Privacy and Human Rights: Comparing the United States to Europe

Solveig Singleton

One premise shaping the debate about privacy law in the United States is that the European Data Protection Directive is a more-advanced model than any so far developed here. A headline in the *Government Computer News* for October 26, 1998, reads "Europeans Lead US in Data Protection Policies."[1] Under Europe's Data Protection Directive, the United States is considered to have inadequate protection for personal information, such as that which data companies might keep on consumer transactions. This finding touched off lengthy negotiations between Europe's guardians of data and the US Department of Commerce, to determine whether and when US companies may store information about their clients, employees, and customers in Europe. In June of 2000, European officials and the Commerce department finally reached an agreement, setting out policies US firms doing business with European clients and customers may follow to obtain a "safe harbor."

But why is the US regime considered unacceptable, as opposed to merely different? To answer these questions, it is important to compare the European approach to privacy with that of the United States, with particular attention to financial services. This analysis concludes that the US approach to privacy—a general rule of freedom of information coupled with a constitutionally-limited government—is actually superior to that of Europe.

THE EUROPEAN APPROACH TO PRIVACY—AN OUTLINE

The basic ground rules for privacy for members of the European Union are laid down in the European Union Data Protection Directive (95/46/ED), which applies to both electronic

and old-fashioned paper-filing systems, including (obviously) financial services. The "data" covered by the directive is information about an individual that identifies the individual by name or otherwise. Each EU nation's government is to implement the directive in its own way.

The Data Protection Directive begins by laying down basic privacy principles, starting with the idea that information should be collected for specific, legitimate purposes only, and be stored in individually-identifiable form no longer than necessary. Central to the European approach is the notion that people are entitled to control data and information about themselves as a fundamental human right.

The European Directive creates specific rights for the person the information concerns—the "data subject." The entity collecting the information must give the data subject notice explaining who is collecting the data, who will ultimately have access to it, and why it is being collected. The data subject also is given the right to access and correct the data. Financial data is not treated in any special way by the Data Protection Directive, but is governed by these general principles.

The rules are stricter for companies wanting to use data in direct marketing, or to transfer the data for other companies to use in direct marketing. 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. To collect this information the data subject must give explicit consent. The law admits several exceptions, including exemptions for employment contracts, nonprofits, or the legal system.

Some Interesting Exemptions

Musing over the principles laid down by the directive—the idea that one has the right to be notified of, and consent to, the use of information about oneself, and to access and correct this information—one might well ask whether such broad principles

can be reconciled with many vital or convenient human activities. May one, for example, take a client's business card out of the country without providing him explicit notice of exactly how it will be used and stored? Send an old roommate a mutual friend's address? At first glance the rules taken literally would turn generations of ordinary human behavior into a regulatory riddle. Thus, for practicality's sake, the directive has come to be riddled with exceptions.

These include an exemption for data kept for personal and household use—so that one may keep an address book with the names of college friends and distant uncles. Synagogues, trade unions, churches, and other nonprofits are permitted to keep even "sensitive" information about their members. Indeed, it is hard to imagine how they would operate if they did not.

The European idea of privacy and controlling information about oneself as a human right thus has peculiar characteristics. Ordinarily, a fundamental human right would not be so riddled with broad exemptions. It would be decidedly peculiar, for example, to announce that the right not to be tortured was a human right, except when it came into conflict with the government's need to collect taxes. But governments in Europe naturally exempt themselves from the directive when it comes to the state's own monetary or financial interests (*e.g.* taxation) or criminal matters. The human right to privacy simply gives way to fiscal convenience or a general need for public order.

While that result is natural enough and probably essential, the breadth and number of the exemptions to the Data Protection Directive threaten to swallow the "human right" itself. This in turn indicates that this "human right" is on shakier philosophical footing than the regulatory consensus in Europe suggests. In particular, the Data Protection Directive recognizes at least one conflict with another basic right, free speech, providing that national governments may exempt journalists from provisions of the directive when *in the government's view* the interest in free speech outweighs privacy interests. This level of deference to government on a question of free speech would be constitutionally unacceptable in the United States.

The Origins of the European Data Protection Directive

The horrors of the Holocaust inspired many Europeans to give renewed attention to the problem of privacy in the years following World War II. National-socialist governments in several countries used census data to identify households of certain ethnic, religious, or other targeted groups. In the United States, around the same time, census data was used to identify Japanese-Americans for relocation.

This shameful history yielded the lesson that information collected for innocent purposes can become a tool of oppression in the hands of a powerful government. As various welfare states swelled in size and power in Europe, the first "data protection" laws sought to guard against this danger. The German province of Hesse passed such privacy laws in 1970 in reaction to the computerization and centralization of personal information. Sweden passed the first national data-protection law in 1973—during the period that it adopted national identity cards. Support for data-protection law grew in Britain when the country began to use a centrally-administered system of national driver's licenses.

As each country developed its own national privacy regime, trade disputes arose. For example, Sweden denied a British company a contract to make magnetic-stripe cards, finding Britain's laws failed to give Swedes enough protection. To prevent such trade disputes, data-protection laws were harmonized across Europe, first with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The EU's Data Protection Directive followed, ratified in 1995.

Swiss banks meanwhile offered a contrasting lesson in privacy and its relation to human rights. The banking secrecy offered by the Swiss banking system allowed hundreds of refugees from war-torn Europe to secret their savings in pseudonymous bank accounts (although this was not the purpose for which banking secrecy in Switzerland was established). Swiss bankers have taken criticism for making it difficult for survivors to find those funds. But this is partly a consequence of secrecy, without which no money would have been saved at all.

Data Protection and the Private Sector

Privacy laws in Europe apply to data held in the private sector as well as those held in the public sector. Indeed, given the breadth of exemptions that give government the freedom to manipulate data for tax and criminal powers, the directive poses scarcely any challenge to the heart of government power, and applies far more stringently to the private sector. Given that the logic of the privacy laws is rooted in concern about the expansion of government, why target the private sector? Two reasons are commonly put forth:

- fear that governments will gain access to data held in the private sector; and
- the view that the private sector itself violates human rights by using information for direct-marketing or other purposes without notice and consent.

This analysis concludes that the former argument is impressive, though ultimately insufficient to justify restraints on the freedom of information in the private sector. The latter argument barely makes it off the ground.

PRIVACY LAW IN THE UNITED STATES

Privacy has not been the focus of much political attention in the United States since Vietnam, until recently. Perhaps this is because the welfare state has not progressed as far or as fast in the United States as it has in Europe. US citizens and policymakers are less suspicious of big business—and downright supportive of small business—compared to their counterparts in some European countries. On an issue with a close nexus to privacy, the need for "protection" of consumers from advertising and direct marketing, the United States takes a far-less regulatory approach than Europe. Even many left-wing or moderate policymakers in the United States would find a German court's ruling that Lands' End's advertising of a lifetime guarantee is "unfair competition"[2] something of a head-scratcher. Whatever the reasons, the recent debate in the US on privacy certainly has

been driven by events in Europe. However, the overall health of the US economy, especially the service-industry sector, gives opponents of top-down privacy regulation good reason to push back.

Privacy and the Federal Government

The Fourth Amendment to the Constitution does not limit what information the government may collect. It does limit the means by which that information may be collected, making information collectors accountable to the judiciary. Lax judicial scrutiny has somewhat eroded this protection. The courts have held, for example, that the Fourth Amendment does not protect businesses from "regulatory searches."

Historically, concern about privacy has flared up from time to time in response to proposed government programs. The public was mollified at the time of the creation of Social Security with the promise that Social Security numbers would only be used for Social Security purposes. More recently, public resistance to the idea of a national ID card blocked the implementation of this idea. In the financial-services area, the FDIC's proposed "Know Your Customer" regulations were defeated after a public outcry in early 1999.

During the 1970s, concern over privacy reached new heights, spurred largely by surveillance of Vietnam War protestors and abuses of wiretapping powers and tax, bank, and telephone records during Watergate. In the words of one commentator, "All of these show what government can do if its actions are shrouded in secrecy and its vast information resources are applied and manipulated in a punitive, selective, or political fashion."[3]

These concerns gave birth to the Privacy Act of 1974. The act applies only to records of personal information held by federal agencies, stipulating that the government create no secret files, and provide the public with a right to access and copy their own files. Agencies are obligated to keep reasonably-accurate records, and to keep records only if "relevant and necessary." Federal agencies are not supposed to sell or rent records. Agencies are supposed to obtain an individual's consent before disclosing the content of his records—except within the agency,

for "routine use," or to law enforcement. CIA records and other law-enforcement offices are exempt from the right of access and correction. Other exemptions cover materials prepared in anticipation of litigation.

Subsequent privacy concerns were addressed on the federal level by the Electronic Communications Privacy Act of 1986, which protects private electronic communications from unauthorized surveillance by the government, as well as the Computer Matching and Privacy Protection Act of 1988.

Privacy protection on the state level is a different story. In contrast to federal efforts, many states permit the sale of state-held records such as driver's license information, and a variety of public records are available to commercial enterprises. As of this writing, many bills to regulate privacy are under consideration in various states, some of which would adopt the European model.

Privacy and the Private Sector

In the United States at the federal level, the freedom of information remains the rule for many transfers of information between private companies. There are a handful of statutes governing the private sector's use of data in health care, the video-rental industry and the cable-television industry, and a few other areas. Generally, actors in the private sector are bound by state common law, which offers basic and minimal privacy protections in the form of privacy torts. These torts are narrowly defined, often closely linked to a violation of property rights. Courts recognize that these torts are tightly confined by the rights of free speech, especially as applied to media defendants.

Several federal statutes create privacy-related laws for financial services in the United States. In this sense, financial services are the regulated exception, rather than the unregulated rule, for information held in the private sector in the US.

Credit-reporting laws applicable to the private sector include the Fair Credit Reporting Act (FCRA), passed in the 1970s. The main purpose of this act was to allow consumers to access and correct mistakes in their credit reports. Consumers can sue for

damages if the law is violated. They may also insert explanatory comments in their own credit report concerning disputed information. Information over seven years old may not be included in a report. Particularly-detailed reports, known as investigate reports, may be released only with notice to the consumer. The FCRA also limits the uses of credit information, and requires that measures be taken to limit the dissemination of reports. Under the 1996 Amendments to the Fair Credit Reporting Act, businesses can share certain consumer information with their affiliates, but they must first give customers the choice of opting out of the sharing.

The Financial Services Modernization Act of 1999 took regulation of financial information a step further. The new law applies to any entity that engages in financial activities, including not only traditional banks but a merchant or manufacturer that offers credit, stored-value cards, or money orders. It applies to personally-identifiable financial information about consumers. Essentially, the law requires that consumers must receive notice of a privacy policy and a chance to opt out of information sharing with third parties. The law will take effect in November of 2000.

Government is not the only guarantor of personal privacy. The market also weighs in, as evidenced by the self-regulatory requirements of some banking associations. The Consumer Bankers Association's guidelines, for example, state that financial institutions should not reveal specific information about customer accounts to unaffiliated third parties for marketing purposes unless the customer has been informed and can opt out.

OLD WORLD VS. NEW WORLD

Privacy and Human Rights

US and European principles on privacy share one key similarity. Europe's data protection law and America's Privacy Act of 1974 both attempt to reign in dangers to human rights from the expansion of government. Both, however, do little or nothing to check the growth or scope of government databases or information-collection powers. Neither cuts to the heart of government powers—taxation and law enforcement.

Since so much of the privacy debate is conducted in the terminology of human rights, it is worth noting that the fundamental danger to human rights stems from the growth of government *power*—not simply from the growth of *databases*. As long as we assume that federal authorities should take responsibility for regulating more and more aspects of our daily lives, from education to health care, from labor markets to child-support payments, we will be unable to resist authorities' demands for more information. Likewise, governments with huge tax systems that demand more and more of taxpayers will naturally want to keep track of their citizens. It would be downright illogical to argue that yes, we trust governments to help us here, there, and everywhere, but we do not trust them with the information that they consequently require to run these programs more efficiently.

For all the sporadic battles privacy advocates win, whether against "Know Your Customer" or national ID cards, in the end federal databases will remain as threats to individuals' privacy as long as government power remains. Centuries ago, young national governments in Europe and China decided they needed to keep track of who belonged to which family. Thus developed the surname. John, known in his neighborhood as John the Short because of his stature, became John Short, and his son Tom became Tom Short, not Tom, son of John. Tax systems demanded this new system of nomenclature, and got it. Over time, we have all become accustomed to having surnames and even find them useful; privacy protests would be futile if not downright silly. Note, however, the *real* issue is a question of government power, specifically how broad powers of taxation will grow.

Changes in the way governments process information thus follow inexorably from changes in their substantive roles. Unless the state's growth is restrained at a substantive level, it will remain a danger to human rights no matter how it administers data. The growth of government power and its level of involvement in our lives is the fundamental issue—not what information or nomenclature it may incidentally collect.

The answer to the threat of human-rights violations by powerful governments is thus not to impose trifling restrictions on the use of data (from which the governments then exempt themselves), but to restrict the power of governments to regulate our daily lives. If we do not assign government the task of tracking money launderers or dispensing health care, it will not collect from citizens the information needed to do so more efficiently.

Assessing the European Model

The European model of data protection is surprisingly weak, because it is premised on the notion that the danger to human rights from the growth of the welfare state can be controlled, *without controlling the power of the welfare state itself.*

Take, for example, France. French authorities rigorously regulate (among other things) the hours per week that one may work. Stories have appeared in the press of how police have been sent into private businesses, appearing at the doors of offices to demand that people stop working immediately, or be ticketed. Inspectors stand outside the doors of office buildings, stopping and searching businessmen as they leave; laptops and cell phones are confiscated to ensure no work will be done at home. The dangers to human rights are obvious and enormous. The violations of privacy are severe and outrageous. But the European Data Protection Directive does nothing to stop this.

On the other hand, the relative secrecy provided by Swiss banks is an excellent example of how to prevent information from becoming a vehicle for human-rights violations. The private sector should remain free to use technology or to negotiate contracts that provide confidentiality. But the data-protection laws simply have not proven to be a check to government surveillance in Europe.

The Hidden Potential of the US Model

A cursory glance suggests that the United States, having little omnibus privacy law as such, has no way of preventing the use of information to violate human rights. But a closer look suggests the US constitutional model has the *potential* to

protect human rights. The problem in the United States has been persuading the judiciary to take the Constitution seriously—not a lack of laws or principles, but difficulty with enforcing them.

The US Constitution, in a nutshell, describes a system of limited government. The federal government's powers are limited and restricted to those enumerated in the Constitution. Were this principle given teeth, the growth of the federal government would be reigned in, restraining new government demands for more information. The idea behind the US Constitution as originally conceived is to have a government limited in size and substance—a government that will naturally make fewer demands for information, and have fewer powers to abuse.

Another traditional limit on the power of government in the United States is the nondelegation doctrine. When Congress delegates broad authority to administrative agencies, it increases dangers to privacy, because the agency is free to "regulate" without public scrutiny. The recent outcry over the FDIC's "Know Your Customer" proposal shows that agency snooping programs will rarely sit well with the public when exposed to its scrutiny. The FDIC withdrew its *official* "Know Your Customer" proposal in response to public comments. But many banks, cowed by the regulators' broad powers over their economic welfare, continue to comply with "voluntary" "Know Your Customer" rules. The original model of US government would check such "informal" legislation on the part of regulators.

FINANCIAL PRIVACY AND THE PRIVATE SECTOR

The Logic of Regulating Private-Sector Data

As noted previously, one major difference between European data-protection laws and US laws on privacy is that the US private sector remains comparatively free of regulation, even when data is used for marketing. Some freedom remains even where more-heavily-regulated financial data is concerned. This makes sense. The private sector is not armed with the unique powers to control police, armies, and the courts. It is not a danger to human rights in the sense that governments are.

The view that uses of information for marketing in the private sector violate human rights is a peculiar one. Why should a business not be free to record and use facts about transactions, about real people and real events, to develop products and to identify people who might have an interest in its products? Once a consumer enters into a transaction with another entity, this entity has as much of a right to use the information about the transaction as the consumer. Why would it violate someone's rights to use information about him to sell him something? Junk mail may be annoying, but it is difficult to see it as akin to torture.

A legitimate argument may exist that restraints on the private sector are justified because of the risk that government will seize the information. This is a real risk. But there is little in Europe's data-protection model to prevent this. The data-protection model must exempt many private databases (such as those kept by trade unions or churches) just to allow normal life to continue. These databases remain and can be targeted by police or tax authorities. The data-protection authorities in Sweden have purged from the airline-reservation system information about travelers requesting kosher meals. But what difference does this make if a hypothetical future police state can simply get the information from the local synagogue? Meanwhile, the US Constitution at least makes government seizures subject to scrutiny from the judicial branch.

The most important objection to the argument that private databases must be restricted to prevent government abuse is that it is wrong to restrict private freedoms to prevent wrongs by miscreant public servants. Germany and France, in their desire to prevent the rise of extremist political movements, censor political speech such as Holocaust revisionism, anarchist newspapers, or books about the illness of the French president. There is a tremendous irony in noting that what some European countries have apparently concluded from World War II is that one may restrict government power by increasing controls on the private sector. This approach is simply not consistent with preserving private citizens' rights. If one's concern is abuse by governments, by all means enforce restrictions on governments and

their employees. But do not take away the freedom of the private sector in the name of defending it.

Economic Considerations and Consumer Welfare

With all of these assaults on personal liberty in the name of protecting privacy, it bears asking: What are consumers losing?

Europe's implementation of the Data Protection Directive offers some clues. We are likely to lose some small businesses (in Britain, bankruptcy rates for small businesses have increased markedly; commentators attribute this partly to data protection and partly to other regulatory initiatives that have fallen heavily on small business). A small business in Britain, for example, might face a devastating fine of thousands of pounds for disposing of a PC without erasing a file of customer names and addresses—even if the stray information is never used for harm.

Consumers could lose big by reducing the free flow of information between banks and affiliates (and/or third parties). The use of this information to target offerings of new financial services in new markets dramatically reduces the costs of getting information out to consumers. Being able to precisely target a marketing offer to likely first-time home buyers, for example, might lower the costs of marketing the offer from as much as $10 or $12 to as low as $2. And this will often mean the difference between whether the offer can or cannot be financed at all. Do we want to assume, as do many European officials, that marketing is not a fundamentally legitimate activity?

Bureaucratizing the information flow between financial-services organizations could mean that many new services cannot be offered, or that many consumers will never hear about a favorable new type of account or loan. This means less competition, with fewer new companies and business models. Extending notice-and-consent requirements to transfers of data between financial-services affiliates would give the advantage to big, integrated firms over smaller ones that contract out for services such as printing accounts.

A grave concern should be that consumers may find it increasingly difficult and expensive to obtain credit. In Greece,

for example, even a professional may find a credit card impossible to obtain. Elsewhere in Europe, the cost of obtaining a credit card is much higher than in the United States—with interest rates for an ordinary credit purchase as high as 25 percent.[4] A major problem overseas is that restraints on the flow of verification information make fraud rampant.[5] Consumers with a poor credit history may find it particularly difficult to obtain any credit at all.

Top-down regulation of privacy also conflicts squarely with free-speech rights—not only for journalists and regulated companies, but for grassroots political ventures. In Sweden, for example, a law was passed making it illegal to publish personally-identifiable information on the Internet. The prosecutor was embarrassed to realize a literal reading of the law meant a human-rights group could no longer legally have a web site with the heading "Pinochet is a murderer."[6] The prosecutor tried to save the situation by explaining that "minor" violations of the law would not be punished. But reportedly this resort to prosecutorial discretion has not saved animal-rights groups and consumer activists from liability under the privacy law.

Data Protection and the Information Economy

The data-protection model cannot easily be adapted to information-age technology. The purpose of information technology and innovation is to make the conveyance of information faster and cheaper, while the purpose of data protection seems to be to make the transit of information slower and more cumbersome.

Supporters of the European directive have had to scramble to adapt data-protection laws to new technology. The original premise of the directive was that express consent was to be required (turning normal rules of contract law on their head). But how can this be reconciled with the telephone system? When one makes a call, one's billing information is automatically relayed from switch to switch across many jurisdictions—all without notice or consent. When one sends an e-mail, one's personally-identifiable header information often is flung from shore to shore, across many servers in many lands in an

unpredictable pattern. It would not be uncommon for an e-mail sent from Brussels to Paris to travel through a server in California.

EU authorities have decided to "deem" the person sending the information to be the person making the call or sending the message. This fiction painfully strains the principles of the directive itself—implicit consent in effect "snuck in" to save the regulations from the embarrassment of technological backwardness.

EU authorities remain uneasy about the Internet's fundamental nature—making communication of all information seamless and cheap. European privacy authorities reported, "Presently it is almost impossible to use the Internet without being confronted with privacy-invading features which carry out all kinds of processing operations of personal data in a way that is invisible to the data subjects." And Dutch regulator Diana Alonso warned, "We just want to let (companies) know when they are making new software and hardware, they should pay attention to [privacy] principles."[7]

As with phone calls, would the EU be willing to abandon the restraints of the directive to permit new technology and innovative business models to go forward? For example, if credit reporting had not been invented yet, would EU authorities allow it to begin? If so, they must reject the rule that it is wrong to use information about consumers without their consent, gutting their directive and implicitly admitting that it will often be an obstacle to consumer welfare. If not, the result would be to "freeze" in time the types of information collected, and the purposes for which they are used, in the late 1990s.

A large part of the wonder of information technology is that it will empower us not just to send our names and addresses around faster, but also to create and store types of information that historically have been lost and wasted. Every event in the life of a human being is a potential source of information—our decisions not to buy as well as those to buy, our idle wanderings as well as purposeful ventures, our casual interactions with coworkers. A top-down regulatory model, the principle of which

is that what is not expressly permitted is forbidden, would appear to be fundamentally hostile to such experiments in creating new libraries of data and learning from them.

CONCLUSION

The most effective rules for ameliorating federal threats to privacy are to limit the powers of the federal government overall and restrict the growth of federal programs. So long as such programs grow unchecked and taxes rise unchecked, government demands for more information will prove irresistible.

Top-down regulatory models of how information "ought" to be used are incompatible with innovation in financial services. If we in the US continue to turn the default rule of freedom of information on its head, we will find ourselves trying to operate a modern economy on the principle that what is not explicitly permitted is forbidden. It is only because we have for ages gone by the opposite rule that our economy and people continue to thrive.

Notes

[1] "Europeans Lead US in Data Protection," *Government Computer News*, October 26, 1998, p. 1.

[2] Peter Girard, "Lands' End Winks at German Ruling," *Catalog Age* (January 2000); Carol J. Williams, "Market Forces Loosening State's Grip On 'Germany Inc.'," *Los Angeles Times*, June 11, 2000; Mary Lisbeth D'Amico, "German E-Commerce Faces Legal Tangle," *InfoWorld Daily News*, March 10, 2000; Deborah Hargreaves, "Lands' End to File Brussels Complaint," *Financial Times (London)*, January 11, 2000, p. 8.

[3] Unnamed ACLU representative, quoted in Major John F. Joyce, "The Privacy Act: A Sword and A Shield But Sometimes Neither," 99 *Mil. L. Rev.* 113, 122.

[4] See *e.g.* Sarah Cunningham, "John Lewis Succumbs to Consumer Pressure," *The London Times*, September 18, 1999; "U.S. E-Merchants Fail to Gain Market Share in Europe Due to Differences In Buying Habits," *Business Wire*, June 22, 2000 ("differences in monetary policy and banking regulations in many European countries have severely restricted the availability of credit cards").

[5] See *e.g.* "Online Europe," *New Media Age*, January 27, 2000, p. 12 (quoting merchant Kevin Sefton, "Merchants try to mitigate risk, but we're in an

extremely difficult position…UK credit card transactions are verified against the card number and date only.").

[6] Jacob Palme, "Freedom of Speech, The EU Data Protection Directive and the Swedish Personal Data Act," June 9, 2000, available at http://www.dsv.su.se/jpalme/society/eu-data-directive-freedom.html. See also e-mail from Jacob Palme to Declan McCullagh, June 9, 2000, archived at http://www.politechbot.com/p-01218.html.

[7] Suzanne Perry, "EU Regulators Seek Internet Privacy Protection," *Reuters*, March 4, 1999.