collecting certain data.

(b) Private Entities Must Provide "Data Protection"
Another important aspect of the Census Decision is that the Court stated the right to informational self-determination not only protected an individual's rights vis-à-vis the government but, given its importance in a democratic society, also applies between an individual and private entities that might process personal data. The Court referred to various earlier cases in which basic rights guaranteed by the Basic Law go beyond the protection of an individual against intrusions by the government and have an impact on the relationship between private parties (*Reflexwirkung*). Hence, the Court argued, private entities must observe the citizen's right to informational self-determination when they process personal data. The Court also made it clear that there are no unimportant personal data: names, telephone numbers, addresses, license tags, photos, etc. are all equally protected. The Court was very concerned that data viewed as irrelevant (such as that provided in a census questionnaire) could be combined with other personal data to create a composite picture that, the judges warned, could lead to the creation of a "citizen of glass." The judges also wrote that "a situation in which citizens do not know anymore who knows what at a certain time about them" infringes upon the Basic Law and is unconstitutional. In fact, the Court stated, it should be left to each individual to determine what personal information and under which circumstances he/she discloses it to others.

(c) Pre-defined Purpose
Through these statements, the Court affirmed another important principle of German data protection, namely that personal data may only be processed for a pre-defined purpose. At issue was whether the census data should also be used for updating the local residential registers–which the Court denied. While these statements set far-reaching constraints, the judges also realized that "data processing by automatic methods" could not be prohibited as a whole. The judges therefore clearly stated that the right to informational self-determination is not without limits. The right can be restricted by general laws and regulations, provided that they are clear, proportionate, and limited to a minimum. In particular, such laws would not be proportionate if the goals could be reached by processing anonymized data instead of personal data. To ensure the anonymity of the census, the Court held that various modifications should be made to the Census Law, which Federal Parliament adopted shortly thereafter.

Whereas many observers criticized the Census Decision as an exaggerated reaction to an irrational fear of new technologies, it was widely regarded as being in line with large parts of the population who simply felt uneasy with or even hostile toward the Census Law. The Court decision had a tremendous impact on the concept of data protection in Germany and, in the longer run, within the EU. In light of the Court's Census Decision, legal scholars, institutions, and political parties held a contentious debate on how the right to informational self-determination should be protected and what its limits were. Legal scholars began to develop a system of connoting spheres of an individual's privacy (intimate life, interaction with other, etc.), but it soon became clear that this concept would be very difficult to implement and was unlikely to reconcile with the Court's ruling that there is "no unimportant data." In time, what was reached was a broad consensus that general rules and sector-specific regulations were needed to protect the information of the citizens against the backdrop of a general law data protection. This is why Germany now has a general Federal Data Protection Act, state data protection laws, and sector specific laws, such as the data protection provisions in the German Telecommunications Act.

THE FEDERAL DATA PROTECTION ACT ("BDSG")

More than twenty years after the Census Decision, the famous "right to informational self-determination" is still not mentioned explicitly in the Basic Law, despite being inserted into all state constitutions in Germany. There is consensus in Germany that the ultimate goal of this right is not solely to protect the individual, but also to strengthen democracy, based

on the concept that a responsible citizen in a democracy should be in control of his or her personal data. This right is not without limits however: restrictions can be imposed to protect society against criminals, to prevent illegal arms deals, terrorism, etc. Indeed, after September 11, the number of cases of governmental eavesdropping increased dramatically.

In 1990, seven years after the Census Decision and following more than ten failed attempts by the Federal Parliament to revise the law, the BDSG was finally amended. Parliament's intent was to bring the BDSG in line with the evolving concept of data protection and to include additional provisions to safeguard the right of informational self-determination regarding governmental and private sector use of personal data. The BDSG was revised again in 2001 to bring several of its provisions into compliance with EU data protection law and to take into account various technical developments.

The revised BDSG, in spite of a variety of sector-specific regulations, remains the omnibus law for data protection in the public and private sector. Legislators expanded the notification requirements (e.g. for using data for advertisement purposes), expanded individuals' rights to object to data processing, and defined more precisely the circumstances under which data transfers out of Germany are legal. The revised law also raised the bar for "sensitive data" (pertaining to religion, health, etc.) to be processed. Moreover, the BDSG now defines more clearly the tasks of the Data Protection Officer ("DPO") within a company and his rights and obligations vis-à-vis the Data Protection Agency, including, for example, the DPO's right to be involved before a new data processing technology is used. Compared to the original legislation, today's BDSG is broader since it covers the phase of data collection (questionnaires, medical samples, video observation of any individual). The BDSG also defines more precisely a data subject's rights to demand correction, deletion, and blocking of his personal data. Finally, the BDSG also contains a mechanism for sanctions: providing for compensation, including fines and criminal penalties, if public bodies and private entities infringe upon an individual's rights under the BDSG.

The liability and compensation rules of BDSG are particularly important, because companies processing data face a shift in the burden of proof: BDSG allows a data subject to raise a claim against a private body for compensation, arguing that the processing of his personal data has violated data protection law and caused damage. The burden is then upon the private body to substantiate that the body has observed the law and that the damage was not caused by negligence or intent within the entity (exculpation). The company can be held liable for its agents and for not organizing the data processing properly—due to lack of training of the employees or lack of network security. In these cases, provided that the company does not demonstrate that it is not at fault, it must reimburse the individual for all damages caused by the infringement, including compensation for immaterial damages (e.g., compensation for pain and suffering). The judicial case law covers a variety of circumstances, such as illegal registration by video cameras or illegal publication of personnel data in a newspaper. The BDSG does not preclude the company's liability under other laws and regulations, for instance for violation of contractual obligations.

The BDSG also stipulates that personal data may only be processed for the purpose for which it has been collected—which, as mentioned above, is another key principle of German data protection law. Companies must not collect and store personal data arbitrarily for later use. Moreover, the individual must be told at the time of collection the purposes for which the data is needed. If the purpose of the data collection changes at a later stage, the data subject must consent before his/her data can be used for the new purpose, unless the BDSG provides otherwise; for instance, if the company does not know and cannot find out with reasonable means where the individual is.

Another feature of the BDSG is that companies are obliged to collect and store as little personal data as possible. These principles of "data avoidance" and "data economy" are now codified in Sec. 3a BDSG.

> § 3a BDSG: Data Avoidance and Data Economy
> Data processing systems are to be designed and selected in accordance with the aim of collecting,

> processing or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for using alias descriptions [of the individuals] and rendering names anonymous, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection.

In practice, it is very difficult to enforce these principles and there is always discretion for their implementation. In most cases, the Data Protection Authorities can only advise companies on how to avoid "unnecessary" data selection and storage and provide guidelines on how and when the data should be anonymized or fully deleted. For instance, a Data Protection Authority cannot prescribe that a company should accept cash only instead of credit card payments in order to avoid the collection of credit card numbers. A Data Protection Authority could probably not tell a company to buy expensive new hardware and software so that less personal data are processed. Rather, the underlying motive of § 3a BDSG is that it is in the best interest of the company to organize its systems in accordance with these principles, so that no enforcement mechanism is needed.

SECTOR-SPECIFIC DATA PROTECTION LAWS AND REGULATIONS IN GERMANY

More recently numerous so-called sector-specific data protection provisions have emerged, such as provisions in the German Tax Code, the Code on Statistics, and various sections in the 1997 Multimedia Act (*Informations- und Kommunikations dienste-Gesetz*–IuKDG).

The most important sector-specific data protection provisions, however, are Sections 91 to 106 of the new German Telecommunications Act (*Telekommunikationsgesetz*–TKG), which was enacted in June 2004, replacing various former provisions in several different laws and ordinances. In particular, the Telecommunications Services Data Protection Ordinance under the IuKDG ceased to exist. The provisions in the TKG govern a whole spectrum of data and data security for voice carriers, data carriers (e-mail, online databases), and service providers; for instance, there are restrictions on the customer's data categories (name, address) that a carrier or provider is entitled to. Using the data for marketing purposes requires explicit prior consent of the customer, unless there is already an "existing customer relationship." The TKG further imposes strict limits on processing traffic data of the customer (e.g., telephone numbers the customer has called, beginning and end of the connection). Traffic data may only be stored if this is necessary to establish or to maintain the technical connection, or if they are needed for billing purposes. Billing data are only to be stored for up to six months, counted from the day when the invoice is sent, unless the customer challenges the invoice. It is up to the customer to decide whether the numbers he called are deleted by the provider/carrier or stored in an anonymized form (by deleting the last three digits).

The TKG also contains restrictions on the itemized bills that a carrier/provider sends to the customer. Itemized billing is allowed only following a written request or with the consent of the customer. Calls to certain religious, social, or welfare organizations must be anonymized. Data needed for troubleshooting, for detecting errors in the network, or for detecting abuse of the service may be collected and stored—but for no longer than a period of six months. In addition, the TKG contains a detailed provision on when the data may be disclosed to block nuisance calls: if users receive nuisance calls, they are entitled to file a written request with the carrier to inquire from where the calls are placed. The carrier may then disclose the data (including the name and address connected with the number), but only for calls being made after the written request is received. The provisions on the suppression of caller identification are also largely motivated by data protection considerations. Finally, the users can determine whether they want to be listed in a directory and what information about them should be listed.

IMPACT OF EUROPEAN UNION LAW ON DATA PROTECTION IN GERMANY

As mentioned, the recent revisions of the BDSG are mainly driven by EU law, whereas the BDSG and the German Census Decision themselves have significantly influenced the EU law on data protection. In

particular, the EU has passed various "Directives" addressing data protection in the spirit of the Census Decision and the BDSG. Under the EU Treaty, the Directives are in almost all cases not directly binding upon the individual member states, but leave the member states to determine how to "transpose" the contents of a given Directive into national laws. However, Directives almost always contain provisions on the time limits for implementation, after which the individual member state may be sued by the EU for not "transposing" a Directive at all (or for not transposing it correctly) into national law—a process that usually takes years. German courts are reluctant to allow individuals to sue a country for not properly "transposing" EU Directives into national law.

a) EU Data Protection" Directive of 1995

The EU Directive 95/46/EU of 5 November 1995 is the most important EU legal document in the area of data protection. This Directive takes a comprehensive "top-down" approach to privacy issues. Its objective is to protect individuals with respect to the processing of personal information and to ensure the free movement of personal information within the EU through the coordination of national laws; in other words it aims to "harmonize" individual privacy rights and duties EU-wide and imposes obligations on companies and organizations that process personal data of EU customers. The Directive distinguishes between "Data Controllers"—any person that, alone or jointly, determines the purposes and means of processing personal data (e.g., a company that processes personal data of its clients and employees) and "Data Processors"—any person that processes personal data on behalf of a data controller. The Directive also contains detailed provisions on the transfer of personal data from one country to another country, in particular outside of the EU.

b) Other Relevant EU Directives

A number of other EU Directives contain provisions on data protection, such as Directive 1997/66/EC ("Privacy Protection in the Telecommunications Sector"), which was, to a large extent, replaced and expanded in scope by Directive 2002/58/EC on "Privacy and Electronic Communications." The most important feature of this 2002 Directive is that its provisions apply to "electronic communications" (data and voice traffic), whereas Directive 1997/66/EC only applied to telephony services. A provision in the 2002 Directive governing unsolicited e-mails (SPAM) was particularly disputed. The compromise that the EU found on blocking SPAM is relatively complicated and how to deal with unsolicited e-mails is a provision that one would usually not expect in a data protection law. Also noteworthy is that there are specific provisions in "location data" (determining the location of a person) in the 2002 Directive. The minimum and maximum retention of data (e.g., telephone numbers called, e-mail addresses) for national security protection and prosecution of crimes is left to the member states to determine. Germany claims that it has fully "transposed" this Directive into its 2004 Telecommunications Act. Another important Directive containing data protection provisions is the Directive 1999/93/EC on Electronic Signatures that Germany has "transposed" through its *Signaturgesetz* (Signature Act) of 13 June 1997, as amended.

NEW CHALLENGES

The current challenges that the German BDSG faces stem primarily from the world evolving to a point at which network personal data can be processed everywhere, and data are collected and stored by tools other than computers, e.g., by smart tags on goods in stores. Social mobility has also increased and an increase in data movement has occurred as well. The German authorities are aware that it is illusory to prohibit such applications or to rein them in for data protection purposes. To a large extent, this process is driven by individuals who want to have their personal data, e.g., their credit card numbers, available at any location and at any given time. The new technologies also open the doors to a very granulated "data" picture of an individual. Given the high complexity of data processing, it is virtually impossible that, as the Court stated in its Census Decision, "everyone should know who knows what about him/her at a certain time." Given the multitude of applications and the increased tasks of modern government, this means that the principle of "data economy" (Sec. 3a BDSG) must be balanced against the requirements for using these new technologies. There is no easy way out.

Key Institutions and Actors

GERMANY AND THE EU

The easiest way to understand the relevant actors and their roles is to start from the bottom to the top—from the in-house Data Protection Officers to the EU institutions and courts. They are different from the key actors in the United States (consumers, consumer advocates, pollsters, and investors), a by-product of the German "top-down" approach of imposing data protection rules and regulations on private and public entities.

1. Data Protection Officers (DPOs)

a) General Concept

The concept of having an in-house data protection commissioner (*Betrieblicher Datenschutzbeauftragter*—DPO) is the lynchpin of the data protection concept for private and public entities in Germany. The BDSG stipulates that companies processing personal data in Germany must appoint a DPO if the company:

(i) processes personal data and has more than four employees that process the personal data by "automatic procedures;"
(ii) has more than twenty employees that process personal data; or
(iii) irrespective of the number of employees, stores, uses, transfers, or otherwise processes personal data as its primary business.
In any case, a company can also appoint a DPO on a voluntary basis at any time.

The principal rationale for having a DPO, similar to the concept of a privacy officer in the Unites States, is that DPOs are usually very familiar with on-site problems. They may serve as an early warning system for the company; a DPO should be able provide advice to his company on how to solve a data protection problem "on the spot" and, consequently, ease the work load of the State Data Protection Agency ("DPA") that is supervising the company. Once a company appoints a DPO, the company is no longer obliged to register its databases with the DPA that supervises the company (there are, however, a few exceptions to this rule; for instance, companies in the business of processing health data). A company that does not appoint a DPO when it is obliged to do so can be fined up to €25,000.

A DPO is an employee of the company that appoints him. He is not imposed on the company or otherwise assigned by the DPA. A DPO's primary tasks are to advise the management of the company on privacy matters, to control the processing of personal data within the company, and to be the interface with the data protection authorities. Under the BDSG, companies are free to choose an internal or external DPO (the latter could be a sub-contractor helping them to comply with the rules of the BDSG). Most companies opt for an internal DPO to ensure the secrecy of the data and to save costs. Depending on the size of the business and the amount of personal data that is processed, the DPO can work part-time in this function and otherwise work as a regular employee of the company, provided that there are no conflicts of interests with his DPO function.

The company must ensure that the DPO is kept abreast of the data processing within the company and that the DPO receives appropriate resources and training in order to perform the job properly.The BDSG sets forth a number of requirements in this respect: Generally speaking, the DPO must educate the company personnel, ensure that the data security systems are functioning properly, and maintain contact with data protection authorities. However, in the end it is incumbent upon the company's management to adopt and implement relevant policies and corporate resolutions in order to reach their security goals.

b) Rights of a DPO

The most important right of a DPO is that he or she is entitled to supervise (by random checks with and without prior notice) the company's data processing to ensure its compliance with the data protection law. In this context, the DPO may suggest adopting or amending the company's internal data processing policies. The DPO is also entitled to be involved in new company projects that have an impact on the processing of personal data (e.g. introduction of new databases and IT systems). The DPO is entitled to be supported by all employees of the company, for

example, the DPO must be told which data files exist and who has access to them. If a DPA requests a data protection audit, the DPO is in charge of the supervision of the audit and serves as the contact point for the DPA. In this context and with regard to any data protection issue, the DPA has the right to file requests, submit questions, and seek advice from the DPA. The DPO also serves the company's employees as a point-of-information and ombudsman on data protection issues.

c) Duties of a DPO

Supervision of the company's data protection policies and its compliance with the data protection laws and regulations, in particular, is not only the right but also a duty of the DPO. The goal is to provide safeguards ensuring that personal data is kept secret within the company and that it is not illegally transferred to a third party. For this purpose, the DPO must maintain and update an in-house data processing register (an overview of how data is processed within the company, including hardware and software and a listing of who has access to the data). Education and training of the company's staff to improve their awareness of data protection issues (training sessions, posting messages on the company's information board, etc.) are additional DPO duties, and he or she must also provide regular reports to the company's management on his or her work and the status of data protection. Not all DPOs are prepared, however, to play whisteblower by standing up to management and identify abuse of personal data within the company against great internal pressure. This is one of the biggest drawbacks of the DPO concept.

2. Agencies

a) State and Federal Data Protection Authorities (DPA)

As stated, most businesses in Germany no longer have to register their databases with the data protection authorities if they appoint a DPO. While this change relieves most companies from burdensome and bureaucratic filings and updates, it does not mean that the companies that do not file are exempt from complying with all relevant German data protection laws. Only if personal data is a business's core purpose (consumer survey agencies, detectives, address brokers, etc.), must a registration of the databases be submitted to the relevant DPA. There are particular rules that apply to data processing by the media (broadcasting and press) and by churches and religious communities.

If a filing is required or a question arises with regard to data processing within a company, the DPA of the state where the company is located is in charge. The State DPA is also the primary contact for the DPOs and is responsible for the audits/controls of all public agencies of the state including municipalities and local authorities according to this state's Data Protection Law.

Tips for Appointing a German Data Protection Officer (DPO)

- In his function as the DPO, the individual must report directly to the CEO of the German company;
- There is no restriction in the BDSG that the DPO must be a German national, but in general a DPO must be someone who has the "sufficient professional knowledge" with regard to the IT systems the company operates and the data flows. In practice, there is some flexibility. For instance, if an individual does not have "sufficient professional knowledge," he can be appointed if he promises to attend seminars on the tasks of a DPO as early as possible;
- The DPO must be "reliable" (clean criminal record, etc.);
- The DPO does not necessarily need to be embedded in the German subsidiary, but he should spend a significant amount of time with it since he is the contact person for any complaints;
- The DPO cannot have any conflict of interest with other responsibilities; e.g., the head of German Human Resources is probably not a good candidate for becoming the DPO;
- The appointment of a DPO must be in writing and comply with the bylaws of the company;
- The employees must be informed of the appointment.

On the federal level, the Federal Data Protection Commissioner (*Bundesdatenschutzbeauftagter*) in Berlin has similar responsibilities. The Federal Data Protection Commissioner is responsible for the audits/controls of all federal agencies, all telecommunication services, and all postal services. Where personal data is processed or used in databases, the Commissioner monitors its collection and processing. He also handles complaints if an individual (the "data subject") files a complaint that his/her data protection rights have been violated by a federal agency. Federal courts are only monitored by the Federal Data Protection Commissioner to the extent that a court handles an administrative matter—e.g., keeps a commercial register. The BDSG stipulates that all federal public bodies must support the Commissioner and his aides in the performance of their duties. The Commissioner may also perform systematic audits over a several-year period to ensure compliance with the provisions of the BDSG. The Commissioner also has specific responsibilities in the telecommunications sector together with the telecommunications regulatory authority BNetzA (Federal Network Agency).

The State DPAs and the Federal Data Protection Commissioner cooperate very closely to ensure application of the laws and to exchange information on current issues and new challenges in the data protection sector. Representatives of these agencies meet at least twice each year and form specific working groups (e.g. on international data protection matters) making recommendations to the agencies on specific matters. These consultative groups also seek to define common ground on pending legislation impacting on data protection. However, from the legal perspective, each DPA acts independently and remains ultimately responsible for data protection within its jurisdiction.

Another important task of the Commissioners on the federal and state levels is to provide detailed activity reports to their respective legislative bodies on the state of data protection and recent developments. These reports usually have a serious impact on the debate and sometimes shape it to a significant extent. They are also a valuable source of information for the public on the issues that the DPAs are facing. In addition, the BDSG stipulates that the Federal Data Protection Commissioner, upon request by Parliament or the federal government, may provide opinions and reports on specific issues. For instance, the Federal DPA testified before the relevant parliament committees in 2004 on the data protection rules in the new Telecommunications Act and delivered written opinions on the proposed revisions.

In addition, most DPAs operate their own websites with various information tools to inform interested citizens, companies, and agencies about their rights and duties under the data protection law. This information regarding rights and duties is partially available in English. The Berlin DPA, for instance, offers a free daily press review called "PRIMA" (headlines and summaries) on privacy-related issues on its website, various recommendations and advisories, sample letters, check lists and advisories, and recommendations on specific data protection issues (using passwords, selling addresses), as well as a large number of links to other privacy-related sources of information.

Some German DPAs offer voluntary auditing and certification of products to companies that fall under their jurisdiction. For instance, the DPA of the German State of Schleswig-Holstein offers a privacy seal (*Gütesiegel*) to any company that on a voluntary basis participates in a data protection audit performed by registered independent experts on the basis of a "catalogue of requirements." It states that the fees for performing the audit and obtaining the privacy seal from the DPA are usually between €1,120 and € 2,240—which, however, does not include the costs of the independent auditor.

b) European Commission and "Article 29 Working Party"

Since the debates that lead to the 1995 EU Data Protection Directive, the European Commission ("EC") has become an increasingly important player in influencing data protection in Germany. Direct intervention by the EC (through its Directorate General "Internal Markets") in German data protection matters is rare (for instance, by issuing warning letters to a Member State that does not "transpose" EU data protection law timely and fully into national law). Of

more practical relevance to companies and individuals is the so-called "Article 29 Working Party"–an independent body of national data protection experts that advises the EC on data protection matters pursuant to Article 29 of the EU Data Protection Directive.

The Article 29 Working Party has the following objectives:

- To provide expert opinions from member state level to the Commission on questions of data protection;
- To promote the uniform application of the general principles of the Directives in all member states through cooperation between data protection supervisory authorities;
- To advise the European Commission on any EU measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy;
- To make recommendations to the public at large, and in particular to European Community institutions, on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.

While Germany is certainly not the only promoter of data protection on the European level, it is certainly an important player. During the German EU Presidency in the second half of 1994, the German Federal Data Protection Commissioner Dr. Jacob presided over the predecessor of the Article 29 Working Party, the Council Working Party "Economic Questions: (Data Protection)," which was a driving force behind the final drafting and adoption of the EU 1995 Data Protection Directive. The current chairman of the body is again from Germany–Peter Schaar, the current German Federal Data Protection Commissioner, who has a distinguished career in the area of data protection. The Article 29 Working Party has issued various legally non-binding recommendations for national data protection agencies: on data protection issues related to intellectual property rights, the transmission of passenger name records and advance passenger information from airlines from the EU to the United States, on the inclusion of biometric elements in residence permits and visas, the processing of personal data by means of video surveillance, and the application of the data protection principles to directories.

Other EU bodies whose work involves data protection are: the Joint Supervisory Body of Europol (coordinating police activities), the Joint Supervisory Authority of Schengen (customs issues), the Committee on the Customs Information System, and the Conferences of European Data Protection Commissioners, which are held as the traditional "Spring Conferences" once a year.

c) The Council of Europe

Germany is a member of the supra-national Council of Europe in Strasbourg, France and has ratified its "Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data." Germany is attending the Strasbourg committees that deal with the Convention 108. It is worth mentioning that the scope of the Convention 108 is in some respects broader than the German BDSG. For example, Article 3 (3) of this Convention protects not only personal information of individuals, but also "information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personhood." In other words, it includes data of legal entities that the BDSG does not protect. Given the detailed provisions of the BDSG and German State Data Protection Acts, the practical impact of this Convention on German data protection is rather limited, and there is some debate as to what extent the Convention 108 is binding. Data protection is also mentioned in the EU Charter of Fundamental Rights:

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Art. 8 Protection of Personal Data

1. Every individual has the right to the protection of personal data concerning him/her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Every individual has the right of access to data which has been collected concerning him/her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

3. Courts

a) German Courts

Various German court rulings have had significant impact on German data protection. As mentioned above, the federal court in charge of the interpretation of the German Constitution "discovered" in 1983 the Constitutional right to informational self-determination in its landmark Census Decision. German courts continue to shape many aspects of privacy, in particular the labor courts in the area of employment law and the administrative courts vis-à-vis government agencies. Given that there is no specific Act on employee data protection in Germany (drafts have been circulating for years), the labor courts fill the legal gaps and render rulings on a variety of employment-related privacy issues, such as the legality of surveillance of employee's e-mail traffic and telephone calls, the rights of employees to inspect their own personnel files, etc.

b) European Court of Justice

In the recent past, the European Court of Justice ("ECJ") in Luxembourg has entered the arena of data protection by rendering an important data protection decision with an EU-wide impact. On 6 November 2003, the ECJ rendered its first judgement on the interpretation of the 1995 Data Protection Directive (95/46/EC) in the landmark "Lindqvist" case. The ECJ held in this decision that personal data published on a private Internet site (produced and hosted in Sweden) did not fall under the 95/46/EC Directive's definition of a transfer of personal data to third countries. However, the judges found that the publication was subject to the rules governing the processing of personal data in the Directive; The ECJ clarified that websites that display personal details (even if trivial) in the context of personal/non-profit-making activity are covered by the Directive. It also held that website operators are not subject to the legal regime regarding the "transfer of data to a third country" when posting personal data on a website unless: (1) they actually send the information to Internet users who did not intentionally seek access to the pages, or (2) the server infrastructure is located in a non-EU country. Finally, the ECJ allowed individuals and organizations to raise claims under their national laws even if the rights go beyond what is prescribed in the Directive. Given that the Germany's BDSG already incorporates the Directive, the ECJ decisions probably does not open new avenues for lawsuits.

Potential for Conflicts

TRANSFER OF PERSONAL DATA FROM GERMANY TO THE UNITED STATES

Transferring personal data from Germany into another country is a particularly touchy issue because, in principle, such data transfers are prohibited by both the EU 1995 Data Protection Directive and the German BDSG if the receiving country does not provide "a level of adequate protection" for the data. From the German and EU perspective, the United States falls under this category. Under the EU's 1995 Data Protection Directive, a DPA may interrupt the data flow and fine companies to a country that does not provide adequate protection. Without adequate protection, the EU has argued, the high standards of data protection established by the Data Protection Directive and the national laws would be undermined. By contrast, all European Union Member States provide a similar level of adequate data protection for their citizens. The European Commission has also found that specific receiving countries provide "adequate" data protection (to date, Argentina, Canada, Switzerland, Hungary). Consequently, the BDSG provides that data transfers to these countries and the EEA are legal. The EEA is made up by the European Union Member States plus Iceland, Norway and Liechtenstein. In order to enable companies still to export data to other countries, in particular to the United States, EU law and the BDSG provide for other tools to protect personal data that is exported:

- The U.S. company must publicly and properly declare its adherence to the U.S.-EU Safe Harbor Privacy Principles ("Safe Harbor");
- The recipient of personal data enters into a contract assuring adequate data protection (e.g., incorporates model contractual provisions issued by the European Commission–"Model Contractual Clauses";
- The sending and receiving parties belong to the same corporate group and adhere to the same "binding corporate rules";

- The data subject "unambiguously" consents to the transfer; or
- The transfer is "necessary to perform a contract" between the controller and the data subject.

a) The Safe Harbor Principles

Since the European Commission has not classified the United States as a country providing adequate protection for personal data arriving from the EU, including Germany, "just do it" is legally not an option for a U.S. company, given the legal sanctions it could face. On the other hand, a complete prohibition of data flows from the EU to the United States is of course unacceptable for industry and simply not realistic. In order to provide a legal basis for data transfers from the EU to the United States, the EU and the U.S. government have negotiated the concept of a "Safe Harbor." The Safe Harbor Framework seeks to bridge the gap between the top-down European data protection regime and the more decentralized U.S. approach. In short, it permits the export of personal data to U.S. companies that have agreed to follow certain principles of acceptable data protection practice.

U.S. "Safe Harbor" Principles:

- Permit U.S. companies to satisfy EU privacy standards;
- Intended for use solely by U.S. organizations receiving personal data from the EU;
- Framework consists of seven Safe Harbor Principles (notice, consent, onward transfer, access, data security, data integrity, and enforcement) and fifteen explanatory texts called "Frequently Asked Questions" (FAQs) that provide supplemental guidance;
- Safe Harbor is voluntary;
- Certain business sectors are not covered (e.g., financial sector, carriers that are subject to the jurisdiction of the Federal Communication Commission–FCC).

In order to register for the "Safe Harbor," the U.S. company receiving the personal data must annually file a written statement containing certain information with the U.S. Department of Commerce. The U.S. Department of Commerce maintains a list of organizations that have filed at www.export.gov/safeharbor, which is updated periodically and accessible to the public. The Safe Harbor has a self-regulatory privacy framework and is based on a public declaration by the U.S. company that it adheres to seven Safe Harbor Privacy Principles (notice, consent, onward transfer, access, data security, data integrity, and enforcement) and the explanatory texts called "Frequently Asked Questions" (FAQs). The benefits of Safe Harbor participation are assured when the company completes a self-certification with the U.S. Department of Commerce that it adheres to the principles. Any violations of the Safe Harbor by such companies will be actionable by the U.S. Federal Trade Commission or, where applicable, the Department of Transportation.

The advantages for a U.S. company of filing a statement under the Safe Harbor are that U.S. law applies and the filing provides for greater certainty and continuity; it can also be used as a marketing tool vis-à-vis German companies. Another advantage of the Safe Harbor Framework is that it is fully backed by the European data protection agencies. In their eyes, it provides the "gold standard" for compliance with EU data protection law when transferring personal data to the United States, as stated by various participants during a recent U.S./EU conference on the Safe Harbor Framework in Washington, D.C. The U.S. government also encourages U.S. companies to participate in the Safe Harbor Framework. Finally, the Safe Harbor Framework typically does not require the implementation of contracts between the European entities and the U.S. recipients. Depending on the circumstances, such as the number and type of EU entities transmitting data to the United States, this may represent a substantial savings of administrative burden and cost. It also may offer a marketing advantage for U.S. companies seeking to do business in the EU.

A drawback for U.S. companies is the administrative burden to comply with the Safe Harbor. In certain cases, these companies are charged a small administrative fee. Far more important, however, is how companies ensure internal compliance with the Safe Harbor requirements, for instance by providing a complaint mechanism. Many U.S. companies are concerned about potential liability under U.S. law

(since the compliance for Safe Harbor is overseen by the Federal Trade Commission or the Department of Transportation) if they do not fully comply. Moreover, U.S. companies must promise to cooperate with European DPAs, and individuals, under certain circumstances, may sue the company for not or not complying fully with the Safe Harbor in Europe. Third party beneficiary rights to sue the U.S. recipient under the Safe Harbor are rather limited, unless HR (employment data) is concerned. The general rule is that individuals owning the data have the right to make complaints to the company, and also the right to a mediation or arbitration process. In practice, a data subject could always seek to find a tort or contract-based action against the U.S. company. Apart from that, some U.S. companies do not file under the Safe Harbor because their name and additional information will be posted online on the Department of Commerce's Safe Harbor List. They argue that this might increase the company's visibility on EU data protection issues, and may attract attention from European DPAs. Another possible disadvantage to the Safe Harbor is that participation in Safe Harbor is only open (at present) to entities that are actually subject to the Federal Trade Commission or the Department of Transportation authority. Financial services, telecommunications, and other industry sectors that are excluded from the Federal Trade Commission and Department of Transportation authority are not eligible to join the Safe Harbor list. For certain areas, such as "Internet telephony" (VoIP–or Voice over Internet Protocol), the application of the Safe Harbor is widely unclear. Finally, Safe Harbor is not a suitable solution to the data protection issues in a multi-jurisdictional outsourcing arrangement, for instance if the data from Europe are only stored temporarily in the United States or if they are passed on to locations of other jurisdiction, although there are talks ongoing to expand the Safe Harbor Framework to these cases.

More than 800 companies in the United States have so far participated in the "Safe Harbor," which represents a growing number. Many businesses still favor tailor-made solutions to the restrictions on exporting personal data to the United States, which might include technical and legal measures to establish an adequate level of data protection for the individual case in question. It is very helpful and advisable to contact the relevant DPA in advance to discuss a practical solution, particularly where the "Safe Harbor" or other tools do not work or do not apply.

b) Model Contractual Clauses

Another solution for data transfers from Germany to the United States is that the data controller in Germany and the recipient in the United States enter into a contract that incorporates model contractual clauses issued by the European Commission. The European Commission has issued two sets of contractual clauses which are rather detailed contracts, instead of short clauses. The purpose of these Model Contractual Clauses, according to the EU, is to provide industry with a basis for transferring personal data from the EU to third countries where "adequate protection" of the data is not provided by law. However, the exact distinction between the scope of the Safe Harbor and the scope of the Model Contractual Clauses remains unclear. The U.S. Government prefers that U.S. companies opt for the Safe Harbor Framework. The European Commission stated explicitly in a recent statement that the Model Contractual Clauses, once adopted, "have no effect on further discussions with the United States to enlarge the scope of the Safe Harbor." One may conclude from this statement, to the contrary, that the Commission deems the Model Contractual Clauses as an alternative to the existing Safe Harbor Principles. However, some clauses of the Model Contractual Clauses may be interpreted to mean that only organizations that are not "Harborites" are entitled to use the Model Contractual Clause.

In any event, many U.S. companies believe that the Model Contractual Clauses are too bureaucratic, complicated, and not tailored to commercial needs, even though the European Commission recently published a revised version. They also believe that their incorporation carries substantial risks since they constitute contractual commitments that third parties can rely on as "third party beneficiaries," and may supersede compliance with Safe Harbor and exceed their protection standards. Consequently, individuals may sue the data exporter or importer or both. Under certain conditions, U.S. companies might be held responsible and brought to court in the EU for the

Data Exporter's violations of the national law; "Associations" may represent individuals in court. By their own terms, the Model Contractual Clauses encourage DPA interference: under the EU decision on the Model Contractual Clauses, national DPAs are explicitly entitled to block or suspend the data flow, in particular "if there is a *substantial likelihood* that the standard contractual clauses in the annex are not being or will not be complied with and the continuing transfer would create an *imminent risk* of grave harm to the individuals owning the data." (Emphasis added). So far, most national DPAs have been cooperative in addressing problems regarding compliance with the BDSG.

c) Binding Corporate Rules

Adopting Binding Corporate Rules is an approach that some U.S. companies prefer where personal data from Germany are shared among a group of affiliated companies that are located, at least in part, in the United States. This approach essentially involves the imposition of a group-wide code of conduct for collecting and processing personal data as "Binding Corporate Rules." The advantage is that the group of companies can tailor the terms and descriptions of the rules so that they can be more easily understood and implemented by the company employees in the United States and elsewhere. The group of companies also is free to seek to incorporate more flexibility into the substantive requirements in the rules, and does not need to automatically accept a standard set of terms "as is." However, there is no standard set of Binding Corporate Rules that German data protection authorities generally accept. To date, any set of Binding Corporate Rules is subject to full scrutiny by competent DPAs and they may require prior approval. The approval process may require significant time and money to negotiate with local authorities regarding the proposed terms. This creates a particularly difficult situation for corporate groups with operations in various EU member states: Once the Binding Corporate Rules are modified to satisfy one authority, the company may need to go back for review by all other national authorities that have already given their approval to obtain their blessing on the modification. The DPAs in the EU Member States recently issued an opinion paper supporting the concept of Binding Corporate Rules. This opinion also indicated a desire of the authorities to move toward a "mutual-recognition" approach to these rules, such that, if one Member State's authority approved a code, it would be recognized in other EC jurisdictions. Such a system has not yet been established. Until then, Binding Corporate Rules remain for many U.S. companies a cumbersome and time-consuming approach.

d) Individual Consent of the Data Subject

This is another tool that U.S. companies use, allowing them to transfer personal data from Germany to the United States. Art. 26 (1) (a) of the 1995 Data Protection Directive states that "Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection … may take place on condition that … the data subject has given his consent unambiguously to the proposed transfer." Consent is usually obtained by having the data subject affirmatively indicate that his or her personal data can be transferred to a jurisdiction that does not provide adequate protection. The company drafts the consent form on its own (although with reference to the applicable legal requirements). The Consent approach may also work particularly well in the online setting, where it is relatively easy to procure an appropriate click on an "I Agree" button or comparable feature. However, it is highly questionable whether this consent via Internet "button" holds water under German law. The BDSG requires a physical, signed consent form, "unless due to the particular circumstances other forms of consents are appropriate." It is not clear what this means for online consents. It is not guaranteed that the individual clicking on the button is actually the data subject. Even if this hurdle is cleared, the consent may not be given "voluntarily", as foreseen by this provision. This is especially tricky in the context of employers asking for consent of their individual employees to send their personal data to the United States since the employee may believe that he does not have another choice than signing the consent form. Another possible downside of the individual consent solution is that there may be a "drop out" rate, where a percentage of individuals will not actually agree to consent.

The consent given by an individual must also be "informed." The European Commission, in a statement to the E-Commerce Task Force of the U.S.

Department of Commerce, (http://ita.doc.gov/td/ecom/priv.htm) has provided the following clarification on the requirements under the EU 1995 Data Protection Directive: "Commission officials draw attention to the definitions section of the [EU 1995 data protection] directive, where consent is defined as follows: the data subject's consent shall mean any freely given, specific and informed indication of his wishes, by which he signifies his agreement to personal data relating to him being processed. In order for the Article 26 (1) (a) exception to apply, consent must be unambiguous–that is, there must be no doubt that consent has been given. Implied consent (e.g., an individual was made aware of the transfer and did not object) is insufficient to qualify for the exemption. Individuals owning the data must be properly informed of the particular risk that their data may undergo as a result of the anticipated transfer to a country lacking adequate protection. If this information is not provided, the exemption will not apply." These standards also apply in Germany, as foreseen by various court decisions.

e) "Performance of a Contract"

In specific cases, companies in the United States that receive data from Germany may rely on a provision in the EU 1995 Data Protection Directive that the data transfer to the United States is necessary to perform a contract between the data controller (the entity in Germany that controls the personal data) and the data subject. If this provision applies, all data processing that is necessary for the purpose of the contract and for compliance with legal obligations of the employer (for example, accounting for taxes, social security) is allowed. However, the German authorities interpret this provision restrictively and would likely require a so-called data processing agreement between the U.S. and the German entity to ensure that the personal data are kept safe in the United States.

EMPLOYEE DATA PROTECTION

a) Consents

Sometime U.S. companies do not realize that the German data protection law not only covers the personal data they store on customers, but also those data referring to their employees (names, age, addresses, health data, religion, etc.). Although there is no omnibus Employee Data Protection Act in Germany (the issue has been on the agenda for years), there are legal provisions under the German Co-Determination Act that apply: The most important provision is that, prior to the processing of such data, the company must inform and obtain consent from the company's works council (*Betriebsrat*). A *Betriebsrat* is the representative body of the employees of a certain size, which has to be established if they vote to have one. In particular, the works council must consent to measures pertaining to all questions of employees' surveillance and control like, for example, introducing telephone monitoring. If consent is withheld by the works council for no valid reason, its decision can be overruled by the labor court having jurisdiction in this matter.

If there is no works council in the German company, which is regularly the case in smaller entities or start-ups, the company must obtain informed consent of the individual employee before processing his personal data in the United States. If individual consent is necessary, the general prerequisites for obtaining consent under the BDSG apply: The consent must be "voluntary" and sufficient information must be given to the employee before the consent is given ("informed" consent). In its already-cited statement to the E-Commerce Task Force of the U.S. Department of Commerce, the European Commission makes the following statement on this issue:

"Transfer of employee data is possible, provided that consent, as defined above, is obtained at the outset of employment. The consent must not be so generally worded that individuals owning the data do not know which of their data are being transmitted to another country, to whom and for what purpose. Repetitive transfers of the same type, however, do not require repetitive information and consent. Commission officials point out that the transfer of certain employee data could also fall under the exception foreseen in Article 26 (1) (b) [of the EU 1995 Data Protection Directive] because it may be necessary for the performance of a contract between the employee and his/her employer. This would be the case, for example, for the transfer of data necessary for the payment of the individual's salary or other related benefits."

It seems that the exception of Article 26 (1) (b)—no consent of the transfer is necessary for the performance of a contract between the data subject and the [data] controller—is interpreted narrowly to avoid the general consent requirement of the employee being undermined by the employer. Some scholars in Germany doubt whether an employee can voluntarily give his consent at all, since he must fear facing serious consequences (such as the loss of his job) if he does not consent. Thus companies may need to walk a fine line.

b) Information Rights

In addition to the co-determination rights of the works council and/or individual "informed" consent, each employee is entitled to know which of their personal data is being stored. Companies must honor their request and provide the employee with information on the data they process on them (Sect. 19 and 34 BDSG). The information the companies provide must be comprehensive and extend to all aspects of the data processing. In particular, the company must include information on the data it stores on the employee, the origin and recipients of the data, the purpose of the data processing, and the service provider in the case of outsourcing. The information must be complete and be provided in a timely manner. Incorrect data must be modified or otherwise purged as early as possible. Usually the information process would involve the DPO of the company.

c) Use of the Internet by Employees

A specific issue that companies are concerned about is to determine in which cases personal data of employees that surf the Internet may be stored. The German Federal Data Protection Commissioner recently issued non-binding recommendations summarizing the status quo:

> Total monitoring of the employees is prohibited. However, the employer is entitled to perform random checks, in a timely manner, provided that this process is as transparent as possible. To the extent that the data are processed to ensure data safety or the orderly operation of the facilities, the data processing is restricted to these purposes alone. If the employer has allowed the private use of the Internet, he must respect the right to communications secrecy of the employees, pursuant to which data may only be processed or used, to the extent that the information is necessary for the provisioning of an Internet services or billing. Since the employer has a justified interest in preventing abuse or criminal activities not only regarding work-related Internet access, but also regarding any private use of the Internet, he is entitled to allow the private use of the Internet only under certain conditions regarding the time periods, the admitted areas and regular checks.

To sum up, prior consent of the works council or individual consent is needed, clear-cut rules for all employees should be set up in advance, and employees must be notified properly.

MANDATORY DATA STORAGE

In the wake of the terrorism attacks of 9/11, German State law enforcement agencies have urged their governments to oblige companies processing data to store the data so that they remain potentially available for law enforcement purposes. In Germany, the Federal Government under Chancellor Helmut Kohl already faced requests of the states in 1996 to oblige companies to store various categories of data, but the request was rejected as being out of proportion and unnecessary. The Schröder government followed this course. In spring 2004, the topic made it back on the Government's and Federal Parliament's agenda when the "New Telecommunications Act" was debated. Industry representatives and the Federal Data Protection Officer voiced serious concerns in the hearings before the panel of the *Bundesrat*, the upper chamber of the German legislative branch. In the end, Parliament voted against imposing mandatory data retention obligations on telecommunications providers and Internet service providers, which would have been costly and difficult to control.

In July 2004, the EC launched a consultation on data retention based on an initiative of four EU Member States, among them the U.K. and Sweden, to create an EU-wide regime for traffic data retention (telephone numbers, caller, number reached, time of the connection, etc.). The underlying problem is that Directive 2002/58/EC on Privacy and Electronic Communications does not contain EU-wide rules and

conditions under which traffic data might be retained or otherwise processed for law enforcement purposes. The EC further stated in the consultation document that "[from] a European single market point of view, a proportionate and consistent approach in all Member States is desirable." Consistency would avoid the situation where the providers of electronic communications services are confronted with a patchwork of diverse technical and legal environments. The EC deems it desirable that any data retention measures taken by member states differ as little as possible, in particular in terms of the types of data concerned, the periods of data retention, the technical feasibility of any requirements and the sharing of costs.

The pressure from law enforcement agencies on Brussels to provide for a directive on mandatory traffic data retention significantly increased after the London terrorist bombings in summer 2005. The U.K. Government, being in the chair of the EU Presidency for the second half of 2005, asserted that data retention has already proven invaluable in the investigations into the London attacks. After intense negotiations between the EU Council, the EC and the EU Parliament the EU Parliament finally approved a Directive on 14 December 2005: It requires EU member states to amend their national laws to include far-reaching rules regarding the retention of traffic data by carriers and service providers, including Internet Service Providers (ISPs). Given the fierce resistance of certain EU Member States, industry (that is particularly concerned about the storage costs), privacy advocates, and various national data protection agencies during the discussion, the Directive may be challenged in the courts. The new Directive has three salient features:

- Traffic data for fixed an mobile calls, Internet traffic, including and Internet Telephony (VoIP) and e-mail must be retained by these companies for a minimum of six months and a maximum of twenty-four months. Individual member states may establish retention periods within those parameters. Retention periods can exceptionally be even further extended by member states, subject to approval by the EU. Examples of the data that must be stored are incoming and outgoing phone numbers, the duration of phone calls, IP addresses, which identify a computer's coordinates on the Internet, login and logoff times and e-mail activity details—but not the actual content of communications.
- Member states are not required to reimburse providers for their costs to set up the vast storage system that is necessary to retain the traffic data of approximately 450 million people in case that law enforcement agencies demand the data. This may hurt, in particular, small and medium-sized companies.
- Member states can determine the purposes for which traffic data can be used. The EU Parliament adopted a provision stating that data can be used to prosecute "specified forms" of serious criminal offenses, but not for the mere "prevention" of crime.

The EU Member States must now "transpose" the Directive into their national laws so that it becomes effective. This process could take a year or longer, especially in those member states that do not currently require traffic data retention or require retention only for carriers (not ISPs). The German government is prepared to prescribe a retention period at the lower end of the scale (six months). Other member states may prefer different periods. Retention requirements are likely to vary among the member states. There is every reason to believe that the "patchwork" of retention rules that the EC wanted to avoid will remain in Europe which makes it difficult for telephone carriers and ISPs to provide their services "across the border."

Some Recommendations for International Business

German data protection officials are very proud of the high standard of the protection of personal data and do not view it as a trade obstacle. On the contrary, they believe that protecting personal data of customers and employees against abuse and storing it only and as long as necessary increases consumer confidence and leads to more trust within the organization. The German DPAs are searching the dialogue with industry on privacy issues, which to-date has resulted in a relatively low number of legal proceedings or penalties against companies prosecuted or fined for violation of the data protection law. Critics

argue that data protection law in Germany is still too preoccupied with the concept of data processing within defined physical boundaries, does not leave enough room for company-specific solutions, fails to incorporate new forms of personal data and processing of the same sufficiently, and fails to react appropriately to the risks and opportunities of new data processing technologies. However, the DPAs increasingly are trying to catch up with the legal and technical developments, for instance by searching common solutions on the level of the Article 29 Working Party.

From the business perspective, the damage resulting from privacy and data protection violations can be extremely high; not merely because of potential fines awarded but also because of bad press and the time and money that they must spend in repairing the damage. The following outlines a strategy to ensure data protection and may help to identify the key issues:

INTERNAL AND EXTERNAL HOUSEKEEPING

Step 1: Top management on board?

- Resources and priorities
- CIO/CPO as leader
- Privacy Team: IT, Legal, Auditing, HR, Sales, PR
  - Industry/trade organization self-regulatory initiatives?
  - Classify information collected:
- Personally identifiable or non-personally identifiable?
- Sensitive or non-sensitive?
- Information subject to special requirements (i.e., medical, financial, children under 13, foreign or domestic origin)?

Step 2: Understanding the data flows

- Why, when, where and how is personal data obtained?
- How is the data actually used?
- How is accuracy assured?
- To whom is it disclosed (within the company and third parties)?
- Where is it stored? For how long?
- Who has access?
- Is it secure?
- How is it purged/anonymized? Who is in charge of this?

Step 3: Making the necessary appointments/ filings

- To notify the DPA if the entity stores, uses or processes personal data for a third party "on a commercial basis";
- To appoint a DPO if necessary or if useful;
- To notify the DPA of the DPO appointment;
- To provide the necessary resources so that the DPO can fulfill the tasks;
- To notify the individual if his personal data is stored (exemptions may apply);
- To cooperate with the data protection agencies;
- To store, modify and transfer personal data only in compliance with the data protection law.

FINALLY: KEEPING THE DATA SAFE

Returning to the beginning of this study, the BDSG clearly acknowledges the nexus between data protection and data security: According to the BDSG, companies and organizations that process personal data for their own purposes and for others must implement the "technical and management measures that are necessary to ensure compliance with the BDSG to the extent that these measures are proportionate." A list that is annexed to the BDSG sets forth the details; this list is, however, not exhaustive, which means that DPAs or the companies processing the data on a voluntary basis themselves can adopt measures that go beyond this list. Many DPAs have issued recommendations pertaining to specific data security issues (e.g., on passwords, the use of laptops), which companies are expected to follow although they are not binding in a legal sense. In addition, companies are expected to have a control mechanism in place that ensures measures are actually implemented and remain in place.

Outlook

Companies doing business in Germany and the German DPA face various challenges. In Germany data protection is a human right, as it is in all EU Member States. German citizens and many German companies do not see their personal data as a mere commodity that can be transferred and sold without the prior approval of the individual. Many individuals are very concerned what companies are doing with their data and are worried about "data mining" and data transfers to other countries. However, most German politicians and industry representatives are also well aware that excessive data protection will harm innovation and nourish a vast bureaucracy and red tape.

The question is how to balance these interests. In the future, data protection must be achieved through, rather than despite of, technology. In this regard, data protection is not only a mere cost factor for companies, but can actually enhance technological development and give consumer confidence a boost. Data protection must endeavor to spearhead the development of processes and the design of hard- and software to the objective of data protection and to promote the diffusion and use of technology in line with data protection. Data protection must be integrated into products, services and procedures, as far as this is possible. This means that data protection law can no longer target only those bodies which are responsible for data processing. Data protection law must influence the design of technology right from the development stage. It must call for and promote technology that is in line with data protection requirements. The vision is for companies to create infrastructures that react automatically if data security is compromised. It should use software that provides for pseudonyms and early anonymization. This means that active participation of the industry and a dialogue with the authorities is necessary, rather than a command and control regime. In-house experts and DPOs should be actively involved to create best practice rules, advising the management on how to protect personal data and to participate in voluntary checks.

Excerpt from the BDSG Annex on Data Security

Where personal data are processed or used, an authority or a company must be organized in such a way that it complies with the requirements of data protection. In particular, such measures must be taken that are suitable, depending on the quality and category of the personal data that are protected, to reach this goal:

1. To prevent unauthorized persons from gaining access to data processing systems with which personal data are processed (entry control);
2. To prevent data processing systems from being used by unauthorized persons (user control);
3. To ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access and that personal data cannot be read, copied, modified or deleted by unauthorized persons (access control);
4. To ensure that personal data cannot be read, copied, modified or deleted when they are transferred electronically or transported, and that the data can only be reviewed and verified, at which point or stage of the process a transfer of the personal data by data transmission facilities is foreseen (communication control);
5. To ensure that it is possible to check and establish, after an input, which personal data have been input, modified or deleted into data processing systems by whom and at what time (input control);
6. To ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal (outsourcing control);
7. To prevent unauthorized input into the memory and the unauthorized examination, modification or erasure of stored personal data (memory control);
8. To ensure that data that are collected for different purposes are processed separately.

02

CHAPTER TWO

PRIVACY AND DATA PROTECTION IN THE UNITED STATES

JIM HARPER

The Purpose of the Study

Privacy and data protection are complex issues for businesses to grapple with, even before international considerations are accounted for. The United States and Germany are tied together by strong bonds but they have different histories and cultural traditions as well as different legal and social regimes. This can make emerging Information Age challenges such as privacy and data protection quite confounding for companies doing business in the United States and Germany—and, of course, globally.

The importance of these issues to multi-national companies cannot be overstated. Information is one of the great drivers of innovation in the modern economy. New insights, opportunities, and cost-cutting measures can be gotten by studying data—including personal information about customers and employees. Competitiveness relies on constantly searching out new efficiencies in this way, and companies that fail to improve will fall behind in the global marketplace. This demand often flies directly in the face of requirements for privacy and data protection. Information that is necessarily treated as a commodity in the business community may be seen in some communities as an essential part of people's personalities. Businesspeople and policymakers are struggling to reconcile this tension.

What is covered?

This part of the study examines the different economic, social, and legal actors that influence privacy and data protection practices and laws in the United States, as well as underlying historical and cultural factors that influence these practices. Though it is not a manual for legal compliance, the study addresses many of the more prominent privacy and data protection laws. Finally, this part of the study brings up some likely points of difficulty for companies doing business in both the United States and Germany, and makes recommendations about practices that may help to avoid problems.

The United States is struggling to address the privacy concerns that its people and leaders face. For companies doing business in both places, it is difficult to reconcile the privacy demands while moving forward with a successful and profitable enterprise. But it is essential to do so, as there is no doubt that globalization and data processing will both continue to increase in the coming years.

"Privacy"—Perspectives and Definition

One of the first and most important challenges in a study of privacy is to capture and define the meaning of the terms that are being used. At this early stage in the development of privacy and data protection laws and practices, people use the words "privacy" and "data protection" to refer to many different concepts and consumer interests.

Some conceptions of privacy are very important to data intensive international businesses. These are the focus of this study. Others help explain why privacy is so difficult a challenge for businesses and policymakers who are confounded when consumers express very high demand for privacy practices and privacy laws, but then exhibit indifference through their actions. This is probably because consumers are interested in one "version" of privacy and are offered a different one.

In neither the United States nor Germany have lawmakers, most privacy advocates, privacy professionals and others, distinguished among the different conceptions of privacy. Indeed, there is opposition among some privacy experts to doing so. It is worthwhile, though, to define the many–sometimes conflicting–concepts that fall within the "privacy" and "data protection" rubric.

Among the most important facets of privacy are:

- Autonomy–In the United States, an important but controversial line of judicial decisions dominates public perceptions of privacy. The U.S. Supreme Court's 1973 decision in Roe v. Wade held that a right to privacy found in the U.S. Constitution includes the right of a woman to terminate her pregnancy. The decision itself and subsequent legal cases are not important for students of informational privacy, but the ongoing controversy it engendered is: Some people support very strongly the "right to privacy" because this includes individuals' power to make life-altering, and sometimes life-saving, decisions. Others feel equally strongly that a "right to privacy" is a judicially-imposed subterfuge that allows the killing of unborn children. What these two camps disagree about is better termed "autonomy" and their debate includes deep moral questions about when life begins and for what reasons it may intentionally be ended. It is no wonder that "privacy" evokes such strong emotions; it connotes hot current controversies about personal and bodily autonomy.

- Freedom from Marketing–Many Americans also feel strongly about unwanted marketing. Whether it is e-mail spam, mailboxes filled to the brim with catalogues, or telephone calls during the dinner hour, commercial solicitations raise the ire of a vocal group of consumers and activists who feel that such things invade their privacy. There are two strains to their objections: One takes offense at the inconvenience and annoyance of untimely phone calls, extra trash, and unwanted e-mails. The other objects to the omnipresent commercialization of life in the United States. They would like their homes and e-mail Inboxes to be free of the United States' sometimes crass commercial culture–or at least they would like the power to exclude commerce and advertising from certain places. Responses to the anti-marketing version of privacy generally fall into two categories: In some cases, outright or conditional bans on advertising and commercial solicitation meet this concern. In other cases, a ban on sharing information for advertising purposes is used. Restrictions on data use make potential customers harder to target by marketers.

- Personal Security – In many cases, people use the word "privacy" to indicate interests that might more accurately be termed "personal security." In recent months and years, many businesses that intensively use information about consumers have seen their systems hacked, suffered embezzlement of data, or have lost data to theft of computers or data storage devices. These breaches have often been characterized as threatening privacy. The loss of control over personal information does threaten privacy but, more importantly, these incidents threaten consumers with victimization from identity fraud or other similar crimes. The freedom from crime and other wrongdoing that consumers rightly want is more accurately called "personal security" because it means they are safe and secure from various tangible harms.

- Cybersecurity–Unfortunately, the word "security" may have as many meanings as "privacy." The technical safeguards that companies must take to ensure protection of data are themselves known as "security" or, in the electronic environment, "cybersecurity." Institutional security includes all the steps that an organization must take to protect the

institution's assets, processes, and functions. This includes securing servers and computers inside of locked buildings that are appropriately patrolled; checking the background of employees, if appropriate, and training them to use procedures that protect data; ensuring that technical systems are up-to-date and that new exploits are patched quickly. Security of this kind relates closely to privacy because a company that lacks security cannot be certain of its ability to protect privacy.

- Fairness—People very much want to be treated fairly. This is another important interest that is often referred to as "privacy." In the United States, for example, the Fair Credit Reporting Act is regularly referred to as a "privacy law." Many privacy activists devote a great deal of time to the practices of credit bureaus and credit issuers who arguably too often make lending decisions based on inaccurate information. When decisions are made based on bad information and a consumer has inadequate recourse, this truly is unfair. The response often propounded is to allow consumers access to data about them held by others, along with the right to correct it. These practices are indeed more fair, but they may have adverse effects on security and true privacy because implementing them would open avenues for fraud. Someone falsely claiming to be another person may access the other person's records and, for malicious or criminal purposes, harvest the information in them or amend them one way or another.

- Control of Personal Information—The truest sense of the word privacy probably goes to the power of individuals to control information about themselves and the terms on which it is shared. Decisions about information-sharing are rarely articulated—people make most privacy decisions based on a "gut" reaction to the circumstances. Their decisions tend to be highly dependent on culture, custom, upbringing, and experience. Most Americans and Germans routinely think nothing of sharing the appearance of their faces, hair, and arms with others, while in some other cultures doing so is taboo. In some families, a son's or daughter's dating life might be a topic of dinner table discussion, while in others it is never discussed. Some individuals may care nothing at all whether their personal income is known to friends and neighbors, while others may guard such information strictly. These are all examples of the boundary setting that amounts to protection of individual privacy. Prior to the 9/11 attacks on the United States, this version of privacy was often advocated for as a relatively absolute "right." The post-9/11 demand for security and concomitant responses of the United States Congress illustrated that privacy of this kind exists on a continuum with other values and interests, including national security. Privacy is now dealt with as more of an economic good that may have costs to other interests like national security.

- Confidentiality—Though very close to privacy, confidentiality differs in important ways. A pledge of confidentiality is a promise not to share further information that has already been shared. For example, medical offices and financial services providers have traditionally performed many of their services subject to a pledge of confidentiality, meaning that a patient or customer can be confident that his or her privacy interests are protected. Thus, confidentiality protects privacy because it allows sharing consistent with what the customer or patient likely wants, and no further. Though assumed (or implied by contract) confidentiality has been eroded somewhat by a number of U.S. federal regulations, it probably remains a significant source of privacy protection. Some institutions promise confidentiality somewhat disingenuously: When governments have mandated the collection of information, they will often put confidentiality rules in place. Because the individual has not been in a position to decline information-sharing, this confidentiality promise does not create privacy. The limits it places on further disclosure are only as strong as the good faith of the agency in the face of changing government priorities.

Privacy has many different facets and it is important to understand them all. The international business that must comply with laws in multiple nations, and serve consumers worldwide as well, must understand

which true interest is being served by different privacy and data protection practices. Doing so will mean better decisions, an easier time with legal compliance, and a more profitable enterprise.

The Roots and Political Context of Privacy and Data Protection

In the United States, many of the different conceptions of privacy discussed above took root and multiplied in the late 1960s and early 1970s during a wave of concern about the use of personal information in computer systems. However, privacy got its start much earlier. Starting with concerns about governmental power, it has changed and expanded in response to concerns with technology.

Individual rights and interests have a strong pedigree in the United States. The nation was founded in a revolution against what was viewed as the oppressive and out-of-touch government of King George's Britain. The Founding Fathers, authors of the Declaration of Independence and the Constitution, were students of the Enlightenment thinkers. They adopted the English common law, but otherwise designed a radically different governmental system from England's—with limited national authority, and with branches of government, and levels of government, pitted against one another for power. This was intended to leave maximal freedom and responsibility to individuals.

For most of America's subsequent history, the country has grown in size and population to cover much of the large expanse known as North America. This "Westering" movement and Manifest Destiny fostered a sense of growth, independence, individualism, and personal responsibility among the American people that persists in many quarters, even if the settlement of the West is now only a chapter in the history books. This background leaves the United States with several distinct features that appear in its approach to privacy and data protection. This first is the fact that the rules governing the public and private sectors are different. The public sector is governed by constitutional rules like the Fourth Amendment, discussed in the next section. The Fourth Amendment has been updated in light of modern technology, though significant holes have opened in its protection.

The private sector, on the other hand, has traditionally been governed by common law rules, including the privacy torts. Markets have been left relatively unfettered, subject to the simple caveat that one may not harm another's legally recognized interests.

With the early dawn of the computer age in the late 1960s and 1970s, the United States began moving toward civil-law style regulation, rather than tort law, to pursue privacy values. Many of the influential studies and papers in this movement are discussed below, followed by the major privacy-oriented regulations that exist today.

THE FOURTH AMENDMENT

Consistent with the independent culture that characterizes America's founding and early history, the Founders included in the Bill of Rights language that stands as a key bulwark of privacy against governmental intrusions. The Fourth Amendment says:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Since it has been applied to the states, the Fourth Amendment has served as the primary, essential limit on the power of governments in the United States to inquire into people's lives, arrest them, and take their property.

The Fourth Amendment requires a search to be based on probable cause. That is, government investigators must have a rational belief that a crime has been committed and that evidence or fruits of the crime can be found in the places they plan to search. Until 1967, the Fourth Amendment largely protected places—namely the home and the areas closely surrounding the home. When the Bill of Rights was drafted, the United States was a low-tech, mostly agrarian, and relatively immobile society. The home really was a person's castle.

THE FOURTH AMENDMENT MODERNIZED

As America has become more mobile and technological, this early interpretation has had to change. After a long delay created by Olmstead v. United States, a 1928 case that declined to give Fourth Amendment protection to telephone communications because the wire they travel on is outside the home, accommodations to modern technology and lifestyles have occurred. Katz v. United States is the landmark Supreme Court decision that updated Fourth Amendment law in light of progress.

In Katz, FBI agents placed electronic eavesdropping equipment on the outside of a telephone booth where the defendant, a bookmaker, conducted his business. The Court held that eavesdropping on Katz in this way without a warrant violated his Fourth Amendment rights because he justifiably relied on the privacy of the telephone booth. The Court stated, in a famous passage, "[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection ... But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

Justice Harlan's influential concurrence described a two-pronged test to determine when a person is entitled to assert Fourth Amendment protection. Harlan suggested, first, that a person should have exhibited an actual, subjective expectation of privacy. Second, the expectation must be one that society is prepared to recognize as reasonable. This test has been the dominant test in challenges to government invasions of privacy ever since.

A 2001 Fourth Amendment case illustrates how protections against government privacy invasions have continued to develop. In Kyllo v. United States, agents of the U.S. Department of the Interior, suspicious that Danny Lee Kyllo was growing marijuana in his home using high-intensity lamps, had aimed an Agema Thermovision 210 thermal imager at his home. The imager detected significantly more heat over the roof of the garage and on a side wall of Kyllo's home than elsewhere on the premises. Based on this information, the agents, suspecting a marijuana growing operation, got a warrant, searched the home, and found the drugs they suspected.

The Supreme Court reversed Kyllo's conviction, finding that when a novel device like the thermal imager is used "to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."

In remanding Kyllo's conviction, the Court essentially found that the reasonableness of a search is to be judged in light of common privacy-protecting practices, not in light of privacy protection from the best technologies available. Thermal imagers are not in general public use so people desiring to keep the hours of their sauna private from neighbors do not line their walls with asbestos. The government's search of Kyllo's home using newfangled technology was not a reasonable search within the meaning of the Fourth Amendment.

Although cases like Kyllo show that the Supreme Court will update the Fourth Amendment in light of new technology and modern practices, it has not always done so.

HOLES IN FOURTH AMENDMENT PROTECTION

In the early 1970s, Congress passed a law called the Bank Secrecy Act, which authorizes the Treasury Department to require financial institutions to maintain records of personal financial transactions that "have a high degree of usefulness in criminal, tax and regulatory investigations and proceedings." It also authorizes the Treasury Department to require any financial institution to report any "suspicious transaction relevant to a possible violation of law or regulation." These reports, called "Suspicious Activity Reports" are filed with the Treasury Department's Financial Crimes Enforcement Network ("FinCEN").

This is done secretly, without the consent or knowledge of bank customers, any time a financial institution decides that a transaction is "suspicious." The reports are made available electronically to every U.S. Attorney's Office and to fifty-nine law enforcement agencies, including the FBI, Secret Service, and Customs Service. A law enforcement agency does not have to be suspicious of an actual crime before it accesses a report, and no court order, warrant, subpoena, or even written request is needed. Law enforcement agencies can, and allegedly do, down-

load the entire harvest of new information from FinCEN whenever they want it.

This law was ratified by a pair of Supreme Court cases in the early 1970s that neatly two-stepped around the Fourth Amendment issues. In California Bankers Association v. Shultz and U.S. v. Miller, the Court denied individuals the right to sue to prevent information being collected for Bank Secrecy Act reporting purposes because it did them no harm. Then, the Court denied individuals a Fourth Amendment claim about that information being passed to the government because it was held by third parties. In other words, the government could require the information to be collected by a third party, then require the third party to turn it over to the government, though Fourth Amendment law fairly clearly would not allow this to happen directly.

Except for the prohibition against slavery in the Thirteenth Amendment, the Constitution, Bill of Rights, and other amendments apply only to government actors. Privacy protection against non-governmental actors has seen parallel developments, however.

PRIVACY AND THE PRIVATE SECTOR

While the Fourth Amendment has been evolving to protect individuals from government privacy depredations, so have the legal responses to privacy threats from the private sector. As on the government side, protections against private actors were grounded in property protection during the United States' early history. But with the advance of technology, the growth of modern, impersonal businesses, and a more diverse social culture, privacy law has advanced to protect individuals' interests from incursions by their peers.

From 1890 until about 35 years ago, privacy protection in the United States was dominated by the development of common law privacy protections. With the onset of computer processing in the late 1960s and early 1970s; however, a new urgency was placed on privacy protection. A series of studies introduced ideas for legislative and regulatory privacy protection. (This coincided with the blossoming of "privacy" from a fairly narrow set of issues dealing with control of personal information to the wide variety of data protection topics it encompasses today.) Though some legislation passed at that time, most notably the Privacy Act of 1974, interest in privacy protection waned until the birth of the Internet in the mid-1990s. At that time, many of the ideas that had been born in the 1970s came forward again as paradigms for protecting privacy in the Information Age.

THE COMMON LAW

In American law, a tort is a private or civil wrong or injury. It is the violation of a duty that the law imposes upon all persons in a certain situation or in a certain relationship to other people. A person commits a tort when he or she performs an act that is recognized by the law as wrongful toward others and for which the remedy is a private legal action.

The general tort law in the United States has been detailed in a document called the Second Restatement of Torts, issued by the prestigious American Law Institute. The ALI was organized in 1923 to address the uncertainty and complexity in American law. Between 1923 and 1944, Restatements of the Law were developed for many areas of law, including torts; many judges and states recognize the Restatement as an influential guide to the law. In 1952, the organization began a second round of Restatements, and the Second Restatement of Torts remains authoritative today. A third series of Restatements was begun in 1987.

The law of torts is largely a product of the common law, which the United States inherited from England during the colonial period. Common law derives from generation after generation of judicial decisions extending back into pre-history. Judges in common law courts draw on precedent from past cases to determine the just course in present cases. The common law generally reflects the longstanding historical usages and customs that have protected individuals and their property in our society. When it has not been reissued in legislative enactments, common law draws its authority from both its deep

roots and its close relationship to western notions of fairness and justice.

Common law is distinct from civil law, which is the dominant legal tradition in continental Europe. Civil law is generally comprised of statutes and codes written (historically) by emperors and kings, and (today) by legislatures. In the past, civil law catalogued the norms of a relatively static society. Modern civil law reflects the best efforts of legislators to articulate the law that will serve all of a society's diverse interests going forward. Bright minds must try to figure out in relative abstraction what the law should be.

Though it does so slowly, the common law evolves and changes as conditions change or as history reveals past decisions to be unjust. Some lines of cases die out; others join together to form new legal theories. The common law incorporates the wisdom of generations of judges, and the lawyers who have argued before them, working through real controversies between real litigants to balance competing interests and achieve just results in an evolving society.

THE PRIVACY TORTS

One relatively recent change in the common law has been the emergence of the American privacy torts. Unlike many other torts, which have ancient roots, the privacy torts have a discrete foundation that is only about 115 years old: an article called The Right to Privacy, published in the 1890 *Harvard Law Review*.

The authors of the article, Samuel D. Warren and Louis D. Brandeis, were concerned with the rise of newspapers, photography, and other technologies that have the potential to expose people's images and personal information to the public. Warren and Brandeis argued that the next step in evolving legal protections for the individual should be explicit protection of privacy. The two compared the contours of explicit legal privacy protection to the law of defamation, to physical property rights, to intellectual property, and to the law of contracts. (Years later, as a Supreme Court Justice, Brandeis dissented from the Olmstead decision, mentioned earlier, which declined to extend Fourth Amendment protection to telephone communications that had been wiretapped.)

Their key concern was with publicity given to sensitive personal information—undesirable and embarrassing scrutiny of private life by the press and public. (Warren and his family, notable Boston "blue bloods," had been embarrassed and annoyed by newspaper coverage of their lives.) Privacy as discussed by Warren and Brandeis did not extend to matters that were of legitimate public or general interest. Publication of facts by the individual concerned, or with that person's consent, cut off that person's right to privacy in that information.

In 1960, eminent legal scholar William L. Prosser documented how privacy as a legal concept has come to constitute four distinct torts. That is, a person whose privacy has been invaded in any of four different ways can sue the invader for damages. These torts still exist today, and are roughly contoured as follows:

- Intrusion upon seclusion or solitude, or into private affairs—The tort of intrusion had its foundation in wrongful entry upon places were private life was being conducted. An early precursor, for example, was a case involving a man's entry into a room where a woman was giving birth. The principle has been carried beyond places and belongings and an intrusion tort may occur when someone eavesdrops using microphones or wiretaps, and when someone peeps through the windows of a home.

  An intrusion probably has not occurred when someone makes excessive noise or exhibits bad manners and obscene gestures. The intrusion tort is not implicated when the matters observed can not be accurately called "private," as when someone is observed or photographed on a public street.

- Public disclosure of embarrassing private facts—The public disclosure of private facts cause of action is probably most like what Warren and Brandeis worried about in their *Harvard Law*

Review article, and it is important today because large amounts of personal information can be collected and disseminated using digital technologies. It allows a person to sue if highly sensitive information about him or her is publicly disclosed. Early cases involved revelation of a woman's past life of prostitution in a movie that identified her by name, publicity given to debts, and publicity given to medical pictures of a person's anatomy.

There are some key limitations on the disclosure tort. First, the disclosure of private facts must be a public disclosure, not a private one. In other words, communicating information to small groups or legitimately interested parties is unlikely to be actionable. Second, the facts disclosed must be private facts. Publicity given to information that is open to the public eye will not give the subject of the publicity a cause of action. Third, making the information public must be an act that would offend a reasonable person of ordinary sensibilities. A person with peculiar sensitivity to exposure will not be able to successfully sue someone who publicizes unremarkable or clearly favorable personal information.

- Publicity which places a person in a false light in the public eye—The false light privacy tort protects people against being cast in a false light in the public eye. It has often been used when people's photographs have been exhibited in ways that create negative inferences about them. People have successfully sued when they have wrongly been associated with cheating taxi drivers, "profane" love, juvenile delinquents, or drug dealing. Like the disclosure tort, a false light complaint must be about publicity given to negative implications that would be objectionable to the reasonable person. The subjective feelings of the highly sensitive are not protected. The tort is similar to defamation, but it goes more to the peace of mind of the individual than to his or her standing in the community.

- Appropriation of one's name or likeness—The appropriation tort prevents exploitation of attributes of a person's identity for commercial gain. It arose in an unusual way, when the legislature in New York sought to overturn a decision by that state's highest court. In a 1902 case, the New York Court of Appeals refused to recognize the privacy torts urged by Warren and Brandeis. The defendant had used an attractive woman's picture, without her consent, to advertise flour. The decision denying her recourse brought a storm of disapproval, and the legislature passed a statute making it both a misdemeanor and a tort to use any person's name, portrait, or picture in advertising or trade. Many other states passed similar such laws, and in other states courts adopted the tort as a part of the common law.

  A successful suit under the appropriation theory must be based on use of the plaintiff's identity, not just coincidental use of the same name. Something must tie the communication to a particular person. In statutory cases, the appropriation must be for pecuniary advantage, but the common law cases may not be so restrictive.

As Prosser emphasized, the four branches of the privacy torts are very different from one another, and they apply differently in different situations. But they are explicit privacy-protecting law that exists in most of the United States. Prosser was not totally enamored with the privacy torts. The link among them—the idea that people have a right "to be let alone"—is slightly tenuous for legal theory. Prosser warned that the different ways each branch of the tort might apply could easily lead to confusion.

THE COMPUTER AGE

Prosser's work on the privacy torts in the late 1950s and early 1960s showed privacy to have been grounded up to this time in protecting people's reputations. But, by the mid-to-late 1960s, the computer age was dawning. Governments and corporations were beginning to acquire large mainframe computers that had impressive computing and data-storing abilities for that time. Concerns with privacy were beginning to surge along with suspicion of corporate power.

A prominent early book from this era was Vance Packard's *The Naked Society* (1964) which sounded

an alarm about techniques corporations were using to gather personal information about consumers. Earlier, Packard had written *The Hidden Persuaders* (1957), discussing the manipulations used by marketers. The conjunction of privacy concerns with concerns about marketing, commerce, and corporate influence were prominent during the counter-cultural late 1960s and early 1970s, and they persist among many privacy advocates today.

The most lastingly influential book during this period was Alan Westin's *Privacy and Freedom* (1967). The book opens with one of the best general theories of privacy yet put into print: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." The first chapter also reviewed privacy from a sociological perspective, including discussions of information-sharing and protecting behaviors among non-Western people who live very differently from modern Americans and Europeans.

Other chapters, however, showed how a surfeit of different concerns animated modern "privacy" debates. Personality testing, for example, was among the topics given ample discussion. The privacy threats from spike microphones, phone taps, and parabolic microphones were fairly heavily explored while "data surveillance," a substantial concern today, got relatively short shrift (in hindsight, of course). A brief section on "The Computer and Privacy" laid out important early thinking on what came to be the "Fair Information Practices" vaunted by so many privacy advocates.

Interestingly, Westin's concerns were prompted by the existence of just one or a small number of mainframe computers exclusively in the hands of large institutions. Westin wondered whether "the organs of criticism [would] get their own computers and try to monitor selectively the operations of the big public and private systems. . . ." Obviously, this question has now been answered: Computers are ubiquitous in the Western world, they are networked via the Internet, and blogging is one among many social practices that counterbalance the power enjoyed by large institutions.

The U.S. government responded to the growth in privacy concerns by convening a study. The Secretary of Health, Education, and Welfare asked a group to peruse the issues and in mid-1973 the Secretary's Advisory Committee on Automated Personal Data Systems issued a report called Records, Computers and the Rights of Citizens. The "HEW report" summarized personal privacy as follows:

> An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law.

The HEW report dealt extensively with the use of the Social Security Number as the issues stood at that time. The report advocated the following "fair information practices":

- There must be no personal-data record-keeping systems whose very existence is secret;
- There must be a way for an individual to find out what information about him is in a record and how it is used;
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;
- There must be a way for an individual to correct or amend a record of identifiable information about him;
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

This appears to be the formal debut of the concept of "Fair Information Practices," the varied suite of policies often put forward as privacy protection.

The intellectual content of this report formed much of the basis of the Privacy Act of 1974. This law, passed hastily in the final week of the 93rd Congress, is codified at 5 U.S.C. § 552a (2000). It took effect on 27 September 1975 and attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies.

The Privacy Act is intended to provide individuals with broad protection from the unauthorized use of records that federal agencies maintain about them. It requires agencies to account for disclosures of records that it maintains, and to take steps to minimize and protect the accuracy of records. It also requires agencies to reveal the purposes for which they are collecting information and gives individuals a right to gain access to records about them. Individuals may sue in federal District Court if their rights under the Privacy Act are violated. There are criminal penalties for knowing and willful violations of the Act.

The U.S. Justice Department's May 2004 overview of the Privacy Act says that its "imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it difficult to decipher and apply." The Privacy Act is an extremely long statute riddled with exceptions and caveats. Privacy Act statements, which are required on the forms used to collect information from citizens, are insufficient in that they do not remind citizens that uses of information can be changed merely on notice published in an obscure publication called the Federal Register. A liquidated damages provision was recently read out of the Privacy Act by the Supreme Court in a case called Doe v. Chao. The laudable intentions of the Privacy Act have not borne themselves out.

Section 5 of the Privacy Act of 1974 established the U.S. Privacy Protection Study Commission which was intended to evaluate the statute and to issue a report containing recommendations for its improvement. The Commission issued its final report, Personal Privacy in an Information Society, and ceased operation in 1977 without having a significant further influence on American privacy law.

Meanwhile, the Organization for Economic Cooperation and Development (OECD) in Paris had picked up an interest in privacy and data protection. In 1980, it issued a set of guidelines that expanded on earlier sets of "fair information practices" and that have had an important influence on current privacy debates. The Guidelines involve eight "principles":

- Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject;
- Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date;
- Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose;
- Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle, except:
  - with the consent of the data subject; or
  - by the authority of law;
- Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data;
- Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller;

- Individual Participation Principle: An individual should have the right:
  - to obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
  - to have communicated to him, data relating to him
    - within a reasonable time;
    - at a charge, if any, that is not excessive;
    - in a reasonable manner; and
    - in a form that is readily intelligible to him;
  - to be given reasons if a request for information is denied; and
  - to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended;
- Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

For ten years following the issuance of the OECD guidelines, major privacy developments were scarce; there were occasional bursts of privacy activity. The controversial nomination of Judge Robert Bork to the Supreme Court in 1987, for example, included an episode when an attempt was made to retrieve his video rental records, which led to adoption of the Video Privacy Protection Act.

The Act forbids a video rental or sales outlet from disclosing information concerning what tapes a person borrows and buys, or releasing other personally identifiable information without the informed, written consent of the customer. The Act also requires such outlets to provide consumers with the opportunity to opt out from any sale of mailing lists. The Video Privacy Protection Act allows consumers to sue for damages if they are harmed by violations of the Act.

In 1995 the European Union's Data Protection Directive was issued. Though it is not law in the United States, it is an important document in privacy debates today. The directive requires member countries of the EU to adopt laws that implement its terms. It represents the first attempt at wide implementation of a set of fair information practices and it has influenced the direction of privacy debates worldwide. For the ensuing ten years up until today, EU member states have grappled with the challenge of implementing the Directive's provisions. Some have adopted them readily, while others have resisted them and a few have yet to enact law as required by the Directive.

The Directive creates rights for persons about whom information is collected, known as "data subjects." Entities that collect information must give data subjects notice explaining who is collecting the data, who will ultimately have access to it, and why the data is being collected. Data subjects also have the right to access and correct data about them.

The Directive creates stricter rules for companies that want to use data in direct marketing, or to transfer the data to other companies for that use. The data subject must be explicitly informed of these plans and given the chance to object. Stricter rules also govern sensitive information relating to racial and ethnic background, political affiliation, religious or philosophical beliefs, trade-union membership, sexual preferences, and health. Before this information may be collected the data subject must give explicit consent. There are exceptions to this rule for employment contracts, non-profits, and the legal system, among other things.

In order not to completely disrupt life in Europe, the Directive has a wide variety of exceptions. For example, data may be kept for personal and household use like an address book. Synagogues, trade unions, churches, and other non-profits are permitted to keep even "sensitive" information about their members. National governments are permitted to exempt journalists from provisions of the directive if the government thinks free speech might outweigh privacy interests.

Unlike in the United States, where data use by governments is generally regulated by special privacy and freedom of information acts at both the state and federal level, European governments may exempt themselves from the Directive when it conflicts with their own interests in taxation or law enforcement.

In order for American companies to transfer information about data subjects with European businesses, the EU and the U.S. Commerce Department negotiated an agreement. Called the "Safe Harbor" agreement, it outlines the conditions under which U.S. companies may receive information about EU data subjects.

Though it was certainly inspired by the discussion of privacy concerns that originated in the early 70s, the EU Data Protection Directive went into effect just as a new era of privacy concerns was dawning.

THE INFORMATION AGE

In 1994, the Internet began its popular ascendancy with the creation of the Mosaic World Wide Web browser by students at the University of Illinois at Urbana-Champaign. The invention of this point-and-click graphical interface allowed millions of consumers to learn quickly how to navigate among sites on the Internet. Internet companies quickly began adopting varied and interesting fonts, colors, graphics, and images.

The public came to recognize quickly that the Internet was an incredible information resource. Almost as quickly, the public realized the Internet's ability to capture and record information about them, and the modern wave of privacy concerns was born.

As computers would soon be ubiquitous—in cars, phones, televisions, toys, and so on—this era of privacy concern is better identified as occurring with the beginning of the Information Age. Concerns with privacy did not limit themselves to computers or the Internet. Privacy practices economy-wide came under scrutiny—and they remain under scrutiny today. In the United States, the response has been to enact regulatory provisions in discrete areas of the economy where sensitive information or sensitive individuals are at issue.

The first milestone in this new era of privacy concern was the U.S. Congress' call for privacy regulation in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Some of the factors that prompted this action were concerns about how data would be used in modernized electronic data interchange systems for health care, concerns about the use of data by health maintenance organizations, changes taking place in the health care market, and agitation by pro-regulatory groups.

Congress did not capture what it meant by privacy in the law. Rather, HIPAA had a provision called "Recommendations with Respect to Privacy of Certain Health Information." This section asked the Secretary of Health and Human Services to make recommendations to Congress about the privacy of individually identifiable health information. Congress asked what rights people should have with regard to such information, the procedures that should be used to enforce those rights, and the uses and disclosures of such information that should be authorized or required. In the event Congress did not act on that advice, the Secretary of HHS was to go ahead and write into law whatever the recommendations were.

The HHS Secretary's original report on privacy put forward five broad "principles" for federal legislation. Like so many modern "privacy" efforts, they ranged across a wide variety of consumer interests with respect to information:

- Principle 1: Boundaries—This was the idea that "[a]n individual's health care information should be used for health purposes and only those purposes ... It should be easy to use information for those defined purposes, and very difficult to use it for other purposes." This principle promotes confidentiality and, thereby, privacy in its truest sense;
- Principle 2: Security—HHS summarized this concept as protecting information against "deliberate or inadvertent misuse or disclosure." This, of course, promotes privacy by seeking to prevent inadvertent disclosure, but also promotes personal security by preventing data from being used in fraud;
- Principle 3: Consumer Control—"Patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them." This principle sought to promote fairness, by allowing consumers to correct information that might be used in decision-making about them, as well as personal security because, in the medical records context, wrong information can lead to wrong diagnoses and treatments;

- Principle 4: Accountability–"Those who misuse personal health information should be punished, and those who are harmed by its misuse should have legal recourse";
- Principle 5: Public Responsibility–"Individuals' claims to privacy must be balanced by their public responsibility to contribute to the common good, through use of their information for important, socially useful purposes..." This fascinating "privacy" principle articulates a wide variety of reasons why people should not have privacy. The detailed list produced by HHS included health oversight, public health purposes, research, emergencies, to maintain state health data systems, to provide information to next-of-kin, for directories, for law enforcement to use against third-party payers, for law enforcement to use against individuals, for use in judicial proceedings, and so on.

With Congress failing to act on medical privacy legislation before the self-imposed deadline in the HIPAA law, the Clinton administration went ahead and issued a proposed health privacy regulation. It issued its proposed rule in December 2000, following the model set forward in the HHS report and addressing a wide range of information policy interests.

The Children's Online Privacy Protection Act (COPPA) was the next major effort in Congress to protect against privacy concerns. Passed as part of an omnibus spending bill in 1998, it took effect in April 2000.

COPPA requires "verifiable parental consent" before a commercial website operator may collect information like e-mail addresses from children. For the internal use of the website, this means getting an e-mail from the parent. For other uses, this means talking to a parent, or getting a parent's snail mail, fax, or credit card number.

Congress passed this law in the absence of evidence that collection of information by commercial websites harms children in any recognized way. In fact, commercial websites pose little danger to children because they stay in business by making children and their parents comfortable and safe. The true reason for the law was to prevent children from receiving too much marketing via the Internet. This is another illustration of the wide variety of interests advanced in the name of "privacy."

The final major legislative reaction to privacy concerns was the Financial Services Modernization Act, also known as Gramm-Leach-Bliley (GLB). In November 1999, Congress passed this long-awaited regulatory modernization bill for the financial services industry, but the new financial combinations it enabled created concern that sensitive financial information about consumers would be shared too easily and too broadly. Title V of GLB set forward a stringent set of guidelines that restrict the use of consumer information by financial institutions.

The GLB Act added new regulations in four main areas: disclosure of privacy policies; "opt-out" of information disclosures to non-affiliated third parties; non-disclosure of account information; and standards to protect security and confidentiality of consumers' non-public information.

- First, the GLB Act requires institutions to annually disclose their privacy policies to consumers. This disclosure must be prominent and must be made to all customers either when the customer begins his or her relationship with the institution or on an annual basis to existing customers. The disclosure must also contain the institution's policy regarding the categories of non-public personal information it collects, its disclosure policy of non-public personal information to third parties and affiliates, and the categories of entities that receive the information.
- Second, the GLB Act gives consumers the right to "opt-out" of allowing the institution to send non-public personal information to nonaffiliated third parties. Even if the consumer does not opt-out, third parties may not re-disclose this information. There are exceptions to this opt-out rule, and for good reason. This provision does not apply to the sharing of information with third parties to process statements or service customer accounts. Opt-out is also unnecessary when information is transferred to complete transactions authorized by the customer, when disclosing customer information to a credit bureau, complying with a regulatory investigation by state or federal authorities, or to protect against fraud. Opt-outs are also not required for

institutions that want to share information with affiliates—companies that are closely related through ownership by a parent company. This rule applies to all companies, not just financial institutions.

- Third, the GLB Act flatly prohibits institutions from sharing account numbers or other similar identification numbers or codes with non-affiliated parties for the purposes of telemarketing, direct mail marketing, and marketing through e-mail solicitations.
- Finally, the GLB Act requires financial institution regulators to establish standards to ensure the confidentiality and security of consumer records, protect against threats to the security of those records, and protect against unauthorized access to those records that could result in substantial harm or inconvenience to the consumer. The separate regulation that was issued under this provision is called the "Safeguards Rule."

The GLB Act's sweeping definition of "financial institution" means any regulated financial company or business that engages in financial activities. It includes banks, bank holding companies, securities firms, insurance companies, insurance agencies, thrifts, credit unions, mortgage brokers, finance companies, and check cashers. In addition, because of the way GLB defines "financial activities," these protections may extend to travel agencies and even real estate brokers.

An important amendment to the GLB Act, added at the very end of the legislative process, allowed states to regulate financial services in ways that provide greater protections. Since the passage of the law, there has been a good deal of regulatory activity in the states, especially in California. This has prompted Congress to revisit financial privacy issues in the recent Fair and Accurate Credit Transactions Act, but debates about how financial services should be regulated in the name of privacy are sure to continue.

The spate of regulations aimed at protecting privacy in the past ten years, including the GLB Act, COPPA, and HIPPA, are rather different from the approaches used in the past. Privacy has deep roots in U.S. legal traditions and in American society. Historically, privacy protection has been bound together with property protection. But, as technology changed American lifestyles in the twentieth century, privacy broke free and began to gain freestanding legal protection.

Common law evolution did not keep up with privacy and related concerns—or at least it was not perceived to—beginning in the late 1960s and early 1970s. Since then, a number of advisory, legislative, and regulatory bodies have advocated panels of policies under the heading of "privacy," though most of them extend to a relatively broad array of consumer interests.

Unlike Europe, the United States has declined to adopt an overarching privacy or data protection law. Rather, a series of statutes aimed at privacy for particularly sensitive types of information (or vulnerable populations) have been passed.

In the remaining areas, market forces hold sway over information practices. Though naturally legislators and regulators have a significant role in privacy and data protection law and practice, the consumer is the most important actor in U.S. privacy protection. It is with the consumer that we start our analysis of the key institutions and actors in U.S. privacy protection.

Key Institutions and Actors

Though many are not well recognized, a surprising number of institutions and actors influence privacy and data protection law and practices in the United States. There are two main groups of actors: private and public. Private actors include consumers, of course, consumer advocates, the media, pollsters, seal organizations, privacy officers, and investors. Public actors include lawyers and courts, public consumer protection bodies and regulators, and, of course, legislatures.

The starting point for analysis is the consumer. Regardless of the recent growth of regulation as a determining factor in the design of products and services, consumers exercising their choices in the marketplace remain the dominant actors.

Consumers are not alone in making decisions. The phrase caveat emptor—"buyer beware"—has come to symbolize the lone consumer haplessly fighting large corporations. But this image is inaccurate. A variety of social systems attend to the interests of the American consumer. Multiple actors inform consumers directly about privacy (and numerous other concerns) and influence the business community and each other to attend to consumer interests.

Ideally, the ultimate choice remains with the consumer because no one but the consumer can make the final decision about which mix of product characteristics are best for him or her. Examining the interplay among institutions and actors reveals that the consumer making a decision for him- or herself is hardly alone.

Meanwhile, a variety of public institutions seek to make privacy-protective choices for consumers. Public agencies and officials see opportunity to win credit from the public and increase their stature and power by stepping in to protect privacy on behalf of consumers. They use existing law, oversight, and sometimes new law and regulation to drive privacy and data protection practices in the direction they think it should go.

CONSUMERS

Unfettered competition among firms tends to keep profits very low. This means that businesses focus intensely on what they can do to increase their profits, even by small amounts. They will do almost anything they can to bring in new consumers or avoid losing current ones. Businesses in competitive markets survive on the margins, seeking the small increase in revenue that comes from getting a new customer while retaining existing ones. They constantly study what may alienate or please consumers; privacy and data protection are among the many factors they study.

Consumers are the primary actor that helps determine appropriate privacy and data protection policies. They reward the companies that serve their interests by spending their dollars with them, and they punish those companies that do not.

In addition, a small, but influential, contingent of consumers contacts companies directly with their questions and complaints. Angry consumers are hugely influential when their letters or phone calls reach the CEO, the corporate counsel, the marketing executive, or the product manager who realizes the learning opportunity embedded in a complaint. These consumers stand in the shoes of the great mass of consumers who may have only a mild preference for high privacy protections.

To be certain, not every consumer demands privacy. And consumers that ask for greater convenience, lower prices, custom products, and knowledgeable customer service are pushing back against the demands of the privacy-absolutists. But if privacy-demanding consumers are motivated enough, they represent a distinct market that there is profit in serving. A company may offer a separate product that has protection of privacy as a key feature.

CONSUMER ADVOCATES

As Alexis de Tocqueville famously observed in *Democracy in America*, the United States has a wealth of civil society groups dedicated to advancing the arts, education, mutual aid, religious and moral uplift, and nearly every other community and social interest. The U.S. federal tax code exempts from taxation corporations and foundations that are dedicated to religious, charitable, scientific, literary, or educational purposes, as well as the promotion of public safety, sports competition, and the prevention of cruelty to children or animals. State and local tax laws also often exempt such organizations from taxes.

There are many groups that are devoted to consumer welfare or civil liberties generally, and many dedicated specifically to privacy. Examples of such groups include the American Civil Liberties Union, Consumers Union, the Consumer Federation of America, and many others. Groups dedicated specifically to privacy and similar interests include the Electronic Frontier Foundation, the Electronic Privacy Information Center, the Privacy Rights Clearinghouse, Consumers Against Supermarket Privacy Invasion and Numbering, the Consumer Project on Technology, the Coalition Against Unsolicited

Commercial E-mail, and more. Many more groups are devoted to the development of law and public policy, including the Cato Institute, the Center for Democracy and Technology, the Competitive Enterprise Institute, the Progress and Freedom Foundation, Privacilla.org, and many others. Some of these groups incorporate economic study and theory into their work, finding generally that market processes discern consumers' privacy interests better than regulation.

These groups use a variety of methods to influence consumers and other actors. Some are membership organizations: their mailings and e-mail communiqués get the word out. Many have close relationships with the media. Media outlets sometimes avidly report on privacy concerns, and consumer groups reach a broader audience that way. Many file legal complaints with regulatory agencies like the U.S. Federal Trade Commission, state departments of consumer protection, and state attorneys general. Many participate in legislative hearings that focus on specific issues in privacy and data protection.

Though many of these groups believe fervently that they know what protects consumers, they are actually engaged in a contest to win consumer attention and action. More often that not, their complaints about corporate privacy practices fall on deaf ears or merit only passing attention from the community at large. (They are still influential in these cases because the companies that they complain about must carefully consider whether their practices are worth the risk of bad public relations and potential lost customers.) But once in a while, agitation from these groups meets its mark. When it does, a wide array of institutions and actors pounce on the issue and the whole community learns a lesson about which information practices are tolerable and which ones are not.

The most famous such case is DoubleClick. DoubleClick is an online ad serving company that caused a firestorm in late 1999 when it announced plans to combine click-stream information with information in a "real world" database it had acquired called Abacus. The Abacus database contained demographic and contact information on millions of consumers. By combining Web surfing information with lifestyle and contact information, DoubleClick's plan would have delivered highly customized and targeted advertising to consumers.

American consumers were only just beginning to familiarize themselves with the Internet, and this plan was too much too soon. Reaction to the plan was harsh and swift. Only three months later, in March 2000, DoubleClick announced that it would not go forward with this custom-marketing plan. No click-stream information was ever combined with offline information and, as the Federal Trade Commission found, no consumer's privacy was ever invaded. Having pushed the envelope a bit too far without explaining the benefits of its plan to the public, DoubleClick exercised good corporate judgment and relented.

Consumer advocates played a pivotal role in stopping the DoubleClick-Abacus combination and teaching the business community as a whole that tracking Web surfing and tying it back to people for marketing purposes is not an acceptable practice.

THE MEDIA

Obviously, the media can be highly influential with consumers. Radio programs, television news, newspapers, magazines, and online media are constantly striving for the attention of the public by covering stories and topics that are current, important, and interesting to large numbers of people. Each media outlet is constantly searching for stories that its audience will find interesting because that will keep and grow its following, which converts into units sold (for newspapers and magazines) and advertising dollars. Responding to perceived interest, several news outlets have dedicated significant time to privacy issues. The *Washington Post*, for example, had a privacy "beat" for several years, occupied by reporter Robert O'Harrow. *Wired News* has dedicated significant energy to privacy issues, as has *The Register* in the United Kingdom.

Only a few media outlets dedicate significant resources to privacy alone, but when specific events happen, nearly all media weigh in. For example, in early 2005, it was revealed that a Georgia data aggregation firm called ChoicePoint sold data on more than a hundred thousand consumers to identity fraudsters.

This was national news carried in every kind of media throughout the country because of the direct impact it could have on the financial well-being of so many Americans.

In addition to mainstream media, the incident was carried on alternative media like the numerous blogs and online discussion fora that are playing such an increasing role in shaping contemporary issues. The Politech forum, hosted by C|NET News reporter Declan McCullagh is a good example of an alternative news and commentary source that influences how privacy and data protection law and practices develop.

When a privacy story is covered in the media, all other actors in the privacy debate are involved. Obviously, consumers become aware of privacy issues and adjust their behavior to new dangers, both perceived and real. Consumer groups, who may have helped generate the story, are often called upon to comment and make their case for the appropriate response. Pollsters may research public opinion on the issue and lend weight to a privacy issue. Companies work to reassure their customers and customer base that they are protected and corporate data protection officers study the risk that the issue will affect their business. Investors assess whether the companies they own shares of have adequately addressed the issue. Lawyers and courts often get involved when lawsuits are filed. And legislators and bureaucrats may weigh in with enforcement actions or proposals for new law and regulation.

POLLSTERS

Consumer polling has had a prominent place in the development of privacy law and practice in the United States. Especially in the late 1990s, while the Internet was in rapid ascendancy, pollsters routinely investigated what consumers' interests were. Their results influence multiple actors in the development of privacy protection. Companies determine whether they should change their practices. Consumer groups, which often participate in development of the polls, comment on their recommended responses. Politicians and bureaucrats definitely use polls to measure whether consumer opinion justifies new law and regulation.

Because the word "privacy" stands for so many different interests, polls have often failed to discover consumers' true interests. There is a wide gap between what consumers tell a pollster about their privacy preferences and what they actually do to protect privacy. Thus, the actual utility of polls for advancing the true privacy interests of consumers has been limited even if the influence of polls has been substantial.

SEAL ORGANIZATIONS

Responding to perceived consumer desire for privacy assurance, a number of seal organizations have emerged. These organizations offer companies the right to use a trademark denoting that the customer can rely on certain privacy and data protections. The companies pay the seal provider to certify that they meet certain standards. Though the standards are relatively low, the display of a seal communicates to consumers that a company is within the bounds of normal privacy practice.

Truste is the premier online seal organization, but the Better Business Bureau's BBBOnline mark and VeriSign's Secure Site Seal are other marks that communicate assurances to consumers. Others include WebTrust, SecureBiz, and PrivacyBot.

PRIVACY OFFICERS

Though there is no requirement that companies in the United States have a corporate privacy officer, many of the largest and most important consumer-facing companies do, having acknowledged the importance of privacy to their success in winning and keeping customers. Corporate privacy officers do not fit naturally into the corporate structure because their roles are so cross-cutting. Some are focused on legal compliance and so are housed with companies' legal officers. Others are focused more on communications so they sit in a public relations, community relations, or marketing departments.

Corporate privacy officers do their best to assimilate the information coming from all the other actors involved in the development of privacy practices. They translate the privacy demands of consumers, consumer advocates, the media, legislators, and others into policies for their companies to follow.

The International Association of Privacy Professionals convenes meetings for corporate privacy officers that educate them on the latest privacy concerns, compliance matters, and issues on the privacy horizon. IAPP plays a significant role by bringing people together and emphasizing the importance of drilling good corporate privacy practices into the heart of the enterprise.

INVESTORS

Investors also drive home the importance of corporate attention to privacy and data protection. Both institutional and individual investors are constantly reviewing the product mix and practices of companies, including their privacy and data protection policies. Through the equities markets, they adjust their estimates of how companies are doing at serving their customers, including serving their privacy interests.

When share prices drop, this communicates consensus among investors that the corporate management is choosing a path that will not retain customers. This includes choices that threaten consumers' privacy and choices that are too fastidious about privacy (which give away potential revenue for practices that consumers are not actually interested in). Finding the right balance is a very difficult job and companies are punished severely when they veer too far from the proper course.

The DoubleClick/Abacus example again illustrates the role of investors in harnessing companies toward privacy protection that is directly consistent with consumer interests. In late 1999, DoubleClick's share price was rising rapidly (which, in part, is what allowed it to acquire Abacus). On the day of the transaction, DoubleClick's share price was $79 (adjusted for a stock split that came in early 2000). The stock rose for the rest of the year, but complaints and investigations were arising from a number of quarters. DoubleClick's share price peaked at $134 on 3 January 2000 and started to fall as the privacy consequences of DoubleClick's Abacus plan became clearer. DoubleClick's share price bounced around the $100 level for the first quarter of 2000, then fell away after that, dropping below $50 by summer. DoubleClick shares fell both farther and faster than the NASDAQ which was dropping with the tech bust in the same timeframe. In early 2005, DoubleClick shares were trading below $10.

Investors are the enforcers that make sure corporate leadership see the consequences of bad choices when it comes to privacy and any other property of a good or service.

ATTORNEYS AND COURTS

Nearly every major issue arising in the United States ends up in a court of law at some point. Privacy is no exception to this rule. Whenever data practices are contested, there is inevitably a lawsuit filed. Usually, the allegations include violation of common law privacy rights, fraud and misrepresentation, or violation of privacy protective statutes.

Though lawsuits have not been widely successful—many contested practices are not ultimately privacy invasions—the fact that suit is filed highlights the contested data practice and leads the media, privacy officers, consumer groups, and consumers to focus attention on it.

PUBLIC CONSUMER PROTECTION BODIES

A number of public agencies in the United States are charged with enforcing consumer protection statutes. Many states have consumer protection agencies which seek to inform the public about privacy threats, among many others, and they may file actions themselves or refer them to state attorneys general.

California is one of few states that has a freestanding Office of Privacy Protection, created by law in 2000 and beginning operations in 2001. The office wields some influence on privacy and data protection in the state and has issued interpretations of California law that are seen as influential.

State Attorneys General have been active participants in the development of privacy and data protection law. They are empowered to enforce state law

dealing with data practices, of course, and the National Association of Attorneys General was for a time an active proponent of federal privacy law. Some federal statutes give authority to state attorneys general to bring enforcement actions as to violations of those laws and the use of this model seems to be increasing.

At the federal level, the Federal Trade Commission is the primary consumer protection regulator. It issued the regulations under the Children's Online Privacy Protection Act and has primary enforcement of that law. It was also the lead agency on the Gramm-Leach-Bliley financial privacy law.

The FTC also does privacy work under its general consumer protection authority, which prohibits "unfair trade practices." The agency has wide latitude to give that term definition and it has used that authority occasionally. For example, in August 2002, it entered into a consent decree with Microsoft in which it alleged that the company had misstated its privacy and security practices. The FTC regularly receives requests from consumer advocate groups to find that certain data practices are inherently unfair and, thus, illegal. It has been reticent to use this authority, however, generally waiting for Congress to specifically create new privacy law.

The Federal Trade Commission regularly convenes meetings and workshops about privacy-related issues. It has conducted extended investigations into online access and security, spam, spyware, and radio frequency identification (RFID) technology.

Under Chairman Robert Pitofsky, an appointee of President Clinton, the FTC actively lobbied for new privacy laws. When Chairman Timothy Muris took over, appointed by President Bush, the agency narrowed its call for new statutory authority, preferring to pursue privacy issues under existing authority, and it pressed through a substantial limitation on telephone solicitation called the "Do Not Call" list in mid-2003. The newest Chair of the agency, Deborah Majoras, has not served long enough to make a recognizable impression on the agency's privacy activities.

LEGISLATURES

Legislatures are extremely influential actors as well. At nearly every level of government, they play a role. The U.S. Congress regularly holds hearings on key privacy and data protection issues. These hearings tend to energize and educate all other actors in the U.S. privacy protection scheme. Of course, from time to time, the U.S. Congress also passes legislation, such as the laws discussed earlier: HIPAA, GLB, and COPPA.

The U.S. Congress has authority to preempt state regulation related to privacy but it has not always done so. In the Gramm-Leach-Bliley Act, it allowed states to regulate more heavily than federal requirements called for and states have exercised that authority.

States and localities often drive federal action. Recent amendments to the federal Fair Credit Reporting Act were prompted in part by San Mateo County in California, which passed a financial privacy ordinance. This caused the State of California to adopt a law of its own, preempting the county and setting a state-wide standard for sharing of information with corporate affiliates. The state-wide standard was uncomfortable enough for the financial services industry that it sought a federal amendment which, in turn, preempted the California law.

Another area where state action prompted federal action was spam law, where a draconian California measure prompted federal action. This may well happen again with spyware law. In late 2005, several states had anti-spyware legislation on the books and several more were considering it. A proliferation of uneven state standards appeared likely to drive adoption of a federal law.

Privacy is a confounding and difficult issue for a number of reasons. One of them is the surprising array of institutions and actors that have an influence on privacy and data protection practices in the United States. Many observers believe that European data protection is stronger because of the substantial and comprehensive regulatory regime. But the United States relies primarily on a wide variety of market actors, including consumers themselves, consumer

advocacy groups, the media, pollsters, privacy officers, and investors to police data practices and reward the good ones while punishing the bad ones. In limited areas, or with vulnerable populations, the United States has adopted regulatory mechanisms as well.

Potential for Conflicts

A number of potential conflicts exist for companies doing business in the United States and Germany. These are not specific to these two countries, but will apply to most international business transactions.

OFFSHORE DATA PROCESSING

In the United States offshore data processing has been a concern and a focus of attention by political leaders. Generally, free trade in services has been shown to be much like free trade in goods: it grows the economic pie and makes all parties to the transactions better off. One of the few remaining arguments against offshore outsourcing has been the privacy concerns. For several reasons, and as consumers' familiarity with offshore outsourcing grows, these concerns will probably give way.

First, even without special protections, privacy and data protection obligations entered into in one country follow wherever the data goes. If a credit card company has promised confidentiality and it ships data offshore to be processed or to a customer service call center, the company must ensure that the confidentiality promise they made in the consumer's country is enforced everywhere. Along with contractual rights, they are subject to bad press and consumer retaliation through loss of business if they violate privacy promises. It is no excuse that data was offshore.

U.S. legal obligations like the privacy torts apply no matter where the data moves. It does not matter if data collected by a company in one country is revealed through a breach in a foreign country. The various regulatory requirements in state and federal law like HIPAA and Gramm-Leach-Bliley also go wherever the data goes. They do not cut out when data moves offshore to be processed.

Second, good practices protect privacy well, wherever the data goes. The point is not where data moves, but how it is moved and how it is protected. Indeed, the special precautions companies take in light of concerns about off-shoring may mean that data processing in a foreign country is better protected than data processed domestically.

Good outsourcing companies take a number of steps to ensure the security of data in transit and where it is processed. They investigate the outside service provider carefully, they make sure that there is proper training of employees, they monitor the sites where work is done, and they require best practices. For example: The computers on which data is processed should not have direct connections to the Internet or extraneous programs like e-mail or Instant Messaging. The rooms where the processing is done can be kept free of pencils or paper, printers, and copy machines, so that employees cannot abscond with data. They ensure that data is not stored at the remote location any longer than necessary. And, of course, they must use encryption when transferring data.

Likewise, bad practices fail to protect privacy, onshore or off. This is illustrated by one of the few cases where offshore outsourcing threatened a privacy breach:

The incident started at the UCSF medical center in San Francisco, California where managers outsourced their medical transcription work to a firm in Marin called Transcription Stat. Transcription Stat, in turn, outsourced the work to a woman in Florida, and they believed that she did the work. In fact, she was outsourcing the work yet another step, to a man named "Tom Spires" in Texas. "Tom Spires" outsourced the work yet again to a woman in Pakistan.

The woman in Pakistan was an English speaker with some medical training who had begun her own transcription business. When she got in touch with Tom Spires, she was very excited because he promised her a lot of work at good pay. He was an uncertain business partner because he was hard to reach sometimes and wouldn't give a phone number, but a hungry small-businesswoman was in no position to be picky about customers.

After a period of time, "Tom Spires" fell behind on his payments and reached $500 in arrears to the Pakistani transcriber. This is more than a month's wages and the Pakistani woman had bills to pay. When she was unable to reach "Tom Spires" for some weeks, she took matters into her own hands and contacted the UCSF Medical Center saying that she would put patient medical records online if she were not paid. Needless to say, she got paid right away.

The story of this privacy threat was big news, and it is regularly circulated as an example of why offshore outsourcing threatens privacy. But a reporter for the *San Francisco Chronicle* researched the incident carefully, and what he found shows that it was bad practices and mendacity in the United States that caused this threat to privacy.

"Tom Spires," it turned out, was probably a name invented by the Florida woman. The Florida house she lives in is owned by people named "Spires" and the payments to Pakistan came from Florida, not Texas. The transcription service in Marin did not know that work was being outsourced further, much less outsourced offshore. In short, this long chain of careless outsourcing, and some fishy business in Florida, created the threat to privacy.

The story illustrates that careless information practices anywhere lead to privacy threats anywhere, onshore or off. Substantive offshore data processing concerns can be addressed by proper security techniques and responsible business practices.

U.S. DATA PROCESSING UNDER THE USA-PATRIOT ACT

There is one threat from offshore outsourcing that is significant. This is when the "insourcing" country has investigatory laws that are not as protective of data as the outsourcing one. While this issue began when U.S. interests were concerned with data being moved offshore, it has rebounded into the United States' lap with the recognition of threats to data protection from the USA-Patriot Act.

The USA-Patriot Act was the American government's primary response to the attacks on the World Trade Center and Pentagon on 9/11. It made several changes to U.S. law that lowered privacy protections in ways that are relevant to data processing.

Section 215 of the USA-Patriot Act dramatically lowered the threshold for secret judicial orders requiring data holders to turn over information about non-U.S. persons. It also expanded the scope of what could be sought. American law enforcement officers now may seize entire databases of information. It is also against the law for anyone to reveal this when it happens.

Section 218 of the act also broadened the authority of investigators to perform physical searches and electronic surveillance in foreign-involved cases. Formerly, foreign intelligence gathering had to be the "primary purpose" for such activities. Now, it only need be a "significant purpose." This small change in wording is a huge expansion in investigative authority, particularly where data about non-U.S. interests are involved.

USA-Patriot Section 505 lowered the threshold for the FBI to issue secret orders requiring businesses to disclose customer information without the permission of a judge. Subsequent legislation broadened the scope from financial services providers, phone companies, and Internet service providers to include travel and real estate agents, the U.S. Postal Service, jewelry stores, casinos, and car dealerships. In early 2005, that section has been enjoined by a court in New York because the secrecy requirement is so restrictive.

In light of these statutory provisions, the information and privacy commissioner for British Columbia released a report exploring the risk to British Columbians from outsourcing of data across Canada's border with the United States. It concluded that the personal data of Canadians transferred to the United States is at unique risk of seizure thanks to the USA-Patriot Act. It even found that data held in Canada by a subsidiary of a U.S. company could be at risk. These findings apply equally to personal data about Germans and to German companies.

Recommendations for International Business

One of the most important things that international businesses can do to meet the many complex data requirements of the United States and Germany is to understand the true nature of the interests that different privacy and data protection policies pursue.

As discussed early in this paper, there are many different concerns that consumers have and that the laws require companies to address. These include true privacy, security from harmful data use, fairness, freedom from unwanted marketing, and so on.

The company that "translates" legislative, regulatory, and market demands into a sensible, natural framework will be better able to adjust to these demands. International privacy professionals must understand the true essence of the issues they are dealing with. When they are, they will be better able to describe to upper management and line employees alike the importance of good data practices. Otherwise, "privacy" dictates will seem unnatural, inefficient impositions that run counter to the interests of the enterprise.

Almost all businesses are data intensive in one way or another. Those that understand the importance of good privacy and data protection practices will have an edge on their competitors that do not.

Ideally, this study has helped to enlighten the reader about basic privacy and data protection concepts, the different paths that German and American data protection policies have taken, and the different actors in the U.S. and Germany that affect the direction of data protection policies in the two countries.

AICGS

1755 Massachusetts Ave., NW
Suite 700
Washington, D.C. 20036 – USA
T: (+1-202) 332-9312
F: (+1-202) 265-9531
E: info@aicgs.org
www.aicgs.org

AMERICAN INSTITUTE
FOR CONTEMPORARY
GERMAN STUDIES

THE JOHNS HOPKINS UNIVERSITY

Located in Washington, D.C., the American Institute for Contemporary German Studies is an independent, non-profit public policy organization that works in Germany and the United States to address current and emerging policy challenges. Founded in 1983, the Institute is affiliated with The Johns Hopkins University. The Institute is governed by its own Board of Trustees, which includes prominent German and American leaders from the business, policy, and academic communities.