February 2013

# Privacy by Default

## Key Points

- Microsoft recognizes the important role that default settings can play in protecting privacy; however, a prescriptive approach to Privacy by Default could lead to unintended consequences, such as limited innovation, limited functionality, and user frustration.
- Microsoft believes that the goals of Privacy by Default are best accomplished when default settings are tailored to the technology or service. Appropriate default settings are best determined on a case-by-case basis as part of an overall approach to implementing Privacy by Design.
- Microsoft products and services undergo privacy reviews, which identify privacy issues and help product teams follow Microsoft privacy policies and standards.

## BACKGROUND

Privacy settings play an important role in helping people protect their privacy online. Consumers expect companies to create privacy settings that provide transparency and control over the ways that organizations collect, use, and store personal information. Companies with online operations and services must develop privacy practices that meet these expectations.

Privacy by Default is a software design concept that is presently being considered by a number of data protection authorities, including the European Commission. Broadly defined, Privacy by Default would prohibit the collection, display, or sharing of any personal data without explicit consent from the customer. More detailed definitions often include a requirement that privacy settings that limit the sharing of personal data be turned on by default. For example, a social networking service would not make any information about customers publicly viewable until customers take affirmative steps to allow it.

Advocates for Privacy by Default claim that many people don't know how to actively enable their privacy settings; that people believe it's too difficult or tedious to configure privacy settings; or that a lack of default settings can lead to a higher risk to children's privacy on services such as social networks.

There are a number of challenges to implementing Privacy by Default. First, it's problematic to create universally agreed-upon settings that address all types of software and online resources. It's also difficult to create and implement settings that satisfy the needs of a broad range of customers. Finally, Privacy by Default could result in software design that confuses and frustrates customers with repeated notices and warnings.

## MICROSOFT APPROACH

- **Privacy by Design at Microsoft** describes not only how Microsoft builds products, but how the company operates its services and organizes itself as an accountable technology leader. For Microsoft, it includes all of the people, processes, and technologies that help maintain and enhance privacy protections. Privacy by Design is in place because the company must earn the trust of customers and partners every day by being as transparent as possible about those policies and processes.
- **Accountability** for data privacy is a key Microsoft principle that determines how the company and its vendors and partners manage the personal information of Microsoft customers. Each Microsoft business unit is responsible for developing procedures to uphold the company's accountability commitment.
- **Case-by-case approach.** Microsoft believes the goals of Privacy by Default are best accomplished when the default settings are appropriate to the context of the technology or service and are determined on a case-by-case basis.
- **Education.** Microsoft knows customers want and expect strong privacy protections built into its products and services, and is committed to providing tools to assist people in making better choices about their online privacy. To help people better manage their personal information online, Microsoft created a Privacy in Action page that explains Microsoft privacy settings, offers videos about how people can protect their privacy online, and includes a report on Microsoft's privacy research.

## POLICY CONSIDERATIONS

Microsoft believes privacy regulations should meet certain fundamental requirements:

- **Technology neutrality.** There is no question that technology will continue its rapid change. Consequently, any privacy regulation framework should avoid preferences for specific services, solutions, or mechanisms to provide notice, obtain choice, or protect consumer data. Preference for one privacy default over another, for example, could restrict innovation because it might deter providers from developing alternative or improved protections for consumer data.
- **Flexibility.** Privacy regulation frameworks should be flexible enough to allow businesses to develop innovative privacy technologies and tools. Flexibility means that businesses can adapt their policies and practices to the contexts in which customer data is used and disclosed and to fit the relationship that a business has with its customers.
- **Certainty.** In addition to having flexible privacy regulation frameworks, businesses must ensure that their implementation of privacy settings meets international standards. Multiple default requirements that are contradictory or are not properly harmonized internationally will slow development and create uncertainty in the release of new products and services. Regulators should encourage innovators to assess the full spectrum of potential privacy risks and make appropriate decisions about privacy designs and settings.

## Helpful Resources

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

Privacy by Default: Microsoft's perspective and approach
**aka.ms/PrivacyDefault**

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

Privacy in Action
**www.microsoft.com/yourprivacy**