Microsoft

Trustworthy Computing

Privacy from the Ground Up

Microsoft's approach to providing privacy protections in software products and Internet services

July 2011

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

Contents

Microsoft Privacy Principles

Accountability in handling personal information within Microsoft and with vendors and partners

Notice to individuals about how we collect, use, retain, and disclose their personal information

Collection of personal information from individuals only for the purposes identified in the privacy notice we provide

Choice and Consent for individuals regarding how we collect, use, and disclose their personal information

Use and Retention of personal information in accordance with the privacy notice and the consent that individuals have provided

Disclosure or Onward Transfer of personal information to vendors and partners only for purposes that are identified in the privacy notice, and in a security-enhanced manner

Quality Assurance steps to ensure that personal information in our records is accurate and relevant to the purposes for which it was collected

Access for individuals who want to inquire about and, when appropriate, review and update their personal information in our possession

Enhanced Security of personal information to help protect against unauthorized access and use

Monitoring and Enforcement of compliance with our privacy policies, both internally and with our vendors and partners, along with established processes to address inquiries, complaints, and disputes

"[W]e have a responsibility … to build the technology that will protect the anonymity, the privacy, the security of what I say, who I say it to, where I go, what's important to me."

—Microsoft CEO Steve Ballmer

Bringing Privacy into Design, Development and Deployment

The Microsoft Privacy Principles (see sidebar), our internal privacy standards and the specific privacy statements[1] we make to our users guide our collection, use, and management of customer and partner data.

Our company has more than 40 full-time privacy professionals and several hundred other employees who oversee the application of our privacy policies, standards, and procedures across Microsoft products, services, processes, and systems. This multidisciplinary, cross-company team comprises not only dedicated privacy professionals but computer scientists, engineers, legal professionals, business executives, and marketing experts.

In order to make privacy an integral part of a new product or service, privacy requirements and considerations need to be identified and addressed throughout development. Our 'privacy review process' encompasses the development lifecycle and is generally equivalent to what many organizations refer to as a "Privacy Impact Assessment" or PIA. Though PIAs vary widely, the 2007 Loughborough University study "Privacy Impact Assessments: International Study of their Application

[1] Examples include Microsoft's Online Privacy Statement at http://privacy.microsoft.com/en-us/fullnotice.mspx and the Windows Internet Explorer 9 Privacy Statement at windows.microsoft.com/en-US/internet-explorer/products/ie-9/windows-internet-explorer-9-privacy-statement .

and Effects" [2] which examined PIA from various countries, found four common elements in the PIAs they reviewed. The Loughborough study notes:

> "PIAs everywhere are designed to:
>
> - conduct a prospective identification of privacy issues or risks before systems and programmes are put in place, or modified
> - assess the impacts in terms broader than those of legal compliance
> - be process rather than output oriented
> - be systematic."

Beyond these common elements PIAs necessarily vary based on the project or process being assessed and other environmental factors that affect the organization that is performing it such as the specific market, culture and legal context in which the organization operates. PIAs can be employed to evaluate endeavors such as the design, development and deployment of technology products, services, marketing campaigns and other efforts.

The first step in Microsoft's typical privacy review process, the privacy assessment, will yield a privacy risk rating (See Figure 1, phase "New"). Based on various factors such as the functionality of the proposed product and the rating, privacy professionals with appropriate backgrounds (a team may include legal, technical, marketing, etc.) are brought in to the project. Next, the assessment and rating are validated ("Validation" phase in Figure 1) by the privacy team, working jointly with the development team. From this point on, as the development team designs and builds the product, work in progress may undergo successive privacy assessments. Necessary remediation actions may also be identified and implemented to minimize privacy risks ("Review" and "Remediation" phases in Figure 1). Here, it is important to underscore the fact that the privacy assessment marks the beginning of a privacy review process that may iterate multiple times, following product development, until the privacy risks that are identified have been addressed as per company policies. Once the product or service is completed, a final privacy assessment and approval takes place to determine if all requirements have been met ("Complete" phase in Figure 1). Independent validations and audits may also take place depending on the service ("Archive/Deliver" phase in Figure 1).

[2] http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf

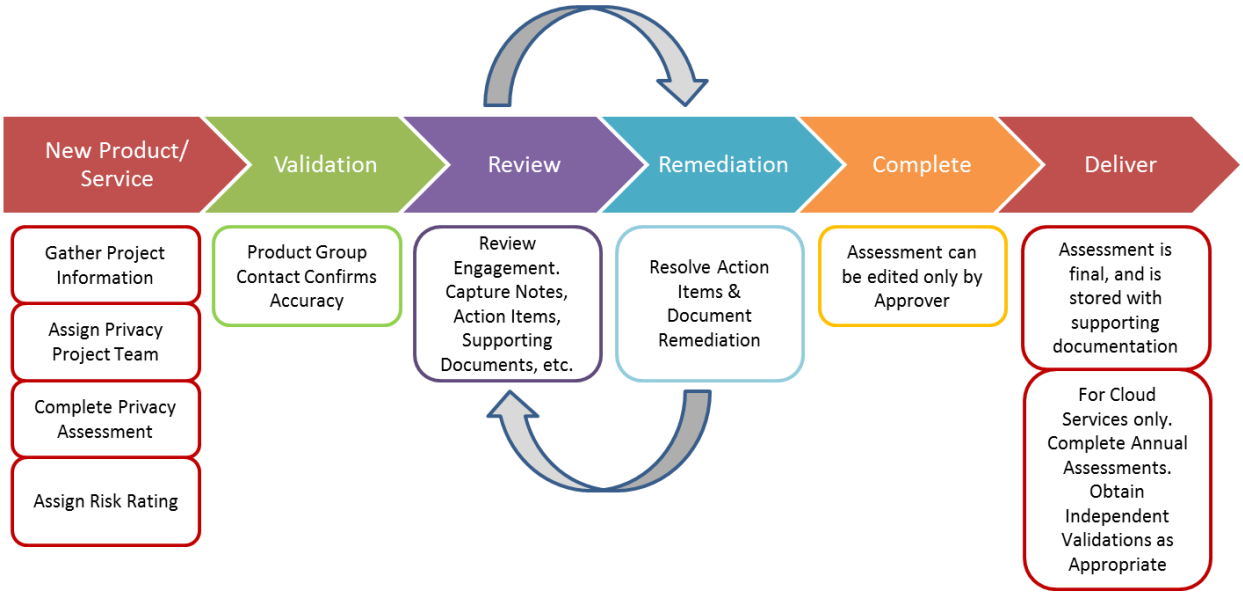

Figure 1. The Microsoft privacy review process analyzes and determines product and service privacy requirements and risks early on. It also provides a series of checks and balances to help ensure that the end products of this process comply with Microsoft's privacy principles and policies.

The privacy review process is supported through the deployment of internal tools that employ project-specific criteria to help determine the information that is required to complete the review. These internal tools also track the evolution of the privacy requirements as the product moves from concept to release. The most widely used tool is the "Policy Approval Manager," (or PAM) (shown in Figure 2), developed by Microsoft internally, to help manage projects which range from the development of a packaged product, to the development and deployment of an Internet service, to a web-based marketing campaign.

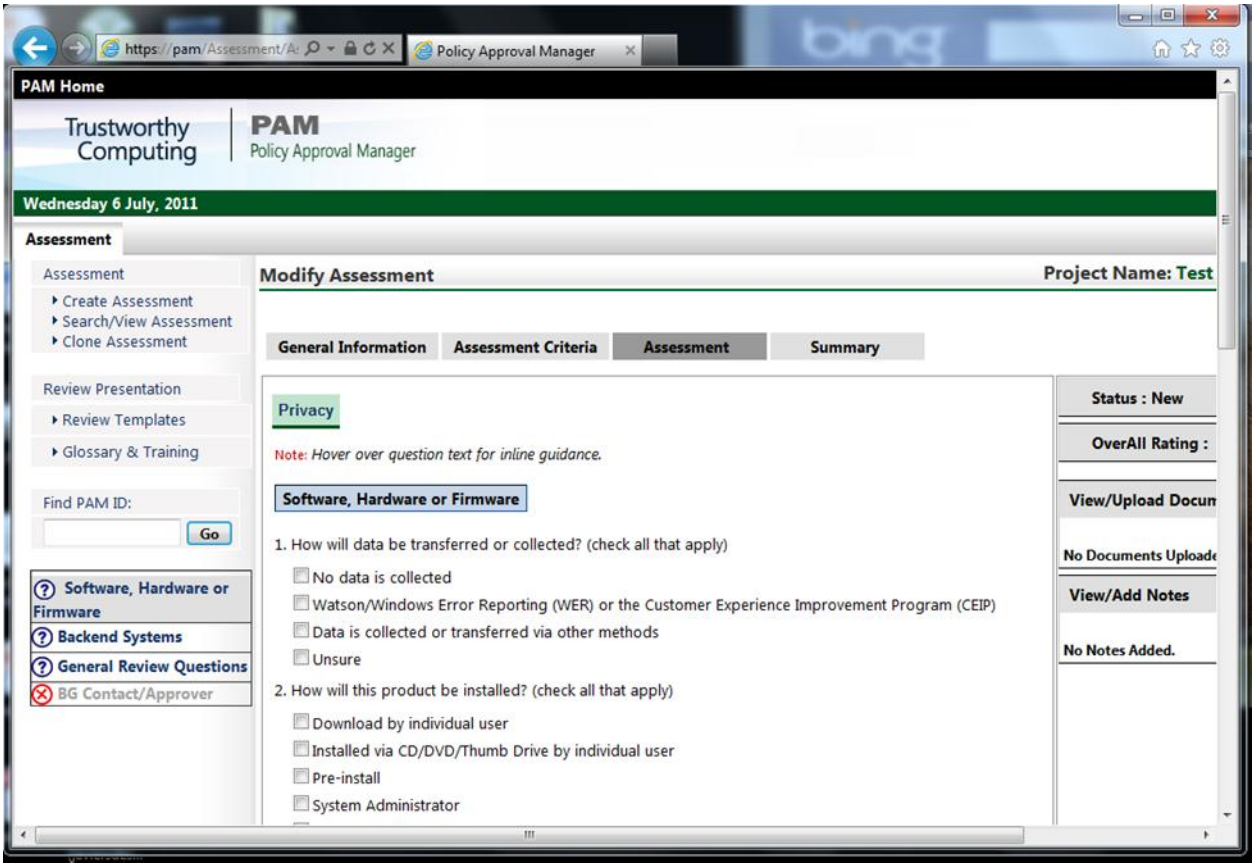

Figure 2. The Policy Approval Manager (PAM). The "Assessment" tab shown above includes questions that may be revisited multiple times during the review process; answers to the questions may change along the way. Thus, the product development team may be "Unsure" as to whether they transfer or collect data at the beginning of the process. If that happens however, PAM will automatically flag that particular project as a high priority item and the "Unsure" choice may affect some or all of the decisions that are made at the beginning of the privacy process. The high priority flag will remain active until the "Unsure" box is unchecked, assuming that there are no other issues that may require it to remain active.

This privacy review process represents only a portion of Microsoft's overall privacy efforts. The Privacy Governance program (which encompasses the privacy review process) also includes ongoing training for privacy professionals, the identification and analysis of emerging privacy issues and a regular review and updating of our internal privacy standards to meet the rapid pace of technological change.

Decisions on how to implement privacy enhancing technologies and privacy-friendly features are guided by numerous factors including: product- and consumer-focused research, customer feedback that is gathered by our technical support staff and sales force, Microsoft's Privacy Principles, company policy and regulatory requirements. We also hope that some of the exciting efforts that Microsoft Research has undertaken in this area will yield significant results in the future. For more information on this topic, see the box "Scientific Research on Privacy at Microsoft."

Scientific Research on Privacy at Microsoft

Microsoft Research employs more than 800 research scientists, including some of the world's foremost computer scientists, sociologists, psychologists, mathematicians, physicists, and engineers. Based in eight locations around the world, Microsoft researchers conduct both basic and applied research in computer science, software engineering, and the interaction between information and communications technology and society.

Current privacy-specific projects at Microsoft Research include the following:

- Database Privacy. This project focuses on privacy challenges related to revealing accurate statistics about a population while preserving the privacy of the individuals that make up that population. The central concept here is *differential privacy*, which ensures that the system behaves essentially the same way, statistically-speaking, independent of whether any individual, or small group of individuals, opts in or opts out of the database. Moreover, this property holds even if the database is cross-correlated with other databases in an attempt to reveal the identity of specific individuals in its population.
- Social Media Collective. This project explores people's practices and attitudes when interacting through social media applications such as instant messaging, online chat, and social networking websites. Focal points include users' expectations and concerns about privacy and how these might vary among different age groups.
- Cryptographic Cloud Structure. Researchers are working on cryptographic tools that will enable an individual or organization to secure data stored in the cloud, even if the data resides on a computer infrastructure that is not controlled or trusted by the user. Potential outcomes of this project include tools that enable patients to generate and store encryption keys that give them full control over which entities can access which portions of their health information.

Other research areas include the creation of tools for automatic verification of computer code that uses cryptography; efficient, anonymous aggregation of data from distributed networks; verification of trust and reputation using statistical tools; maintaining anonymity while roaming through wireless networks; detecting PII in digital documents; and maintaining location privacy. Details about these and other privacy-related research projects, including scientific whitepapers and results summaries, can be found at the Microsoft Research website.

For a comprehensive list of projects, go to http://research.microsoft.com/apps/dp/pr/projects.aspx. Privacy and security projects can be filtered from this list by using the filtering options available on that page.

Through its governance program and investment in research and new technologies Microsoft seeks to create a climate where company employees are aware of privacy in general, and helps foster opportunities for our engineers to create technologies, services and features that are based on customer needs, all backed by sound policies and principles.

Microsoft also seeks to address the challenges that organizations in different industries face every day in maintaining the privacy and confidentiality of personal data concerning their employees, customers, and partners. These organizations must prevent leakage or breaches of this information and, at the same time, derive business value from it by making information accessible to the right individuals for the right purposes. In addition, Organizations must comply with a diverse and growing list of legal requirements, industry standards, and internal policies. To help them meet these goals, Microsoft provides a number of tools and technologies including those that help with data classification, minimizing the collection and unnecessary distribution of personal information, and securing files through encryption. Such capabilities are essential to an organization's efforts to provide appropriate data privacy and security protections.

The final section of this document describes our focus on privacy and data protection in a consumer product, and the types of results we look for from Microsoft's privacy process.

Kinect for Xbox 360: "You are the Controller"

In November 2010, Microsoft introduced Kinect, a hardware accessory, to the popular gaming console Xbox 360. With Kinect, as the tag line for the marketing campaign reads, "you are the controller." Kinect enables individuals to play games in the Xbox console by simply acting the movements they want to make in the game, in front of the Kinect device. Gamers have no need for hand-held game controllers as the Kinect device simply tracks their body movements and then commands on-screen avatars to mimic those movements, as shown in Figure 3.

Figure 3. Gamers do not need to carry or hold any type of physical device while playing a Kinect-enabled Xbox game. They simply use their bodies to act the movements they want avatars to mimic on screen, the Kinect device takes care of the rest.

Gamers can also opt to sign on for a session by using Kinect ID, a feature that enables the Kinect device to recognize the player's facial features, and then provide online access to the right Xbox LIVE account (if the game console is connected to the Internet).

Kinect-enabled games may take snapshots or videos of individuals while at play, and make them available for download, copying or sharing through the Internet-based service KinectShare.com.

Given this set of capabilities, soon after the product was conceived the Kinect product team recognized new ground would have to be broken in terms of privacy protections, and that these would eventually play a significant role in the commercial success of the device. This illustrates our approach to the concept of Privacy by Design.

Figure 4. The Kinect device.

Privacy Protections: In order to enable the described capabilities, Kinect employs four types of data:

- Kinect Performance Data. This information helps Microsoft continuously improve Kinect performance. It does not personally identify any individual, and collection of this data cannot be disabled. As gamers play, Microsoft collects information on how the Kinect device and platform software are functioning, usage patterns within the Xbox Dashboard applications, and other data that does not directly or personally identify anyone. The company may analyze this performance data to ensure users are receiving the optimal game experience, and to help improve Kinect games and the Xbox 360 platform. Microsoft may also share some of this aggregated data with companies that provide Kinect-enabled games which will help them improve their product.

- Tracking movement. Kinect uses its built-in cameras and sensors to scan the gamer's body - this is called skeletal tracking - and create a numerical signature of up to 20 body joints. A graphical representation of this signature would look like the stick figure shown in Figure 5. Skeletal tracking data, which does not personally identify an individual, is stored on the Xbox console's memory only while a session of one or more gamers is going on. This data will be deleted from the console once the session stops or the console is turned off. It may occasionally be sent to Microsoft for analysis and game-experience improvement. If the gamer is using the Xbox LIVE service, which allows him or her to interact with other online gamers, skeletal tracking data is

sent to the other players' Xbox consoles to enable on-screen interaction between avatars. Once the game session is over, however, skeletal tracking data is deleted from all consoles.

Figure 5. A laboratory view of a graphical representation of skeletal tracking data.

- Facial recognition data. This data can be used to identify an individual, and is collected only from those gamers that choose to create a Kinect ID. The Kinect ID is an optional way to sign in to an Xbox LIVE account. It is stored permanently in the local Xbox console, and is not transmitted to Microsoft. To create a Kinect ID, the device's camera collects information about the person's facial features in different poses and potentially in different light conditions, and builds a representation that is based primarily on the depth of facial features. As with skeletal tracking data, Kinect recognizes facial features as numerical data, not as a photograph of the individual.

- Some Kinect-enabled games can take snapshots or videos of gamers and make them available for download, copying or sharing through, KinectShare.com or through a game publisher. There is a specific setting that controls whether those photographs and videos can be shared with others outside of Xbox LIVE. It is called Kinect Sharing, and it is a privacy setting found within the console. Kinect Sharing has two settings: “Blocked” and “Allowed.” For children under the age of 13, the default setting is “Blocked.” For everyone else is the default setting is “Allowed.” The setting can be changed by whomever has permission.

Finally, as an additional step to ensure a safe and private gaming experience, Microsoft publishes a set of Technical Certification Requirements (TCRs) that all game publishers must comply with before they can market a game for the Xbox console. Kinect enabled games must meet not only the same requirements as other Xbox games, but also Kinect-specific TCRs with guidelines for topics such as taking pictures and videos during games, and how and when these can be used, provided the user has given consent.[3]

[3] For more information about the way in which Kinect protects user privacy and online safety see "Privacy and Online Safety Guidance for Kinect," which can be found at: http://xbox.com/kinectprivacy .

Conclusion

Microsoft is dedicated to making data protection an integral part of our product and service lifecycle—from design and development to deployment and operation. The end results of this effort are technologies that enable individuals to more safely and confidently share their information online and that allow organizations to more securely manage personal data.

We are also committed to sharing our privacy knowledge and best practices with the broader technology industry and privacy community. Thus, in addition to making our "Security Development Lifecycle"[4] (a methodology for incorporating security analysis and related considerations into software development) and our "Privacy Guidelines for Developing Software Products and Services"[5] publicly available, we have published a whitepaper series entitled, "A Guide to Data Governance for Privacy, Confidentiality, and Compliance."[6] This whitepaper series is intended to help IT managers, security and privacy officers, and risk management professionals manage challenges associated with information security and privacy.

We seek to create a more trustworthy computing environment by working closely with the IT industry, government leaders, policymakers, privacy advocates, and our customers. We believe that strong data protection and privacy capabilities are crucial to building trust in software products and Internet services so users can realize the full benefits of these innovative technologies.

[4] www.microsoft.com/sdl
[5] http://go.microsoft.com/?linkid=9746120
[6] www.microsoft.com/datagovernance