Privacy in a Connected World

An IBM White Paper

The Issue

The ability to protect individual privacy has been a concern for hundreds, if not thousands, of years. Whether the frame of reference is the privacy we seek behind closed doors or on the Web, the issue continues to redefine itself. And the process of defining privacy is complicated by the reality that privacy means different things to different people at different times.

A paraphrased version of one widely-accepted definition of privacy recognizes the fundamental importance of individual preferences: "Privacy is the ability of individuals to determine for themselves when, how and to what extent information about them is communicated to others." This definition can still be applied today, even in our fast-paced world.

The Challenge

The advent of the Internet and other pervasive technologies compounds the challenge of finding the right balance between individual expectations of privacy and other important values such as physical safety and security, law enforcement, personalized services and economy-wide benefits from information sharing.

The privacy challenge extends far beyond the information technology, financial or health care industries, into many aspects of our lives. This fact becomes even more compelling when we realize the relative infancy of the Internet revolution--one that experts estimate is less than 10 percent complete. Many organizations and consumers are only just beginning to realize the value of applied information technology and the increased efficiency and effectiveness of innovations in data collection and management.

Complicating the landscape today are heightened interests and concerns about privacy and personal and national security resulting from the unprecedented attacks on the US on September 11th. The search for a balance between personal privacy and the benefits of the networked world became immediately amplified by the desire for enhanced national and personal physical security. Government's ability to collect and use personal information in the interest of national security is now a core piece of the broader public policy debate on privacy.

In business, respect for personal privacy is integral to maintaining trusted relationships with existing and prospective customers. It's a reality that when businesses strive to offer more tailored, personalized services, the need to effectively and efficiently collect, store, analyze and disseminate information proportionately increases. This equation leads to the desire on the part of customers and employees to be repeatedly reassured that their personal information is secure from harm and fraud and is adequately protected. In fact, surveys show that most consumers will only shop online if they believe that their privacy and security will not be compromised.

"In our own actions, and for societies that want to avail themselves of the opportunities presented by e-business, striking a balance between the appropriate use of information on the one hand, and privacy and data protection on the other, is mission critical. IBM recognizes that imperative."

Harriet P. Pearson,

Chief Privacy Officer, IBM

Architecting an environment in which an individual's concern for privacy can be respected and protected while allowing businesses to offer tailored customer service is challenging, but not impossible. As the world's largest information services and technology company, IBM has taken a leadership role in understanding the many aspects of privacy -- from the perspective of the individual, to the enterprise and government. Through the establishment of sound, cross-company privacy policies and practices and business innovation, we are helping ourselves and our customers integrate privacy and security into their business models and objectives.

Towards a Framework

Today's increasingly information-dependent society demands the careful development of thoughtful frameworks that help us address the complex issues of privacy and data protection. To start from the broadest perspective, it is necessary to identify the roles and responsibilities of the core audiences involved -- government, industry and consumers. Then we can begin to map current practices and identify those that need to be evolved or created.

Government Action

Policy makers throughout the world have worked for years to balance national security and domestic law enforcement, civil liberties and free speech, open public records that support private-sector needs for data with economic benefits to citizens, such as lower product and credit costs.

Government leaders also recognize that they have at least two roles to play when it comes to privacy: setting the rules for the operation of the private sector and establishing guidelines for the government's own use of information--whether it's to provide improved government services to citizens or to carry out law enforcement.

The growing interconnectedness of society underscores the need for government officials to understand the broad implications of the Internet and the information technology revolution. Shifts in computing models—from centralized to distributed, from desktop-driven to 'Net-driven', from closed to open—have opened up the gates for data to freely flow around the world at lightening speed. These data flows can be originated by a single person working on his or her PC or by an international organization managing its activities across borders in order to realize operating efficiencies.

These challenges spurred the development of an internationally-accepted set of principles by the Organization for Economic Cooperation and Development (OECD) nearly two decades ago. A solid start, the OECD Guidelines were the first to outline "fair information practices" for organizations, including disclosure of data practices, use of appropriate security, and offering choices to individuals as to use of data.

With the OECD offering high-level guidelines, the challenge confronting many governments now is how to move these principles into practice. Over the years several models have emerged. In the European Union, comprehensive laws that govern information uses within the region and that attempt to regulate its flow outside the EU have been enacted. Canada and Australia have done the same, perhaps with a greater reliance on industry codes of practice. The US has legislatively-required protections in focus areas: government, credit reporting, banking and finance, health, and children's information. In other commercial areas, such as retail and online marketing, the US relies on its common-law traditions coupled with industry responsibility and leadership to chart the way. What is clear here is that when it comes to privacy, one size does not fit all. Countries will continue to work through the challenges of establishing a balanced approach.

IBM believes that government has a legitimate role to play in safeguarding privacy, as well as furthering the Internet revolution and supporting the global economy. To be able to play a meaningful role, government needs to stay on top of technological innovations and their impact on society at large. Only when our policy makers understand new technologies, the legitimate uses of data and the potential risks involved, can they effectively shape the right policies and focus their unique tools of legislation and enforcement.

Beyond putting to use tools of legislation, government must:

- openly encourage the private sector to further adopt appropriate information policies and practices on their own or through industry leadership groups such as TRUSTe or the Better Business Bureau.

- set an example to the private sector by becoming an "early adopter" of sound privacy policies and practices.

- recognize the global nature of the Internet and the international flows of data inherent in today's economies and build policies that accommodate these realities.

IBM can and is making a significant impact on privacy policy. From working closely with government officials and business leaders to offering testimony on issues of information technology policy, we are helping shape and drive the privacy debate.

"Privacy is the subject of considerable legal attention in Europe. But privacy is not just a legal consideration. It also makes sense from a business point of view, as our surveys show the growth of e-commerce depends on data privacy. Customers don't give their trust to us, they only lend it to us."

Armgard von Reden
Europe, Middle East Africa Chief Privacy Officer, IBM

Industry Responsiveness

What are the responsibilities and roles of the private sector? Even in geographies with considerable privacy regulation, governments recognize that robust and accountable market-led measures must play a prominent if not preeminent role. Europeans call it "co-regulation." In the US, we refer to private sector participation as "market-led governance" or industry "self-regulation."

The private sector can and is contributing a great deal to ensure a trusted marketplace. Why is that? The straightforward answer lies in the pervasiveness of technology within organizations and especially in such organizations' adoption of leading-edge technologies. Clearly the private sector has an immediate and critical need to effectively and efficiently respond to existing and unfolding privacy challenges.

One key point to remember is that in order to achieve privacy, one must cover the fundamental security policies and practices. In today's security-conscious environment it is critical to recognize that much of the infrastructure that secures data and other assets is under the control of the private sector--and thus much of the responsibility lies with individual companies and collective industry efforts.

As a starting point, private sector institutions can:

- establish a level of corporate commitment to privacy and security at the top of the company, beginning with the chief executive officer.
- establish and implement clear and effective privacy and security policies
- participate in collective action by relevant industry groups, to address society-wide privacy and security concerns.

Individual Empowerment

Protecting one's privacy, by its very nature, requires individual responsibility and action. It's easy to overlook the power of the consumer. But consider an individual who is dissatisfied with the way a particular company or organization presents and handles personal information. They have the ultimate recourse – break the relationship, no longer be a patron, and communicate their dissatisfaction to others. They can also publicly complain and seek recourse from the company. The bottom line is that respecting the privacy preferences of customers is good business.

Active participation and responsibility comes in many forms: from using available technologies to achieve greater security and privacy on the Web; to frequenting only those organizations and Web sites that have public, solid privacy policies; to educating children to be vigilant; to learning and pursuing one's rights under law and industry guidelines. Responsible individuals who provide personal information only to those organizations that gain their trust will in turn experience better-tailored and personalized services.

Many resources are available to help individuals. For basic information on privacy-related guidelines, tools and laws, start with www.understandingprivacy.org and explore the resources listed at the end of this paper.

IBM's Contribution

"e-business gives enterprises a powerful new capability to capture and analyze massive amounts of information they can use to serve individual customers more effectively. Yet this very capability troubles some people, who see it as a means to disclose or exploit their information. These are legitimate concerns, and they must be addressed if the world of e-business is to reach its full potential."

Louis V. Gerstner Jr.,
Chairman, IBM

More than three decades have passed since IBM became one of the first companies to adopt a global privacy policy, focused on employee information. Since then our commitment has produced a much broader range of data protection and privacy actions. As the Internet emerged, we continued to lead the industry with our privacy actions, including:

- Adopted one of the first global privacy policies for the Web on IBM's Web site, www.ibm.com.
- Established commercial Web privacy guidelines with other industry leaders and adopted them ourselves.
- Provided seed funding and support for the establishment of independent Web trustmark programs, TRUSTe and BBBOnline.
- As one of the largest advertisers, committed that IBM would advertise on a Web site only if it posted a privacy notice, influencing the industry to follow suit.
- Appointed one of the industry's first corporate Chief Privacy Officers.
- Established industry's first comprehensive, global privacy technology research initiative.

Underscoring these milestones, IBM has actively supported and participated in supporting the development of promising privacy technology standards including contributing substantial work to the World Wide Web Consortium on the Web standard P3P, or Platform for Privacy Preferences. During 2002, these efforts will continue within IBM and in conjunction with our customers and partners.

And now for the marketplace IBM has an extensive portfolio of privacy and security-related services, from technologies for enterprises and individuals to help define privacy preferences, to leadership and solutions expertise for large companies and governments. We recognize that the amount of valuable information enterprises gather is growing exponentially--creating both benefits and sometimes risks. Information that is appropriately secured and managed will help organizations better understand their markets and thus reduce costs and increase revenue. But not properly managing this information can lead to significant risks and exposures. IBM believes that the right technology and business processes--combined with strategic vision and policies--can help organizations extract value and minimize risks.

Through business units such as our Tivoli software group, the office of our Chief Privacy Officer, the IBM Global Security Solutions organization, Privacy Research Institute, and public policy programs, IBM has the resources to address the many dimensions of the privacy issue. We can help provide answers to some of the tough questions facing our existing and potential customers, including "How do we approach privacy?" or "Where do we start?"

The Conclusion of the Beginning

Privacy is a shared responsibility requiring well-planned management practices and systems to support it. It is an issue that requires the attention of everyone in a company or institution. Only then can privacy become pervasive and an expected part of how an organization interacts with its customers and stakeholders. IBM stands ready to play a leadership role.

"Addressing privacy, maintaining our leadership stance, and helping our customers address privacy is not only the right thing to do, it makes business sense. Trust is an imperative for any business and we will not jeopardize the trust of our customers, nor our workforce."

Harriet Pearson,
Chief Privacy Officer, IBM

Resources from IBM

- www.ibm.com/security/privacy -- comprehensive information on IBM's security and privacy offerings.

Other Resources for Businesses

- UnderstandingPrivacy.org -- provides a Privacy Manager's Resource Center and other information. Co-sponsored by IBM.
- PrivacyExchange.org -- an online resource for consumer privacy and data protection laws, practices, issues, trends and developments worldwide.
- TRUSTe -- IBM is a member of the TRUSTe program; TRUSTe is an independent, nonprofit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent.
- BBBOnline -- the online subsidiary of the Council of Better Business Bureaus. IBM has sponsored BBBOnline and its parent organization.

Resources for Individuals

- UnderstandingPrivacy.org – educational information from the Privacy Leadership Initiative.

- Consumerprivacy.org – educational material from several sponsoring consumer organizations.

- TRUSTE – www.truste.com – IBM is a member of the TRUSTe program; TRUSTe is an independent, non profit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent.

- BBBOnline – www.bbbonline.com – the online subsidiary of the Council of Better Business Bureaus.

- Center for Democracy and Technology – www.cdt.org – their mission is to promote democratic values and constitutional liberties in the digital age.

- Governmental organizations:

    - United States: Federal Trade Commission – www.ftc.gov
    - Australia: www.privacy.gov.au

- European Union – http://europa.eu.int/comm/internal_market

- Multilateral – www.privacyservice.org – A virtual partnership of several data protection offices, including Germay and Ontario, Canada.

May 2002