February 2013

Next-Generation Privacy Models

Key Points

- The current data protection model of notice and consent as the primary means for individual control should be reconsidered, in light of the burden to consumers posed by the increasingly complex uses and reuses of their data.
- Instead, other models of control should be considered, such as a model based on the use of data. This may be more appropriate for the privacy protection of both the organizations that collect data from individuals and other parties that may also use data.
- A model based on use can exist with many current fair information practices, as well as applicable law, and in no way diminishes the requirement that information be collected in a fair and lawful manner.

BACKGROUND

In January 2002, Bill Gates sent an email to all Microsoft employees announcing the Trustworthy Computing Initiative. His email outlined what today are still the key tenets of trustworthy computing: security, privacy, and reliability. Gates recognized that privacy concerns would be critical to building trust in information technology and, as a result, Microsoft invested heavily in a privacy program. These investments continue to help foster opportunities for its engineers to create technologies, services, and features that are based on customer needs, including sensitivity to their privacy concerns.

Traditionally, data privacy in many parts of the world has been based upon the concept of Fair Information Practices, which include notions such as notice and consent. These require a company to give notice to individuals through a privacy statement that describes what information will be collected and how it will be used. The company promises not to use data in a manner inconsistent with the consumer's choice. Consumers give their consent by agreeing to the privacy statement. In some jurisdictions, consent requirements play an even larger foundational role in privacy protection models.

In the modern information economy, however, the massive aggregation of computer data (sometimes referred to as big data) and cloud computing are creating highly complicated flows of data, putting the notice-and-consent model under heavy strain in three significant ways:

- First, choices regarding collection of an individual's data and its use have become so complex they are difficult for most individuals to understand, let alone manage.
- Second, the model assumes an interactive relationship between the individual and the entity collecting and using the data, a relationship that increasingly may not actually exist.
- Third, the true value of data may not be understood at the time of collection, and future uses that have significant individual and societal benefit may be lost if privacy models focus solely on the collection of data.

Asking individuals to assume responsibility for policing the use of data in this environment is no longer reasonable, nor does it offer sufficient checks against inappropriate and irresponsible data use. As a result, consumers have a disproportionate burden of responsibility.

Instead, a model based on the use of data may be better suited as a means of providing effective protection for both the organizations that collect data from individuals and parties that use it. Such a use model requires all organizations to be transparent, offer and honor appropriate choices, and ensure that risks to individuals related to data use are assessed and managed. Such an approach also emphasizes the need for greater accountability by organizations that manage and share personal data.

A model based on use would be designed to help achieve five goals: (1) protect privacy in meaningful ways; (2) optimize the use of data for the benefit of both individuals and society; (3) ensure that those who use data are accountable for its use; (4) provide a regime that permits more effective oversight by regulators; and (5) work effectively in a modern connected society. In a data-rich world, achieving these objectives requires meaningful user control and transparency.

MICROSOFT APPROACH

- Microsoft believes that the way data is used, rather than how it is collected, could be a more effective premise for defining data protection and privacy obligations related to that data. Microsoft supports an approach that emphasizes a model based on use rather than relying on traditional notice and consent.
- Microsoft recognizes the need for self-regulatory principles governing data usage that give individuals greater control over their data and greater transparency into how companies manage and use their data. Microsoft's own practices include commitments to customer notice of and control over data use, and to providing data security.
- Microsoft's privacy principles are generally tailored to account for the types of information the company collects and how it intends to use that information.

POLICY CONSIDERATIONS

- Microsoft encourages the adoption of privacy models based on use within self-regulatory principles, a concept being explored in legislative proposals in both the United States and Europe.
- A model based on use can exist with current fair information practices, as well as applicable law, and in no way diminishes the requirement that information be collected in a fair and lawful manner.
- As governments act to address issues associated with emerging technologies and online services, they should not stifle innovation and technology adoption in the process. Government and industry can work together to establish appropriate principles.

Helpful Resources

Microsoft Trustworthy Computing Next
www.microsoft.com/twcnext

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

A Use and Obligations Approach to Protecting Privacy: A Discussion Document. The Business Forum for Consumer Privacy, December 2009.
aka.ms/Use-Discussion