Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation

Brad Smith
Senior Vice President, General Counsel and Corporate Secretary
Microsoft Corp.

November 2005

Microsoft

Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation

Concern is growing among consumers, businesses, policymakers and privacy advocates about the misuse of personal information, the loss or theft of sensitive data files containing individuals' confidential information, and related privacy considerations.

A bewildering jumble of overlapping state and federal laws intended to address these concerns — though well intended — is creating confusion among consumers about how best to protect their personal information. It is also creating major challenges for businesses trying to comply with the growing complexity of inconsistent legal requirements.

Microsoft Corp. believes a comprehensive, yet flexible legislative solution is required at the federal level to provide robust and complete protection for consumers, and to provide consistency for organizations facing increasing risks and costs associated with managing and protecting personal information.

Historically, Microsoft has favored market-driven solutions and self-regulatory efforts to address data privacy and security issues. We believe that focusing on technology and industry best practices are the most immediate and effective ways to protect individual privacy. For example, Microsoft has developed innovative technical solutions such as advanced spam filtering in our e-mail software, the Microsoft® AntiSpyware tool, and cookie management in Internet Explorer. And we have collaborated with law enforcement, other industry leaders, privacy organizations and policymakers on a variety of efforts to create a trusted environment for users of the Internet and other technologies.

A Call for Uniform Federal Privacy Legislation

Over the past few years, however, several factors have altered the privacy landscape in such a way and to such a degree that we now believe the time has come to support national privacy legislation as a component of a multifaceted approach to privacy protection. As a strong supporter of free-market solutions, Microsoft did not come to this decision without careful consideration. But it is one we now believe is the right course in order to provide meaningful protections for individuals, while avoiding unnecessary obstacles to legitimate business activities.

As we see it, the goal of federal privacy legislation should be twofold: to establish ***baseline privacy protections*** for consumers, and to provide organizations with ***a uniform standard*** on which they can build effective privacy policies and compliance efforts. There are several reasons why this is an appropriate time to consider such legislation:

- An increasingly complex patchwork of state and federal laws is not effectively serving the interests of consumers, but *is* requiring businesses to navigate and adhere to a growing web of inconsistent legal obligations.

- Growing concerns among consumers about privacy and identify theft are eroding public trust in the Internet and threatening to dampen online commerce.

- Widely-publicized security breaches in recent months have exposed the need for comprehensive measures to improve not just security, but also consumers' understanding and control over their personal information.

The Legislative Collage

Today, much of the privacy regulation in the United States occurs at the state level, where many of the 50 states have enacted privacy laws that govern specific industries, issues or practices. Often, these laws are inconsistent, so that a set of business practices that is legal and commonplace in one state may be prohibited just across the state line. In addition, the *number* of state privacy laws is increasing quickly — for example, more than 20 states have passed separate financial privacy laws just since the beginning of 2004.

At the same time, Congress has enacted federal privacy legislation specific to certain industries. For instance:

- The Gramm-Leach-Bliley Act applies to financial institutions;
- HIPAA applies to health care providers;
- The privacy provisions of the Cable Act apply to cable operators;
- The privacy provisions of the Communications Act apply to telecommunications carriers;
- Specific privacy laws address children's online privacy, spam, telemarketing and junk faxes;
- And concerns over spyware and identity theft are now prompting an array of federal legislative proposals.

While all of these are well-intended efforts, this ad hoc approach to privacy legislation has many drawbacks. It has led to an overlapping, inconsistent and incomplete patchwork of state and federal laws that creates compliance chaos for businesses and uncertainty for consumers.

Consumers and businesses alike are often faced with the daunting task of determining whether one or more of the existing laws applies. The answer may depend on the type of data involved, the kind of company that collects it, where and how it's collected, and how it might be used.

For example, personal information collected by a bank is covered by one privacy standard, but that same information collected by a hospital is covered by a different standard. If that information is from a child under the age of 13, it's protected by yet another standard if it's collected online, but it may not be protected at all if it's collected offline. And each of those standards may be affected by state law, but in a different way from state to state. Yet, despite all of these legal distinctions, the consequences of misuse of that information could be exactly the same in each scenario.

Microsoft believes that a legislative framework that encompasses the core components of data privacy and security would obviate the need for a proliferating array of issue-specific, stopgap measures, and create a logical foundation on which appropriate, incremental legislative, technology and industry solutions can be built.

Privacy Concerns Are Growing

There is little question that the Internet and information technologies continue to bring enormous social and economic benefits to individuals and nations worldwide. They're empowering school children and seniors to learn, communicate and exchange ideas with family, teachers and new friends they've just met halfway around the globe. They're creating a whole new world of online commerce for individuals and for business. And, perhaps most important, they offer powerful tools to help individuals and governments participate in the opportunities of the 21st-century knowledge economy.

But the potential of information technology to continue to drive social and economic advances depends on building and maintaining a solid foundation of trust. Individuals will not take full advantage of the Internet or any other commercial medium if they believe their personal information could be compromised or disclosed in unexpected ways. A CBS News/New York Times Poll in September reported that nearly nine in 10 Americans are concerned about identity theft, with more than half saying they're "very concerned." This was underscored by a recent survey by Consumers Union, which indicated that 25 percent of Internet users have stopped making purchases online, and 29 percent of those who do shop online have cut back because of concerns about identity theft.

Effective federal legislation will help provide consumers with the confidence and knowledge that the legitimate businesses with which they engage are following an established set of baseline privacy practices.

A Comprehensive Approach to Identity Theft

The final reason Microsoft believes it's the right time for privacy legislation is that it has become increasingly clear that a comprehensive approach is needed to help protect consumers from identity theft and other misuse of their personal information.

Recent, highly publicized security breaches have resulted in the theft or loss of personal information about millions of American consumers. In response, numerous state and federal lawmakers have proposed or enacted legislation requiring businesses to implement security procedures that apply to personal information, and to notify individuals of certain security breaches.

Many of these measures make sense, and Microsoft has supported them. But these approaches do not fully address an underlying concern: a lack of transparency about how companies are collecting, using and disclosing personal information in the first place.

In many instances, prior to the publicity of a security breach consumers didn't realize these particular companies even existed, let alone that they maintained personal information about them. It's now clear that people want to understand who has their personal information, what information they maintain, how they use that information, and with what third parties they share it. Two out of three Americans think the government should be doing more to regulate the personal information that can be collected about them, according to a CBS News/New York Times Poll.

A tailored but more complete approach to privacy and security legislation at the federal level will help address these concerns by better informing consumers about who is using their personal information and how. And it will empower them to exercise meaningful control over their personal information both before and after any security breach occurs.

A Framework for Federal Privacy Legislation

With this context, Microsoft has outlined some core principles and specific proposals that we believe should be reflected in a comprehensive legislative approach to privacy and data security.

1. A Baseline Privacy Standard

The first goal is to create a baseline standard that applies across all organizations and industries. Such a standard should address the need for privacy legislation regarding both online and offline data, federal pre-emption, and harmonization with international privacy law.

Online and Offline

Federal privacy legislation should apply to both online and offline data collection, and to data stored in either electronic or paper form. This is important to avoid inconsistent standards that could jeopardize the free flow of information between the two media. It's also important because the potential risks to consumers are the same, regardless of where or how the data was originally collected.

Indeed, the consequences of the loss or misuse of personal information can be just as devastating whether that information is in paper form or electronic form. Of course, notification and security requirements may need to be different in offline and online environments, and any privacy legislation should recognize those differences. But these operational differences should not deprive individuals of core protections with respect to that data or obviate the need for businesses to keep the data secure. A single, flexible framework for all personal information will create broader and stronger protections for consumers, while enabling businesses to comply with one coherent set of privacy and security requirements.

Federal Pre-Emption

To address the current patchwork of state and federal law, federal privacy legislation should pre-empt state laws that impose requirements for the collection, use, disclosure and storage of personal information. Only a uniform national standard can address the complexities, inconsistencies and incompleteness of current laws, and bring the clarity and consistency needed to benefit consumers and businesses.

Federal legislation must do more than just create a "floor" above which states are free to impose additional requirements. That approach would still require any company that participates broadly in the national economy to either abide by the strictest applicable state law — transforming that state's law into default federal legislation — or to somehow compartmentalize its transactions on a state-by-state basis, which is impracticable and potentially to the detriment of the more important goal of protecting the privacy interests of consumers. The only realistic solution that protects consumers, while minimizing the operational burdens on responsible businesses, is to adopt a nationwide privacy standard. That standard should certainly be robust, but it should apply uniformly.

However, it's important that state attorneys general play a vital role in ensuring that companies adhere to sound privacy and security practices. In the spam and spyware arenas, Microsoft has successfully partnered with several state attorneys general to bring illegal actors to justice. Accordingly, in the privacy context, Microsoft supports any clarification that enables state attorneys general to enforce the federal legislation, and which ensures they can continue to rely on their enforcement authority under state consumer protection laws.

International Harmonization

To the extent possible, federal privacy legislation should be generally consistent with privacy laws around the world. Many U.S. companies operate globally — whether by doing business with consumers in other countries or having operations that require data to flow freely across national borders. Conflicting national privacy laws may thwart this global commerce by imposing inconsistent legal obligations that are at best confusing and at worst irreconcilable. A U.S. privacy law that is largely compatible with those of other countries would not only help reduce the complexity and cost of compliance, but also promote international business. Such legislation may help reduce barriers to data flowing into the United States — particularly from those countries that already have robust privacy laws. At the same time, U.S. legislation should avoid imposing new burdens on data flowing out of the United States, since there is no privacy need for such barriers if it is made clear that U.S. companies will remain responsible and liable for how that information is handled by their service providers, whether domestic or overseas.

2. Transparency

The second major goal of data privacy legislation is to increase transparency regarding the collection, use and transfer of personal information. This can be achieved in several ways.

Privacy Notices

Some form of privacy notice is a key component of virtually every privacy law and legislative proposal, and such notices have been widely adopted by industry. It's important that federal privacy legislation provide flexibility in how a privacy notice may be presented. At the same time, we believe it's important to establish basic, uniform standards that apply to the collection of personal information from an individual.

- The privacy notice should be made available *before* collecting personal information from an individual;
- It should describe what types of data are collected, how that information will be used, to whom and for what purpose it will be disclosed, and how and when an individual can limit its use and disclosure;
- It should permit and encourage innovative notification approaches such as "layered" privacy notices — typically a one-page or shorter privacy notice that is consumer-friendly, and supplements the traditional longer privacy statement.

This flexibility and support for innovative privacy notices is very important. For example, at Microsoft — where we offer online services on a global basis — we are faced with many different requirements for specific items that must be contained in a privacy notice. And in interactions with regulators, privacy advocates and others, Microsoft is often asked to add

additional detail or explanation into our privacy notices. As a result, privacy statements tend to get longer and more complex with time. And while that may make them more complete and precise, it makes them very difficult for the average consumer to read and understand.

Layered notices are an innovative way to bridge these competing needs. Microsoft's MSN® division has been a leader in developing and deploying layered notices, and we believe it represents a significant step forward in helping users understand a company's privacy practices and make informed decisions.

Material Changes to Privacy Practices

Federal legislation should also establish clear standards for handling material changes to privacy practices. An organization that wants to use or disclose personal information in certain ways not described in its privacy notice at the time the data was collected should first be required to take additional steps to ensure individual notice and choice. Those steps should include updating the applicable privacy notice; affirmatively notifying each individual of the new use or disclosure; obtaining an acknowledgement of that notice from the individual; and providing the individual with an opportunity to provide or withhold consent for the new use or disclosure.

Individual Access to Personal Information

Another way to increase transparency is to permit individuals to see the information about them held by organizations. Thus, federal legislation should mandate that businesses provide individuals with access to the personal information maintained about them, as well as a means to correct or amend incomplete or inaccurate information. Certain reasonable exceptions must accompany this legislative requirement for it to be workable, of course. For example, access should be required only if the requesting party reasonably verifies that he or she is the person to whom the personal information relates. The obligation to provide access may also need to be limited where providing access would be unlawful; violate the rights of other persons; compromise proprietary or confidential information, technology, or business processes; affect certain litigation or judicial proceedings; or impose a burden on the organization that is disproportionate to the risk of harm to the individual.

Breach Notification

Finally, individuals should be informed in the event of a security breach that could reasonably result in the misuse of their unencrypted sensitive financial information. Several current bills focus specifically on this point, and as is the case in most current legislative proposals, the standard must be narrowly focused in order to prevent notifications from becoming so frequent that consumers disregard them, or find that they're unable to differentiate between those that indicate a significant risk and those that don't. The requirements for the notification itself should be flexible — taking into account the size and type of the entity providing it, the number of people required to receive it, the relative costs for different methods of providing it, and the ways in which the entity typically communicates with its customers. Microsoft believes the Interagency Guidance interpreting the Gramm-Leach-Bliley Act, which gives discretion to covered entities to provide notice in any manner designed to ensure that a customer can reasonably be expected to receive it, is a sound model for federal legislation.

3. Control Over Personal Information

A third goal of federal privacy legislation is to provide individuals with meaningful control over how their personal information is used and disclosed. Specifically, Microsoft believes federal privacy legislation should require organizations to obtain the consent of an individual *before* an organization can use or disclose personal information for "secondary purposes" — that is, purposes not reasonably related to why the individual provided the information in the first place.

Here again, the requirements for this consent should be flexible: The greater the risk to the consumer, the more robust the required consent should be. And these requirements should avoid mandating excessive and unnecessary levels of choice for consumers which would bombard them with a confusing and annoying stream of warnings and options every time a piece of personal information is collected or used. The consent requirements should be grounded firmly in common sense. For example, explicit consent would make sense before certain sensitive personal information — such as information about a medical condition or access to a bank account — can be used or disclosed for a secondary purpose.

Explicit consent may also be appropriate to prevent certain unauthorized reuses or redisclosures of information by third parties. For instance, a third party may receive personal information from an organization either because the information was disclosed to the third party for a primary purpose described in a privacy notice, or because the individual consented to its disclosure for a secondary purpose. But that third party should not be free to later decide that it wishes to use that information in a way that goes beyond the original notice provided to, or consent obtained from, the individual. In order to prevent the complete loss of control over data once it has been transferred, third parties that receive personal information for one purpose generally should not be permitted to reuse or redisclose that information for other unrelated purposes without obtaining additional explicit consent from the individual.

Where the privacy risk is *lower* — for example with the disclosure on *non-sensitive* personal information for a secondary use — organizations should be able to obtain consent by offering individuals a meaningful opportunity to opt out. This would give consumers who are particularly concerned about their privacy an up-front choice. Explicit consent should not be mandated because most secondary disclosures of personal information do not pose a high across-the-board risk to consumer privacy, and the benefits of explicit consent do not outweigh its burden on legitimate business activity.

Finally, where the privacy risk is *lowest* — for example, where an organization uses personal information for its own internal purposes — the consent option should be the least onerous. In that case, the organization should be able to condition the receipt of an ongoing service on individual consent to such use — *if* that condition was made very clear to the user at the time he or she registered for the service. For example, many online services rely upon the display of targeted advertising to users in order to provide these services free of charge. If these companies could not require users to consent to receive ads as a condition of the service, many free or discounted online services would disappear.

4. Information Security

The fourth major objective of federal privacy legislation should be to ensure that organizations in possession of personal information take reasonable steps to protect against unauthorized access, use, disclosure, modification or loss. These steps should include administrative, technical and physical safeguards that are appropriate given the sensitivity of the personal information, the potential risks, the state of the art and the cost of implementation.

The security provisions of the Gramm-Leach-Bliley Act and the FTC's implementing regulations provide a good model — a flexible framework that gives organizations the discretion to implement the most appropriate technologies and procedures for their respective environments. This makes sense, because each business is in the best position to understand the particular security measures that are right for the different types and forms of personal information it maintains.

In contrast, a prescriptive set of federally mandated technical specifications would inevitably impose too high of a burden on some organizations for some information, but not adequately protect some personal information held by other organizations. And because security measures are constantly changing and improving as technology advances and engineers respond to evolving threats to information security, a one-size-fits-all regime would likely become obsolete.

The Need for Action

Clearly, these are complex issues with significant implications for consumers and for business. Doing nothing may, at first glance, seem an easier path. Should the industry and policymakers fail to act effectively however, organizations will face increasing risks and costs associated with a growing patchwork of inconsistent, overlapping and complex obligations; consumers will feel even more alienated, uncertain and fearful about disclosing personal information; and the promise of information technology as a new vehicle for economic growth will be at risk.

Federal privacy legislation is an important priority for Microsoft, and, we believe, for consumers, for our industry and for policymakers to consider. We look forward to working with all stakeholders to solve this important challenge.

##########