Privacilla.org

Your Source for Privacy Policy from a Free-market, Pro-technology Perspective

Prepared Statement of Jim Harper, Editor of Privacilla.org
Hearing on H.R. 4561, the "Federal Agency Protection of Privacy Act"
U.S. House of Representatives Committee on the Judiciary
Subcommittee on Commercial and Administrative Law

May 1, 2002

Chairman Barr, Mr. Watt, and Members of the Subcommittee:

It is a great pleasure to appear before you to discuss H.R. 4561, the "Federal Agency Protection of Privacy Act." I am Jim Harper, the Editor of Privacilla.org, a Web-based think-tank devoted exclusively to privacy. I am also an Adjunct Fellow at the Progress & Freedom Foundation and the Founder and Principal of Information Age lobbying and consulting firm PolicyCounsel.Com.

Privacy is one of the most complex and difficult public policy issues confronting Congress and legislatures across the country today. I am pleased to lend what knowledge I have to your consideration of this legislation.

Privacilla.org is a Web site that attempts to capture "privacy" as a public policy issue. The pages of Privacilla cover the issue of privacy from top to bottom. We deal with fundamental privacy concepts, privacy from government, and privacy in the private sector, including financial, medical, and online privacy. Anyone may submit ideas, information, and links for potential inclusion on the site. The site represents the thinking of many people and I would refer you to the Privacilla "Support" page to get an idea of

the groups we work with. Please visit Privacilla at http://www.privacilla.org and use it as a resource whenever your work brings you to a privacy policy question.

Privacilla takes a free-market, pro-technology approach to privacy policy. There certainly are other views, and you should consider them all. Please also be aware that Privacilla is currently a project of my lobbying and consulting firm, PolicyCounsel.Com. My firm does not represent any interest on privacy specifically, but nearly all issues touch on privacy in some way, so you should consider my potential for bias, as you would with any privacy advocate. The views presented on Privacilla, and those I express today, are not the views of any client.

Chairman Barr, I salute you for introducing H.R. 4561 with broadly bipartisan support, and for holding these hearings today. Mr. Watt, and other Members of the Subcommittee, congratulations to you for joining in introducing this important bill.

Privacy is a complex and widely misunderstood public policy issue. This legislation can help protect Americans' privacy by giving the American people, the press, and Congress information they need about how federal regulation affects privacy. This legislation presents an opportunity to refine the terms of the many different "privacy" debates, so that Congress, the press, and the public can find solutions to a number of important problems.

Though they are motivated only by beneficent purposes, many government programs deprive Americans of control over personal information and their privacy. The Federal Agency Protection of Privacy Act can help restore to the people the power and autonomy that is one of the great benefits of living in the United States. There are several successful precedents in our nation's administrative laws for this proposal. Few, if any, changes are needed to perfect the legislation in terms of privacy. I urge you, though, to be aware of the many important elements of information policy beyond privacy that fall within the scope of the bill.

Defining Terms: What is Privacy?

The Judiciary Committee is the committee of American law and legal institutions. There is no better place to define and give structure to terms such as our focus today: privacy. By digging deeply into privacy as a legal concept, you as congressional leaders can dramatically improve the quality of many public policy debates, and the outcomes Congress produces for the American people.

Left undefined, the word "privacy" has become far too much of a stalking horse for all variety of ideological and special interest groups. Indeed, a coterie of activist organizations — including Privacilla — thrives because there is not an agreed to and limited definition for the word "privacy" in current debate. Moreover, the lack of definition has rendered Congress, state legislatures, the press, and the public less able to find solutions to the many problems and legitimate concerns that popularly fall under the heading of "privacy."

For example, identity fraud is widely perceived as a "privacy" problem. But it is better understood as a group of crimes that thrive on the use of personal identification and financial information. Because of this widespread misperception, the crimes that constitute identity fraud go poorly enforced while Congress considers banning many uses of Social Security Numbers in the name of "privacy." Limiting SSN use would likely stifle many benefits that consumers and the economy enjoy without effectively reducing this serious crime problem.

Similarly, unwanted commercial e-mail, or "spam," is an intrusion into electronic communications and a serious annoyance that is often labeled as a "privacy" problem. Spam exists in large part because e-mail marketers know little or nothing about the interests of potential customers. It is difficult to reconcile spam — e-mails broadcast to unknown people nearly at random — with the heart of the privacy concept, which is too much personal information being available too widely.

At Privacilla, we have a working definition of privacy that we believe should form the basis of policy discussions on the topic: *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.

Privacy is a personal, subjective condition. It is a state of affairs individuals enjoy based on sharing or retention of information about themselves consistent with their own preferences. These preferences are a product of such things as culture, upbringing, and experience. Because privacy is subjective, one person cannot decide for another what his or her sense of privacy should be. You can not tell me, either by giving your opinion or by passing a law, that my privacy is protected when I think it is not.

The first factor above goes to the existence of choice — the legal power to control the release of information. A person who wishes to maintain privacy in the appearance of his or her body, for example, may put on clothes and be relatively certain that no one will remove that clothing without permission. Few laws require people to remove their clothing and, thanks to the concept of "battery" in state tort and criminal law, private actors may be punished for touching our clothing in any way that interferes with bodily privacy. Our choices to hide or reveal information about the appearance of our bodies are protected by law.

Likewise, a person who wants to prevent others from gaining knowledge of his or her purchasing patterns may pay in cash and regularly change the stores at which he or she shops. He or she may also arrange by contract to have personal information maintained in confidence. Various legal protections, such as the law of contracts, give us autonomy and choice that we use to protect privacy.

The second factor is exercising that control of information consistent with our values. This is difficult in many commercial marketplaces. Many consumers are unaware of how the Information Economy works, and the fact that they are a part of it. Many industries are monolithic in their information practices. Arguably, they fail to fully inform consumers about what happens with personal information, and they offer consumers few alternatives. This is arguable, however. It may be that only a tiny, but vocal minority of consumers and activists actually wants to study commercial

information practices and exercise choice among different options. If a significant number of consumers do, they are a market waiting to be served.[1]

As policy-makers, we should not presuppose that a certain amount or type of privacy serves consumers' interests in the marketplace, and Privacilla's definition of privacy does not do this. Advocates who claim to know what consumers want in terms of privacy prove their ignorance by making the claim.

Consumers may rationally determine that they are safe from harmful uses of information when dealing with certain companies and leave it at that. The fact that hundreds or even thousands of mundane facts about themselves are in the hands of businesses may be a matter of indifference to reasonable people. Aware, empowered, and responsible consumers can demand of businesses what options they want in terms of information sharing or withholding. They can also demand, if they prefer, lower prices, customized service, combined offerings, and so on.

Unless Congress and state legislators are going to guess at consumers' true preferences and impose them from the top down, only consumer education will deliver privacy on the terms consumers want it in the commercial world. Governments cannot protect privacy directly; they can only foster or destroy people's ability to protect their own privacy.

Governments Pose a Unique Threat to Privacy

While protecting privacy in the commercial world may be difficult, protecting privacy from government is impossible. Dealings with government are categorically different from interactions in the private sector. When citizens apply for licenses or permits, fill out forms for regulators, or submit tax returns, they do not have the legal power to control what information they share. They must submit the information that the government requires. It is either illegal to withhold information or withholding

[1] *See* Paul H. Rubin and Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*, Progress & Freedom Foundation (July 2001) <http://www.pff.org/RubinLenard.pdf>.

information penalizes citizens of money or benefits to which they are legally entitled. The notorious "Big Brother" in George Orwell's *1984* was a caution against the powers of governments. When dealing with them, the first factor in privacy protection — legal power to control personal information — is absent.

It would be a mammoth, but worthwhile, task to catalogue all the personal information that is demanded by all federal programs. Additional study should include the purposes for which information is collected, other purposes to which it is put, and whether such information is ever eliminated from government records when it has served its original or successor purposes. The Federal Agency Protection of Privacy Act may help us do that.

Some studies suggest the scope of personal data collection and warehousing done at the federal level. In September 2000 testimony to the House Government Reform Subcommittee on Information Management, Information, and Technology, Solveig Singleton, now of the Competitive Enterprise Institute, surveyed federal databases.[2] Her non-exhaustive list included databases at the Commerce Department, the Department of Justice, the Department of Education, the Department of Energy, the Federal Bureau of Investigation, the Department of Health and Human Services, the Department of Housing and Urban Development, the Department of the Interior, the Department of Labor, the Social Security Administration, and the Department of the Treasury, which houses the Internal Revenue Service. Many of these databases include health and financial information.

In March 2001, a study issued by Privacilla.org found that, during the 18-month period from September 1999 to February 2001, federal agencies announced 47 times that they would exchange and merge personal information from databases about American citizens. New information sharing programs were instituted more than once every two

[2] Solveig Singleton, *Testimony Before a Hearing of the Subcommittee on Government Management, Information, and Technology on "Computer Security: How Vulnerable Are Federal Computers?,"* September 11, 2000 <http://www.house.gov/reform/gmit/hearings/2000hearings/000911computersecurity/000911ss.htm>.

weeks.[3] We characterized these programs as only the tip of an information-trading iceberg. The Computer Matching and Privacy Protection Act,[4] which causes agencies to report these activities in the Federal Register, applies only to a small subset of the federal agency programs that use personal data about Americans. New uses of personal information are made by federal agencies constantly. The Privacy Act requires only a declaration in the Federal Register of a new "routine use" before personal data is used and shared in new ways.[5]

In case it needs emphasis, the threats to privacy posed by government programs are not the result of malice or malfeasance of any kind. The political leaders who have instituted such programs, and the administrators who operate them, have the best intentions for serving the public. Similarly, the fact alone that any government program weakens American citizens' privacy should not be the sole reason to terminate or cut back the program. Rather, privacy should be an important factor that policy-makers consider whenever they are creating, implementing, or altering government programs. Studies like *Privacy and the Digital State: Balancing Public Information and Personal Privacy* by Progress & Freedom Foundation Senior Fellow Alan Charles Raul have made progress on that front. The Federal Agency Protection of Privacy Act would help make privacy part of the policy-making calculus in federal agencies and in the Congress.

The Administrative Process Should Inform the Public About Privacy Impacts

A prominent theory behind the Administrative Procedure Act's enactment in 1946 was the idea of "scientific government." This was the notion that a band of impartial

---

[3] Privacilla.org, *Privacy and Federal Agencies: Government Exchange and Merger of Citizens' Personal Information is Systematic and Routine*, March 2001 <http://www.privacilla.org/releases/Government_Data_Merger.html>.
[4] 5 U.S.C. § 552a(o) et seq.
[5] 5 U.S.C. § 552a(e)(4).

public servants would discover the one true public interest underlying legislation, and regulate in its service.[6]

Experience and modern scholarship reveal that the regulatory process, like the legislative process, does not locate some singular public interest. It responds to a cacophony of competing interests and values,[7] among which are the interests of regulators and bureaucracies themselves.[8] Administrative government does not improve on constitutional legislative processes so much as it improvises to accommodate the growth of the federal government in the latter half of the last century.

An increasingly prominent theory of the administrative process — though perhaps still a fallback from the idea that regulation would discern a "pure" public interest — is that it can open administrative lawmaking to public scrutiny,[9] particularly along lines that are deemed important by Congress. Several amendments to the APA in the last twenty-five years are consistent with this approach.

The Regulatory Flexibility Act,[10] passed in 1980, requires agencies to consider the special needs and concerns of small entities. Each time it publishes a proposed rule in the Federal Register, an agency must prepare and publish a Regulatory Flexibility

---

[6] Stephen Breyer, *The Legislative Veto After* Chadha, 72 Geo. L.J. 785, 796 (1984) ("At the time of the New Deal, some believed that the agencies might develop a science of regulation, the canons of which would hold agency managers in check through their sense of professional discipline.")

[7] *Id*. ("Today, few believe, for example, in a science of ratemaking. . . . [W]e suspect that at best [administrative] procedures guarantee a fair result; and we are aware that a fair ratesetting or power plant siting process does not necessarily mean an economically sensible rate or an environmentally optimal plant location."); WILLIAM E. NELSON, THE ROOTS OF AMERICAN BUREAUCRACY, 1830-1900 86 (1982) ("[Today, we] . . . understand that so-called scientific analysis of facts cannot yield answers to legal, political, and ultimately moral questions that require difficult value choices."); MARTIN SHAPIRO, WHO GUARDS THE GUARDIANS: JUDICIAL CONTROL OF ADMINISTRATION 65-67 (1988) (discussing agency 'capture' and 'professional deformation' of bureaucrats).

[8] *See* WILLIAM A. NISKANEN, JR., BUREAUCRACY AND REPRESENTATIVE GOVERNMENT (1971) (building a plausible economic model of bureaucratic behavior around the assumption that bureaucrats act to maximize the budgets of their bureaus). Niskanen later refined his thesis to argue that bureaucrats maximize their bureaus' discretionary budgets. WILLIAM A. NISKANEN, JR., BUREAUCRACY AND PUBLIC ECONOMICS 36-42, 273 (1996).

[9] *See* George W. Gekas and James W. Harper, *Early Returns from Government Regulation of Electronic Commerce: What's New is What's Old*, 51 ADMIN. L. REV. 769, 795-99 (1999). This excellent article calls for further opening of the administrative process through standardized electronic rulemaking and public access to rulemaking information. *Id*. at 797-98.

[10] 5 U.S.C. §§ 601-612, Pub. L. No. 96-354, 94 Stat. 1164-1170.

Analysis describing the impact of the proposed rule on small businesses, organizations, government jurisdictions, and the like. The Initial Regulatory Flexibility Analysis is subject to public comment, and a final regulation must be accompanied by a final Regulatory Flexibility Analysis. The Reg-Flex Act apparently provides the model for the Federal Agency Protection of Privacy Act.

Along similar lines, Congress passed the Unfunded Mandates Reform Act[11] in 1995. Among other things, UMRA requires federal agencies to inform and work with states and localities on major regulations. The Small Business Regulatory Enforcement Fairness Act,[12] passed in 1996, requires agencies to work more closely with small business in formulating regulations. It also subjects the analysis requirements of the Regulatory Flexibility Act to judicial review.[13]

These laws provide extensive precedent for the Federal Agency Protection of Privacy Act. The federal administrative process has been modified several times to accommodate the interests of various private- and public-sector institutions. Opening that process to the privacy interests of individual Americans is a matter of consensus among a broad cross-section of advocacy groups and congressional leaders, as we see from the wellspring of support for this legislation.

Some Important Details and Nuances to Consider

The Federal Agency Protection of Privacy Act is modeled on the Regulatory Flexibility Act, which has been used with success for more than 20 years to get greater information about the impacts proposed regulations will have on small entities. Simply, the Act would require agencies to issue the same type of analysis — an Initial Privacy Impact Analysis — along with a notice of proposed rulemaking. After considering the

[11] 2 U.S.C. § 1501.
[12] Pub. L. No. 104-121, 110 Stat. 856 (codified in scattered sections of 5 U.S.C.).
[13] *See* Northwest Mining Assn. v. Babbitt, 5 F. Supp.2d 9 (D.D.C. 1998); Southern Offshore Fishing v. Daley, 995 F. Supp. 1411 (M.D. Fl. 1998).

comments of the interested public, agencies would have to issue a Final Privacy Impact Analysis along with the finally promulgated regulation.

The success of the Regulatory Flexibility Act increased with the addition of the judicial review provisions to the Reg-Flex law in 1996, and it is pleasing to see that the Federal Agency Protection of Privacy Act also would make agency action subject to judicial review. Knowing that judicial review is available will make agencies naturally solicitous of congressional intent without requiring a great deal of litigation.

As with all legislation, there are some elements that could be improved. The casual reader may suspect that the Federal Agency Protection of Privacy Act would require agencies to assess how private sector implementation of regulatory mandates would affect privacy. This reading is probably a stretch and, judging by the public statements you and your colleagues have made, Chairman Barr, this is not your intent. Rather, it appears that your intent is for agencies to assess the consequences of their own information practices on privacy.

Language perfecting the bill could require agencies performing an Initial Privacy Impact Analysis to "describe the impact of **the agency's uses of information under** the proposed rule on the privacy of individuals." (proposed 5 U.S.C. § 553a(a)(1); suggested added language in bold). Likewise, agencies performing a Final Privacy Impact Analysis could be required to describe and assess "the extent to which **the agency's uses of information under** the final rule will impact the privacy interests of individuals . . . ." (proposed 5 U.S.C. § 553a(b)(2)(A); suggested added language in bold). These minor changes are one way to better express the intent of the legislation.

As you consider this legislation, you should be aware that it incorporates many policies beyond privacy. Security, for example, (made a part of Privacy Impact Analyses at 5 U.S.C. § 553a(a)(2)(A)(iv) and 5 U.S.C. § 553a(b)(2)(A)(iv)) is any number of practices and processes that respond to threats against a company or government's ability to function. Only one such function is carrying out privacy obligations. A business or government that lacks proper security may well violate its

privacy commitments, but may allow much worse to happen as well. The policy considerations that go into security of data in the hands of governments is a separate and significant issue beyond my expertise. There are benefits from requiring agencies to declare that they provide for security of personal information, as long as the agency is not so forthcoming as to breach security in the process.

Providing access and an opportunity to correct personal information is an important consideration (made a part of Privacy Impact Analyses at proposed 5 U.S.C. § 553a(a)(2)(A)(ii) and 5 U.S.C. § 553a(b)(2)(A)(ii)). But access and the opportunity to correct information go to fair treatment much more than privacy. Consider that there is no reason to access or correct information that will never be used. It is only important that information be correct if it may be used adversely to the interests of the individual. Using incorrect information against a person is unfair, not unprivate.

Access is also generally inconsistent with security. Giving access only to appropriate parties presents difficult security challenges clustered around authentication of identity. An Advisory Committee on Access and Security, convened by the Federal Trade Commission in early 2000, concluded its work without reaching consensus because of the complex interaction between these two, essentially conflicting, interests.[14] To illustrate this point: The privacy of information sealed in concrete and dropped to the bottom of the ocean is well protected, and it may remain private for eternity, but there is no opportunity to access it.

As with security, there is no harm in requiring federal agencies to inform the public of access and correction rights. Similar fairness protections are found in the Privacy Act of 1974, which obviously deals with more than privacy.

Using information for additional purposes (a part of Privacy Impact Analyses at proposed 5 U.S.C. § 553a(a)(2)(A)(ii) and 5 U.S.C. § 553a(b)(2)(A)(ii)) may affect privacy, depending on whether there is further disclosure of information. Information

[14] Federal Trade Commission, *Advisory Committee on Online Access and Security* Web page <http://www.ftc.gov/acoas/index.htm>.

about a citizen's medical condition and address, for example, collected for making health care payments, may not be rendered less private if the same part of the same agency uses that information to research whether people with certain conditions reside in certain areas of the country. If a subsequent use of information involves sharing that information with a state agency or a different federal agency, however, then the subsequent use can be said to render the information less private than it was before.

More importantly, though, a Privacy Impact Analysis that claims there will be no further sharing of information may provide false assurance. This is because nothing prevents governments from changing the rules about their use of information after it is collected.

The National "New Hires" Database is an excellent case in point. The Personal Responsibility and Work Opportunity Reconciliation Act of 1996[15] 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.

The purpose of this new database was entirely laudable — helping states locate parents who have skipped out on their child support obligations. But, already, the data is being repurposed. The National Directory of New Hires has been expanded to track down defaulters on student loans. Additional expansions have been proposed that would give state unemployment insurance officials access to the database.

In the better view, privacy in information is lost when it is submitted to government authorities. Unlike in the private sector, there is no higher authority to which Americans can appeal when personal information held by governments is put to new and unanticipated uses. A Privacy Impact Analysis that claims there are protections against use of information for changed purpose may be accurate for weeks, months, or years. But this is weak protection compared to contractual obligations formed in the private sector. Privacy-protecting contracts may be regarded as permanent because their breach

[15] Pub. L. No. 104-193.

is contrary to legally enforceable obligations that neither of the parties can unilaterally change.

This does not counsel against requiring Privacy Impact Analyses to discuss use limitations. Such analyses may make Americans more aware when commitments to restrict uses of information are changed by subsequent Congresses and Administrations. We will be better informed if the Federal Agency Protection of Privacy Act is passed with all its current provisions.

This discussion of the many nuances of the bill is intended to illustrate the enormous complexity of information policy, and to caution against unconsidered adoption of the so-called "Fair Information Practices." Often touted by pro-regulation privacy activists, they represent a vast array of different policies. Some are related to privacy; some are inconsistent with it. One does not have to agree with the baggage-laden concept of "Fair Information Practices" to support the Federal Agency Protection of Privacy Act.

The concept of "Fair Information Practices" appears to have originated in the early 1970s from a committee convened within the Department of Health and Human Services called "The Secretary's Advisory Committee on Automated Personal Data Systems."[16] The intellectual content of its report, commonly known as the "HEW Report," formed much of the basis of the Privacy Act of 1974 and its thinking is useful for controlling government data collection and use.

The report treated the public and private sectors identically despite the vast differences in rights, powers, and incentives that exist in these different worlds. For this reason, it cannot be said that the HEW Report addressed all the complexities of the privacy issue. "Fair Information Practices" do not apply well to the commercial world. As an analysis of government information practices, however, the HEW Report was an

[16] *See* Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, Department of Health, Education, and Welfare [now Health and Human Services] (July, 1973) <http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

important project and document. It also tells us that computers and privacy are not a new concern to Americans.

Conclusion

Again, Chairman Barr, Mr. Watt, and Members of the Subcommittee, congratulations on engaging an issue where you can truly improve the quality and character of life for all Americans. There is widespread consensus that people in the United States want to protect their privacy from government encroachments. The Federal Agency Protection of Privacy Act will inform the public about the privacy impacts of federal regulations, and empower them to make informed decisions about government programs. There are many nuances to consider and understand — privacy and information policy are very difficult areas — but the legislation you have proposed is an appropriate, measured, and important step in the pursuit of enhanced privacy protection for American citizens.