

Trustworthy Computing

Windows 7: Enhancing Privacy and Customer Control

October 2009

Commitment to Privacy

Windows 7 was developed using *Microsoft's Security Development Lifecycle (SDL)*. A Microsoft-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in Microsoft software and culture by introducing security and privacy early and throughout the development process. The SDL mandates that software should include 1) *privacy by design* – provide notice and consent, enable customer policy and control, minimize data collected and reduce data sensitivity, protect the storage and transfer of data; 2) *privacy by default* – software should come pre-set with conservative default settings; and 3) *privacy in deployment* – tools and guidance accompany the software to enable users and administrators to protect the privacy of their customers. Details regarding the SDL can be found at <http://www.microsoft.com/sdl>.

Privacy in Windows 7

Windows 7 includes a number of features that help customers protect their privacy, as well as understand the privacy implications of choices they make. For example:

- *Windows 7 Layered Privacy Statement* (screen shot below), which helps customers understand the choices they make in Windows 7 about their privacy. To make it easier to read, the Windows 7 privacy statement contains three layers: 1) a **highlights layer** that explains at a high level what privacy choices Windows 7 customers have; 2) a **middle layer** that explains the collection and use of customer information; and 3) a **supplement** that contains detailed information about the privacy aspects of Windows 7 features.



- *Internet Explorer 8* gives customers new controls over their data and privacy. Innovations include:
 - An improved *Delete Browsing History* feature, which customers can use to delete their entire browsing history as before, but now they can also choose to retain cookies and temporary Internet files for trusted sites they select (e.g., a cookie that stores a username for a favorite website).
 - *InPrivate™ Filtering*, a new feature, which gives customers greater choice and control over whether third parties providers of content to websites are able to track and aggregate the customers' Web browsing activities. This feature helps customers control third-party content such as maps, advertisements, web beacons, and similar web measurement tools.
 - *InPrivate™ Browsing*, a new feature, which allows customers to prevent their browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being stored or retained by the browser.
 - *SmartScreen Filter* (screen shot below), which helps to warn customers about unsafe websites that are impersonating trusted websites (phishing) or contain threats to their computers (malware).



Security-Related Features that Enhance Privacy

Security is a critical aspect of privacy as well. Security innovations in Windows 7 that can help customers protect their privacy include:

- *BitLocker-to-Go*, which extends encryption protection to data saved on removable storage devices, helping to ensure that only authorized customers can read data stored on portable media (e.g., USB flash drives), even if the media are lost or stolen. Windows 7 also include *BitLocker Drive Encryption*, which provides full-volume encryption (i.e., encryption of user and system files) to safeguard data on a PC that is lost, stolen, or decommissioned.
- *Rights Management Services Client*, which helps safeguard digital information from unauthorized use. Customers can define how recipients use the information contained in a file, such as who can open, modify, print, or take other actions with the file.
- *Windows Defender*, which helps block, control, and remove spyware and other potentially unwanted software that can steal customers' personal information.