International Data Protection Standards

Key Points

- Cloud computing and international commerce are limited by conflicting international laws and regulations governing the privacy of data sent across national borders.

- Microsoft supports efforts to develop globally consistent policy frameworks that recognize the worldwide nature of data exchanges while providing strong privacy protection. Governments need to help develop clear rules and regulations that resolve conflicting privacy obligations.

- International privacy standards should be flexible, applied across industry sectors, and technology neutral. Strong collaboration among industry, government, and civil society is needed to achieve the right balance.

BACKGROUND

The Internet and cloud computing are erasing geographic boundaries for the flow of information. The Internet makes it possible for a business in one country to run a website or store data in a second country, and conduct transactions with customers the world over. This international flow of information benefits the global economy: it delivers new efficiencies, opens up new markets, and creates tremendous opportunity.

Yet when data is shared across regions, it's not always clear which laws, regulations, and protection principles apply. Today's regulatory models are based on a way of doing business that existed before digital globalization. In the European Union, for example, the European Commission's Directive on Data Protection places controls on the use and transmission of personal data to other nations. In the United States, statutes and regulations for data exchanges vary not only from state to state, but also by industry—for example, different privacy laws apply to healthcare and finance. For companies that conduct international business, such complex compliance requirements add to the cost of doing business.

Industry should work with government to develop more consistent frameworks that streamline the increasingly complex set of international, regional, and local laws governing privacy and data protection. In recognition of this need, the 32nd International Conference of Data Protection and Privacy Commissioners in 2010 passed a resolution that called for the organization of an intergovernmental conference with the goal of developing a binding international instrument on personal data protection and privacy. Also, the International Standards Organization (ISO) continues to develop consistent and predictable standards that help to protect data security and privacy around the world.

MICROSOFT APPROACH

Microsoft's longstanding commitment to privacy includes principles, policies, and procedures for building privacy protections into its products and services, from development through deployment and operation.

- Microsoft's privacy standards govern the development and deployment of Microsoft products and services. These standards, a version of which have been made public, offer detailed guidance on customer notification and consent procedures, help make sure data security features are sufficient, maintain data integrity, and provide user access and controls. Microsoft also helps to protect customers by delivering more secure products through the Microsoft Security Development Lifecycle (SDL), a software security assurance process which embeds security and privacy throughout product development. Microsoft designs its cloud services to help ensure data security and user privacy.

- Microsoft works to help ensure that employees, vendors, and partners are accountable for the handling of customers' personal information. Each Microsoft business unit is responsible for developing procedures to strengthen and support accountability, and for assigning specific staff members the day-to-day responsibilities of monitoring and protecting privacy.

- Microsoft follows and implements international privacy and data protection standards. For example, Office 365 is compliant with ISO 27001.

POLICY CONSIDERATIONS

- Microsoft supports current efforts to harmonize data protection rules and is a strong proponent of extending the ISO 27001 standard and its data protection controls as the basis of those rules. Broadly adopted and consistently applied, ISO standards can help to support the protection of cloud-based data.

- International privacy standards should be flexible and technology-neutral, and should be applied across sectors.

- Microsoft supports an accountability-based approach to data privacy, which permits data to be transferred across international borders without restrictions as long as the data exporter remains accountable for protecting the data regardless of its geographic location. This approach would hold organizations responsible for protecting data while still giving them flexibility to accommodate evolving data transfer needs.

- In order to optimize the efficiency of online services and deliver the performance and reliability that customers expect, cloud providers should be able to operate data centers in multiple locations worldwide and transfer data freely among them.

Helpful Resources

An overview of Microsoft privacy policies and initiatives
www.microsoft.com/privacy

Privacy and cloud computing at Microsoft
www.microsoft.com/privacy/cloudcomputing.aspx

Privacy by Design at Microsoft
www.microsoft.com/privacy/bydesign.aspx