White Paper

December 1, 1999

Privacy and Human Rights: Comparing the United States to Europe by Solveig Singleton

---

This paper was written for the Competitive Enterprise Institute's conference on financial privacy, held in Washington, D.C.

One premise shaping the debate about privacy law in the United States is that the European Data Protection Directive is a more advanced model. A headline in the *Government Computer News* for October 26 of 1998 reads "Europeans Lead U.S. in Data Protection Policies." Under Europe's Data Protection Directive, the United States is considered to have inadequate protection for personal information, such as transactional data that companies might keep on consumer transactions. This finding touched off lengthy negotiations between Europe's guardians of data and the U.S. Department of Commerce, to determine whether and when U.S. companies could store information about their clients, employees, and customers in Europe.

But why is the U.S. regime considered unacceptable? Should it be? This paper revisits that question, comparing the European approach to privacy with that of the United States, with particular attention to financial services.

The paper begins by outlining the Data Protection Directive, its history and many exemptions. Next, it explores privacy laws in the United States, identifying a key similarity between data protection and the 1974 Privacy Act--both attempt to restrain the danger of the growth of government databases, but neither strikes at the heart of the government's power to tax or to control the criminal justice system. The paper goes on to assess the potential of a model of limited government to provide better protection for human rights than the data protection model. Finally, the paper assesses whether it is useful or beneficial to restrict the uses of data in the private sector, touching on economic and philosophical arguments.

In the end, restricting the uses of data in the financial services sector along European lines will severely damage the innovation economy without restricting dangers to human rights. The freedom of information is the sounder default rule.

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). The Data Protection Directive 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 somehow identifies the individual by name or otherwise. Each national government will 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.

The directive goes on to create 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 the data 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 that want 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, non-profits, or the legal system.

Some Interesting Exemptions

Musing over the principles laid down by the directive--the idea that one has the right to notice and consent to the use of information about oneself, and to access and correct this information--one might well ask whether how such broad principles can be reconciled with many vital or convenient human activities. Indeed, they cannot be--thus, 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 non-profits are permitted to keep even "sensitive" information about their members. Indeed, it is hard to imagine how they would operate if they did not. National governments may exempt journalists from provisions of the directive, when in the government's view the interest in free speech outweighs privacy interests.

Governments conveniently exempt themselves from the directive when it comes to the state's own monetary or financial interests (e.g. taxation) or criminal matters. Thus, for example, the debate over what to do to catch money launderers in Europe has (partly in response to U.S. pressure) largely paralleled the debate about "Know Your Customer" rules in the United States. In 1991, the EU crafted its own version of "Know Your customer" rules to catch money launderers; these rules were revised in 1997, and are now being implemented by various nations.

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 national 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 within Europe, this lesson began to be written into the first "data protection" laws. The German province of Hesse first passed such 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 drivers' licenses.

As each country developed its own national privacy regime, trade disputes began to arise. 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.

Meanwhile, Swiss banks offered a contrasting lesson in privacy and its relation to human rights. The anonymity offered by the Swiss banking system allowed hundreds of refugees from war-torn Europe to secret their savings in anonymous and pseudonymous bank accounts. Swiss bankers have recently taken criticism for making it difficult for survivor's to find those funds. But this is partly a consequence of the anonymity, without which no money would have been saved at all.

Data Protection and the Private Sector

Privacy laws in Europe apply to data held by the private sector as well as by the private sector. Indeed, given the breadth of the exemptions that give government the freedom to manipulate data for tax and criminal powers--the directive is 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 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.
- The view that the private sector itself is violating human rights by using information for direct marketing or other purposes.

As I discuss further below, the first 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

The welfare state has not progressed as far or as fast in the United States as it has in Europe. U.S. citizens and policymakers are less suspicious of big business--and downright supportive of small business--as contrasted with their counterparts in some European countries. Perhaps partly for these reasons, privacy has not been the focus of much political attention in the United States until recently.

Privacy and The Federal Government

The Fourth Amendment does not limit what information the government may collect, but limits the means by which that information may be collected, making information collectors accountable to the judiciary. Lax judicial scrutiny has somewhat eroded this protection.

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 I.D. 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 1970's, public concern with surveillance of war protestors during Vietnam and by abuses of wiretapping powers and tax, bank, and telephone records during Watergate reached new heights. 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."

The legislative result was the Privacy Act of 1974. The Act applies only to records of personal information held by federal agencies. It stipulates 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 reasonable 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 officers are exempt from the right of access and correction. Other exemptions cover materials prepared in anticipation of litigation.

Other federal legislation concerning privacy includes the Electronic Communications Privacy Act of 1986, which protects private electronic communications from unauthorized surveillance by the government and the Computer Matching and Privacy Privacy Protection Act of 1988.

By contrast, many states permit the sale of state-held records such as driver's license information. Many public records are available to commercial enterprises.

Privacy and the Private Sector

At the federal level, the freedom of information remains the rule for many transfers of information between private companies. There are a handful of sectoral 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 bounded by the 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. Several courts have recognized that these torts are limited by rights of free speech.

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 U.S.

Credit reporting laws 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 credit 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.

Some banking associations have self-regulatory requirements. For example, the Consumer Bankers Association's guidelines 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

U.S. and European principles on privacy share one key similarity. Both data protection laws and the Europe's Data Protection law and the Privacy Act of 1974 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.

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 a huge tax system that demands more and more of taxpayers will naturally want to keep track of us citizens, their natural prey. 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 it takes to help us more efficiently.

For all the sporadic battles that privacy advocates win, whether against "Know Your Customer" or national I.D. cards, in the end, the federal databases will march onwards as long as government power grows. Many, many centuries ago, young national governments in Europe and in ancient China decided they needed to keep track of who belong to which family. They invented 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. The tax system demanded this new system of nomenclature, and got it. Only one or two eccentrics today refuse to use surnames because they present a danger to human rights. This battle was lost long ago and today is now forgotten, a mere administrative quibble. The real issue is the fact that government succeeded--and is still succeeding--in demanding more and more from its citizens in tax money.

The point is this--the fundamental issue is first and foremost the growth of government power and its level of involvement in our lives. Changes in the way governments process information follow inexorably from changes in their substantive roles. Unless the growth of government is restrained at a substantive level, it will remain a danger to human rights no matter how it administers data.

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). The answer is 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, they will never ask us for information to do so more efficiency.

Assessing the European Model

Consistent with the arguments above, the European model of data protection is particular weak. The idea is 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.*

Consider France. French authorities rigorously regulate (among other things) the hours per week that one may work. Stories have begun to appear how police are sent into private businesses, appearing at the doors of one's office to demand that one stop working immediately, or be ticketed. Inspectors stand outside the doors of office buildings and stop and search businessmen leaving their offices; they confiscate laptops and cell phones, to ensure that the businessmen cannot work from home. The dangers to human rights are obvious and enormous. The violations of privacy are severe and outrageous. But the data protection directive does nothing to stop this.

On the other hand, the anonymity 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 anonymity. The data protection laws are not a check to government surveillance in Europe.

The Hidden Potential of the U.S. Model

A cursory glance suggests that the United States, having little omnibus privacy law as such, has no way at all of preventing the use of information to violate human rights. But a closer look suggests the U.S. 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 law or principles, but difficulty with enforcing them.

The U.S. Constitution, in a nutshell, describes a system of limited government. The federal government's power 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 U.S. 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.

The Fourth Amendment does not limit what information the government may collect, but limits the means by which that information may be collected, making information collectors accountable to the judiciary. In practice, the courts have departed from many of these constraints. The courts have held, for example, that the Fourth Amendment does not protect businesses from "regulatory searches." Here, too, revival of the Fourth Amendment would provide additional privacy protection.

Another traditional limit on the power of government in the United States is the non-delegation doctrine. 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 public scrutiny. When Congress delegates broad authority to administrative agencies, it increases dangers to privacy, because the agency is free to "regulate" without public scrutiny. The FDIC withdraw it's *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 orginal model of U.S. 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 above, one major difference between European data protection laws and U.S. law on privacy is that there the U.S 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 themselves 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 entit 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? This is a far cry from torturing him or seizing his home.

What about the argument 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 the 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 information about travelers demanding kosher meals from the airline reservation system. But what different does this make if a hypothetical future police state can simply get the information from the local synagogue?

Finally, it is wrong to restrict private freedoms when the true focus of one's concerns is 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 learned from World War II is that one must restrict government power by increasing controls on the private sector. This approach is simply not consistent with preserving private citizen's rights.

Economic Considerations and Consumer Welfare

With recent legislation, the tradition of freedom of information in financial services is being quickly eroded even here in the United States. 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 new 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 to harm anyone.

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 reduces the costs of getting information out to consumers dramatically. 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?

Thus, bureaucratizing the information flow between financial services organizations could mean that many new services cannot be offered, or 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 a big advantage to big integrated firms over smaller ones that contract out for services like printing accounts.

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 several times higher than in the United States--with interest rates for an ordinary credit purchase as high as 25 percent. Consumers with poor credit history may find it particularly difficult to obtain any credit at all.

Data Protection and the Information Economy

The data protection model cannot easily be adapted to information Age technology. The whole purpose of information technology is to make the conveyance of information faster and cheaper. The whole purpose of data protection seems to be to make the transit of information slower and more cumbersome.

Data protection interpretors have had to scramble to adapt data protection laws to technology. The original premise of the directive, for example, was the express consent was to be required. But how could this be

reconciled with the telephone system? When someone makes a phone call, one's billing information is automatically relayed from switch to switch across many jurisdictions--all without notice or consent.

When one sends an email, one's personally identifiable header information is flung merrily from shore to shore, across many servers in many lands in an unpredictable pattern. It would not be uncommon for an email sent from Brussels to Paris to travel through a server in California. EU authorities decided that they would "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.

EU authorities remain uneasy about the Internet's fundamental nature. European privacy authorities reported that "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 that "We just want to let (companies) know when they are making new software and hardware, they should pay attention to [privacy] principles."

As with phone calls, would the EU be willing to abandon the restraints of the directive to permit new technology to go forward? For example, if credit reporting had not been invented yet, would EU authorities allow it to begin? If so, they have gutted their directive and admitted that it will often be an obstacle to consumer welfare.

If not, the result will be to "freeze" in time the types of information collected and the purposes for which it is used. But 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 that it will enable the creation and storage of types of information that, historically, have always 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 that which 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 U.S. 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 that which 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.