

May 24, 2002

The Hon. Bob Barr, Chairman  
Subcommittee on Commercial and Administrative Law  
House Judiciary Committee  
U.S. House of Representatives  
2138 Rayburn House Office Building  
Washington, D.C. 20515-6216

Dear Chairman Barr:

Thank you for the opportunity to testify at the May 1 hearing on H.R. 4561, the “Federal Agency Protection of Privacy Act.” I have received your May 10 letter posing additional questions for the hearing record. Below, I have copied your questions, then offered my responses. I hope they usefully inform your consideration of the legislation and the privacy issue in general.

Sincerely,

James W. Harper  
Editor  
Privacilla.org

- 1. In your testimony, you stress the difference between personal information obtained by the government and that collected by private actors. Why is it important the government and private sectors be treated differently?**

One of the least recognized elements in current privacy debates is the profound difference between governments and the private sector in how they come to privacy. Businesses and governments are alike in that they thrive on the use of information about people. They differ in important ways, however — ways that change how they use the

information they collect. Radically different incentives affect how governments and businesses collect, use, and store personal information about consumers and citizens, and the two operate in entirely different legal regimes as well.

To businesses, information is a scarce resource that must be paid for one way or another. Businesses may lose customers if they ask for too much information. They seek plenty of information from and about customers, but not so much information, or such sensitive information, that consumers will refuse to transact with them. Governments, on the other hand, can demand information on tax forms, on applications for licenses and benefits, and in numerous other ways without losing ‘customers’ if they collect too much. Without market incentives to limit their data collection, governments will tend to collect more information than necessary and appropriate.

Unlike businesses, governments do not lose the value of information they hold if they abuse it. A business that loses, gives away, or sells information often reduces the value of that information. Competitors may use it to win customers from the company that generated or collected it, for example. A government, on the other hand, may share all the information it has without reducing its ability to carry out its missions.

If a business uses information in a way that is offensive, it may lose customers and the confidence of investors. As we have seen several times in the recent past, companies may suffer bad public relations because of their information practices, and they may suffer dramatic losses in sales and market capitalization. A government may make offensive uses of information without reducing its ability to function, its ability to collect taxes, or its ability to collect more information.

So, where a business must make tactful and intelligent use of scarce information, a government has few similar incentives. This has dramatic consequences for how the two operate when it comes to protecting privacy, and how they should be treated in terms of regulation.

The fact that governments collect information using the force of law cannot be emphasized strongly enough. When a government agency or program needs personal information, that information will be collected. Individuals have no choice in the matter. This is not the case with businesses that, one way or another, must bargain for the information they want.

An important upshot of this is that consumers are more often allowed to remain anonymous or use fake names when dealing with businesses. As long as one is not committing fraud, the penalty for lying about one’s identity to a business may be that a transaction is not completed. When dealing with government, however, anonymity or pseudonymity is often impossible, illegal, or, at the very least, suspicious.

Accountability in government gives rise to privacy problems not found in the business world, as well. The public can and should have access to information that governments

collect because this helps keep governments accountable and because the information was collected using public funds. Open records, a hallmark of open government, may mean that information citizens have been compelled to disclose becomes public. Databases held by businesses, on the other hand, are not available to the public on anything near similar terms. Market conditions apply to their sharing of data. This makes it easier for consumers to demand and receive privacy protections, though the process is never perfect.

In lieu of a healthy system of incentives, governments respond to a patchwork of privacy laws imposed on themselves. These laws do not evolve and respond to change as contract rights do, and as the privacy torts can in common law courts. Government privacy practices move in fits and starts as new uses of information expose loopholes in government privacy protections. The Federal Agency Protection of Privacy Act is such a measure — badly needed because of new public awareness of government threats to privacy.

Because governments are only subject to the laws they make for themselves, information held by governments — even if confidential “by law” — is not as well protected as information held under similar restrictions by businesses. Governments can change the laws that apply to information they hold — and sometimes ignore the laws — without suffering significant adverse consequences. Businesses can not. When governments make objectionable uses of information, there is no higher authority to which aggrieved citizens can appeal. This justifies much more restriction on governments’ access to personal and private information.

## **2. Why is it necessary to place additional safeguards on the collection and distribution of information by the government?**

As discussed above, governments have unique powers to take and use information about people. These represent threats to privacy, civil liberties, and various other interests. We have a great deal to be proud of in the United States because our government characteristically acts with restraint, but there are still many examples where it has acted without sufficient regard for privacy and civil liberties.

One notorious example is internment of Americans of Japanese ancestry during World War II. The United States government used information gathered by the Census Bureau to help round up these Americans. Census Bureau employees opened their files and drew up detailed maps that showed where Japanese Americans were located and how many were living in given areas. Nearly 112,000 people were captured and sent to internment camps during this period.

Privacy invasions and abrogation of civil liberties are not just an artifact of difficult historical times. In 1976, the U.S. Senate’s Select Committee to Study Governmental Operation With Respect to Intelligence Activities (known as the “Church Committee”)

found substantial overreaching in the exercise of domestic surveillance. It established that the targets of intelligence activity in the United States ranged far beyond persons who could properly be characterized as enemies of freedom. Domestic surveillance extended to a wide array of citizens engaging in lawful activity.

In 1997, Congress and the public discovered a practice at the Internal Revenue Service known as file “browsing.” Thousands of IRS employees had access to the files of American taxpayers thanks to a nationwide IRS database. Though there have always technically been rules against browsing those files, the IRS had done little to prevent employees from looking up private information about celebrities, neighbors, ex-spouses, and so on.

In each of these examples, the people wronged received tardy or anemic justice, if any at all. Victims of these types of invasions have relatively little recourse against the government. This necessitates preventative safeguards on collection and distribution of information by governments that would not be appropriate for the private sector. This is not intended as a slight to the beneficent motives of public servants and government programs.

In addition to preventing privacy violations and threats to civil liberties, limiting the collection of information by governments fosters the autonomy and individuality of the American people. People define themselves by exercising power over information about themselves. A free country does not require people to justify the choices they make about what information they share and what they hold close. (This does not mean that public policy should shield people from the costs of their choices.) Our default should be to limit the amount of personal information that governments collect.

American privacy allows our many cultures and subcultures to define for themselves how personal information moves in the economy and society. Collection and distribution of information by the government interferes with the decisions individual citizens would make about what information they share and on what terms. As much as this is an ethereal point, it is an important one about the kind of country we are.

**3. Last year, Privacilla.org issued a report indicating federal agencies routinely exchange personal information among each other. Is this a growing trend? Do any limitations exist on intergovernmental transfer of personal information?**

In March 2001, Privacilla issued a report entitled: “*Privacy and Federal Agencies: Government Exchange and Merger of Citizens’ Personal Information is Systematic and Routine.*” In it, we reported that federal agencies begin a new information-sharing program under the Computer Matching and Privacy Protection Act more than once every two weeks. This is a small subset of the new uses agencies regularly make of personal information.

Though empirical evidence lacks, exchange of personal information by federal agencies does seem to be growing. Computerized databases are increasing in number and size, and standardized formats are making it easier to share data. Many new responsibilities given to federal agencies by Congress require sharing of data, either directly or as the best means to carry out and monitor federal programs. This is why the Federal Agency Protection of Privacy Act is so very timely.

There are few limits on intergovernmental sharing of data. The Privacy Act and the Computer Matching and Privacy Protection Act merely require notice in the *Federal Register* before new “routine use” of information is made or before a computer matching program is initiated. This is the lowest of hurdles, intended to inform rather than impede.

In the Privacy Act, there are limits on what uses can be made of information after it has been shared. Such limits may also exist in the organic laws under which information sharing is often carried out. These go to important non-privacy values like fairness and due process. Limitations on transfer per se are few because, in the past, the advancement of particular government programs has usually taken precedence over abstractions like privacy. The Federal Agency Protection of Privacy Act would help prevent this omission in the future.

#### **4. Do ongoing government efforts to merge data among federal agencies raise significant privacy concerns?**

Rarely is any one exchange of data by federal agencies a significant privacy concern. Taken separately, each is too small to object to on the basis of privacy. And, of course, nearly all new and revised uses of citizens’ personal information are instituted for beneficent purposes like doling out entitlements, managing programs, collecting debts, and investigating malfeasance.

It is the cumulative exchange, merger, and use of personal data across the government that raises privacy concerns. This is why the Federal Agency Protection of Privacy Act will improve consideration of privacy in our public policy. It will allow Congress, the press, and the public to observe the cumulative loss of privacy we suffer due to the scores of new programs and regulations that rely on personal information. With that knowledge, we will all be better equipped to determine the scope, structure, and direction of federal programs and regulations.

Returning to the definition of privacy proffered in testimony submitted for the hearing: Privacy is a subjective condition that individuals enjoy when two factors are in place — legal ability to control information about oneself, and exercise of that control consistent with one’s interests and values.

When government agencies are merging personal data, individual Americans — the subjects of this data — have no effective power to stop it. And they are never in a position to legally opt-out of programs that require data about them. The first factor in privacy is absent. It may be said that information in the hands of government is categorically *unprivate* because individual citizens have no legal power to prevent collection and use of information about themselves.

**5. Why do most government databases eventually wind up being used for purposes inconsistent with their creation?**

It may not be the case that government databases are used for purposes inconsistent with their creation. Rather, they are used for purposes consistent with their creation *plus* many other purposes as well.

One example is the National “New Hires” Database. The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 required the Secretary of Health and Human Services to develop a National Directory of New Hires. This directory is a database of information on all newly hired employees, quarterly wage reports, and unemployment insurance claims in the United States. This is a great deal of personal financial information about American citizens.

The purpose of this new database was entirely laudable — helping states locate parents who have skipped out on their child support obligations. All databases are created for laudable purposes. But they have clear tendencies to grow and adopt new uses, uses which, at some point, may vary dramatically from their original purposes.

Already, the National Directory of New Hires has been expanded to track down defaulters on student loans. Additional expansions have been proposed in successive Congresses, including proposals to give state unemployment insurance officials access to the database.

Databases are useful tools. They are attractive for policy-makers in Congress and federal agencies who want to do creative new things to improve existing government functions and programs. New uses of databases that advance government programs are often, unfortunately, a retreat for personal privacy.

**6. You suggest Fair Information Practices is an ideologically-laden approach to privacy, making no distinction between the government and private industry. Please explain.**

Past studies of privacy have failed to recognize the distinctions between government and the private sector that was articulated in response to the first question above.

In the early 1970s, for example, a committee called “The Secretary's Advisory Committee on Automated Personal Data Systems” within the Department of Health, Education, and Welfare did a seminal study of record keeping practices in the computer age. The intellectual content of its report, commonly known as the “HEW Report,” formed much of the basis of the Privacy Act of 1974. The report dealt extensively with the use of the Social Security Number as the issues stood at that time. (And it shows that concerns about information practices are not as new as we may think.) The report did not distinguish terribly well between private- and public-sector institutions. Scholarship like Public Choice Theory, developed and refined over the years since then, has highlighted the importance of these differences.

The HEW Report recommended a number of information practices, calling them “Fair Information Practices.” The concept remains widely discussed today, but almost 30 years after conception many versions of ‘Fair Information Practices’ are problematic in application and not widely adopted.

‘Fair Information Practices’ do form the basis of 1980 guidelines issued by the Organization for Economic Cooperation and Development, a Paris-based international bureaucracy, and the European Union’s Data Privacy Directive. Happily, the United States is learning from the experience of its friends in Europe. The directives in Europe have empowered government bureaucrats while limiting the ability of European businesses to serve consumers. The experience of Europe does not suggest a path for the United States to follow.

The American tradition of limited government protects privacy somewhat in the public sphere, while market-driven privacy protections appear to be outstripping the European regulatory model. American firms increasingly must have information practices that please consumers. If they do not, they are punished when consumers abandon their products or investors lose confidence in their futures. This means that the great majority of Americans will get a desirable mix of privacy protection, convenience, security, customization, and other interests from our businesses. Europeans may well bristle with privacy “rights,” but when it comes to actual privacy, they may be worse off than Americans.

The “Fair Information Practices” also tend to bring in a variety of other important information policies, such as security, fairness, and enforcement. Each such policy is complex and deserving of careful, separate analysis. Some of these policies are inconsistent with others. As was noted in the testimony submitted for the hearing, the Federal Agency Protection of Privacy Act deals with several separate information policy issues. Because it only requires notice of such things, its requirements do no harm.

Advocates who push an entire menu of ‘Fair Information Practices’ on either government or the private sector may be using the privacy debate to pursue a variety of policies that add up to ideology. There is nothing wrong with ideology per se — Privacilla.org wears a “free-market, pro-technology” stance on its sleeve. We believe

that competition among companies to serve consumers is the best way to discover and deliver privacy on the terms they desire. There are honestly held views to the contrary. Some of them buy strongly into whole-cloth adoption of various ‘Fair Information Practices.’ These deserve careful consideration — and often rejection on the merits.

### **7. Will the Federal Agency Protection of Privacy Act provide sufficient public notice concerning a rule’s potential impact on personal privacy?**

Through *Federal Register* publication, the Federal Agency Protection of Privacy Act will provide some notice concerning a rule’s effects on personal privacy. *The Federal Register* remains a publication of almost perfect obscurity to the vast majority of Americans, of course. They should receive better notice. Thanks to the Web and e-mail, for example, federal agencies could directly notify many citizens about how proposed regulations would affect uses of personal information about them. Furthermore, affirmative limits on data collection would be preferable to mere notice.

But the Federal Agency Protection of Privacy Act takes measure of the fact that information practices in federal agencies have developed over decades and they can not change quickly. It is a moderate step on the path toward more robust notice and more affirmative privacy protections.

Required to examine and discuss proposed rules in terms of privacy, agencies will naturally tend to build privacy considerations into their rulemakings. Thus, the Federal Agency Protection of Privacy Act will have an indirect impact that protects privacy by reducing ever-so-slightly the range of personal information practices agencies adopt by regulation.

The Federal Agency Protection of Privacy Act will also reflect back to Congress how its own actions affect privacy. As agencies will surely make clear in their Privacy Impact Assessments — and they should — many privacy impacts are either directly or indirectly mandated by statute. This, too, will improve the deliberation that goes into public policies.

Governments are the most serious threats to privacy, so one can not call a moderate step like the Federal Agency Protection of Privacy Act entirely “sufficient.” The legislation is a sufficient start toward further discussion of the privacy issue and greater protection for privacy from government.

**8. Other than the changes you suggest in your testimony, how else might the legislation be improved?**

The Federal Agency Protection of Privacy Act would improve the consideration of privacy in our public policy if it were passed as introduced or with the few amendments that have been suggested.