Hearing on
Privacy: The Use of Commercial Information Resellers by Federal Agencies
March 11, 2008

Testimony of Paula J. Bruening
Deputy Executive Director
Center for Information Policy Leadership
Hunton & Williams LLP

before the
U. S. House of Representatives Committee on Oversight and Government Reform
Subcommittee on Information Policy, Census and National Archives

Distinguished Chairman, honorable committee members, I am Paula J. Bruening, Deputy Executive Director of the Center for Information Policy Leadership. I am honored to testify on government use of information collected and retained in the private sector and H.R. 4791.

The Center for Information Policy Leadership is a think tank and policy development organization located in the law firm of Hunton & Williams LLP. The Center was established to develop innovative, pragmatic solutions to privacy and information security issues that reflect the dynamic and evolving nature of information intensive business processes and at the same time respect the privacy interests of individuals. The Center's member companies include leading organizations in health care, information services, retail, technology, financial services and consumer products. Since its establishment, the Center has addressed such issues as conflicting national legal requirements, cross-border data transfers, and government use of private sector data, with a view to how the future direction of business practices and emerging technologies will impact those issues.

The Center and its forty-one member companies believe that difficult information policy issues must be resolved in a responsible fashion if we are to fully realize the benefits of an information age. Center experts and staff, however, speak only for themselves. While I have consulted with Center colleagues and Center members, my comments today reflect my views and do not necessarily reflect the views of the Center member companies, Hunton & Williams LLP, or any firm clients.

I. Summary

The provisions of H.R. 4791 highlight the growing practice of government's access and use of information collected and retained by business, and the lack of legal protections for that information when such access is obtained. Private sector data provides government with important tools to further government objectives, particularly in law enforcement and national security.

The wide-ranging collection of data by government from third parties challenges traditional notions of information governance. The Privacy Act, which was designed to govern the collection and use of information by the federal government, did not anticipate current information collection practices, and interpretations of the Fourth Amendment, leaves data collected from third parties without Constitutional protections.

This failure of protection raises significant concerns for American business by compromising the trust relationship they work to establish with consumers, and by jeopardizing their opportunities to engage in ventures that involve data transfers into the United States.

It is time to establish a disciplined system for data collection and use by government that fosters use of information that is effective and responsible. The system must be forward looking, anticipating developments in technologies and data collection methods. The goal must be a governance approach that is sufficiently rigorous to re-establish trust, and sufficiently flexible to adapt to changes in the marketplace and technology.

II. Government use of information collected by the private sector lacks meaningful protections that take into account the realities of a data-driven society.

Government use of data about individuals is not new. Government has a long history of collecting information from its citizens for census purposes, to administer the tax system, to record births and deaths, to maintain voter registration, and to record real estate transactions. Government traditionally maintained records in courthouses, town halls, public offices and record repositories. Information once stored on paper is now located in government computer databases.

Today, a smaller percentage of the information used by the government is collected and stored by government itself. Increasingly, government turns to business as a source of all manner of data made available by consumers as they conduct their lives and engage in contemporary society. The proliferation of new technologies for data collection, the development of creative, information-dependent business models to deliver goods and services to consumers, the rapid advances in analytics tools, and the migration of such common activities as shopping, managing finances, using a public library and accessing health information to online and computer-based systems greatly increase the volume of data made available by individuals. Individuals leave trails of data as they purchase their morning coffee, access public transportation, use their mobile phone, visit a health clinic, shop, use e-mail and surf the web. Data now drives our most basic activities and interactions, and businesses of all kinds collect and store that data.

Government makes use of these data sources, seeking information to help them deliver services, administer social programs, manage health care delivery costs, combat fraud, secure the transportation infrastructure, protect cyber networks, investigate criminal behavior and combat terrorism. The data available to government from business is not only plentiful, it is powerful.

The protections in place to protect citizens from government abuse of data collected about them, however, no longer serve their intended purpose. The federal privacy law with the greatest sweep, the Privacy Act of 1974, was a response to growing concerns about the computerized databases of information maintained by the government. Based on principles of fair information practices, the Privacy Act was an effort to regulate the government collection and use of personal information. It limits storage of information by federal agencies to that which is relevant and necessary and only for purposes established by statute or executive order. The Privacy Act implements the principle of openness and transparency by requiring notice of the existence of record systems, and requires that the data subject be able to access and copy their records. It provides individuals with redress if an agency violates the Act with respect to data concerning them.

The Privacy Act no longer provides adequate protection for citizen privacy. As written, the Act did not anticipate the way in which our data collection systems would change, the manner in which government would access data, the ubiquity of data collection, or the robust data systems that would proliferate in the private sector to such an extent that business would serve as a primary source of data about United States citizens.

The most often cited limitation of the Privacy Act is that it applies only to information maintained in a "system of records," which the Act defines as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." The U.S. Court of Appeals for the District of Columbia Circuit held that "retrieval capability is not sufficient to create a system of records. . . 'To be in a system of records, a record must. . . in practice [be] retrieved by an individual's name or other personal identifier.'" In many cases government uses methods to access and use information collected by the private sector that do not involve a personal identifier. In other instances government accesses data but never establishes it in its own database, such that the information falls outside the protections of the Act.

This access to information collected in the private sector is further facilitated by Supreme Court interpretations of the Fourth Amendment to the Constitution that do not reflect the realities of a society and an economy in which sharing of data with third parties is a requirement and not a choice in the conduct of daily life. The Supreme Court held in 1976 in *United States v. Miller*[1] that there can be no reasonable expectation of privacy in information held by a third party. The case involved cancelled checks that the Court stated "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." The Court found that the Fourth Amendment was not implicated when the government sought access to them. The Court stated that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the

[1] *United States v. Miller*, 425 U.S. 435 (1976). The Supreme Court reinforced its holding in the context of information about telephone calls in *Miller* in *Smith v. Maryland,* 442 U.S. 735 (1979).

information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

Under the *Miller* holding, personal information can be freely accessed by government, without judicial review, simply because individuals have revealed that information to a third party. In an environment where the volume and sensitivity of information about individuals necessarily held by third parties continues to grow, this holding, taken together with the limitations of the Privacy Act, leaves the information of U.S. citizens extraordinarily open to undisciplined government access, scrutiny and use with little transparency, oversight or accountability.

Without question, the information collected by companies can serve as a critical resource for government, and with appropriate controls, government should continue to be able to access it. The data collected by companies provide keys to furthering law enforcement goals. With appropriate analytic tools, the data reveals points of vulnerability in our national infrastructure. Data helps government deliver services, administer programs and reduce fraud. Government should not be precluded from using valuable information collected by the private sector for these important purposes, but it should do so under established, rigorous guidance that ensures its use is both effective and responsible.

III. Government use of private sector data without legal protections and disciplined governance raises serious risks to U.S. business and compromises their opportunities for growth.

Companies sensitive to concerns about appropriate handling of information invest considerable resources to establish and maintain the trust of their customers by implementing data management and privacy practices that provide transparency and accountability about their data practices. Access to that information by the government without the protection of law places companies of all kinds in the position of acting as government data gatherers that are unable to assure their customers that the information they release to the government will be used for specified, limited purposes, that it will be properly handled when it is no longer useful, that it is accurate, or that the consumer has redress when data is mishandled. This failure of governance erodes consumer confidence in the companies themselves, reduces trust in information-fueled commerce more generally, and compromises growth of the digital marketplace.

Moreover, because of the lack of sound governance and the potential for nearly unfettered access by government to this information, every privacy question related to data collection in the private sector is shadowed by the issue of undisciplined government access and use of information. Efforts to resolve issues of consumer protection and privacy in new services, products, business models and technologies are complicated by this constant concern, making it more difficult to build consumer confidence that their data is being used responsibly. Without the necessary controls around government use of private sector information, companies are left to respond to the argument that because the government can so easily obtain data, it should not be collected at all.

The lack of oversight further compromises U.S. business' ability to engage with organizations and consumers internationally. Even as companies become more global in presence and reach, it has become increasingly unattractive to transfer data to U.S. companies because of foreign concerns about U.S. government access to information about foreign nationals that might occur outside the bounds of the laws of their home countries, and moreover, without any real oversight under U.S. law. The lack of systemic protections related to how the government obtains and uses private sector data sends a message that information about foreign nationals cannot be entrusted to U.S. business, limiting their opportunities to transfer and exchange data that can enable innovative business models, medical research and education initiatives. Lack of discipline and accountability challenges business' ability to make the case that information from foreign companies and about foreign nationals will be managed in a trustworthy fashion.

IV. This practice demands a system for privacy governance that fosters effective and responsible use of private sector data across government agencies.

The data brokers that are the focus of H.R. 4791 represent only one source of private sector data. Data sharing between the public and private sector takes place across a range of business sectors. Government turns to telecommunications firms, health care providers, retailers, financial institutions and Internet service providers for data that would further government objectives. While the provisions of H.R. 4791 single out one data resource, the issues raised by government access to information are not limited to information gathered from data brokers. The bill would not address the broader question of governance related to the government's access, management and retention of data accessed from all private sector sources.

It is time to consider the myriad ways in which government accesses, maintains and uses information collected in the private sector, and develop a governance structure for data use that establishes discipline and accountability in that practice. This inquiry must be forward-thinking and broad in scope, as the solutions we arrive at must be sufficiently rigorous to promote trust, and sufficiently flexible to adapt to as yet unanticipated technological and market developments.

The goal of this inquiry must be to develop a system of governance for government access and management of private sector data that fosters data use that is both effective and responsible. Such principles must mandate that government entities identify clear objectives, and understand what data will be used and how data will be used to accomplish those objectives. They must also set limits for its use, establish procedures for handling of data within government agencies and provide for its disposal. They must provide redress for citizens when their data has been misused.

Developing this guidance will require review of new and emerging technologies for data collection and storage, and the trajectory of future technological development. It will be important to consider the legitimate needs and activities of government for this data and the manner in which it uses it to further legitimate government objectives. It must involve development of reliable structures that establish accountability, oversight and

protocols for government collection, retention, use and disposal of data. At the same time, it must ensure that access to data is not unduly hindered when it is legitimately needed.

While the results of this effort must reflect the current and emerging environment for data collection and use, the Privacy Act can serve as a starting point for this inquiry. The fair information practices that form the foundation of the law continue to provide sound goals and guidance for establishing responsible information management practices, even as they are challenged by new technological and data processing developments.

I also recommend to the committee "Government Data Mining: The Need for a Legal Framework," an article authored by my colleague at the Center for Information Privacy Leadership, Professor Fred H. Cate,[2] to be published in the spring of this year in the *Harvard Civil Rights-Civil Liberties Law Review.* Professor Cate proposes recommendations for marshalling the power of data mining for appropriate uses while protecting personal privacy. While his comments are focused on data mining for national security, he notes that his recommendations apply equally to government data mining for other purposes. I would be happy to provide this article to the Subcommittee upon its publication.

V. Conclusion

Data about individuals collected in the private sector can provide government with an important tool in furthering its objectives, many of them critical to our national security and law enforcement. However, the failure of discipline and accountability in accessing, using and managing this data jeopardizes the trust between business and their consumers, and compromises their opportunities to engage in ventures that reach outside of the U.S. This gap in trust has implications for the development of information-driven businesses and services, the ability of companies to share data across borders, and ultimately the growth of the domestic online economy.

The provisions of H.R. 4791, while well-intended, do not reach the overarching question of trust in government access and use of private sector data across industries. Information maintained by data brokers is not the issue, nor is the private sector collection of data. The urgent issue is the lack of governance and accountability surrounding government access, use and management of data.

It is time to address this important question and to develop privacy governance for government that fosters effective, responsible data collection and use.

Thank you again for the opportunity to testify. The Center looks forward to working with the Committee as it pursues this important issue.

---

[2] Professor Cate is a Distinguished Professor and the Director of the Center for Applied Cybersecurity Research, Indiana University and Senior Policy Advisor, Center for Information Policy Leadership at Hunton & Williams LLP.