Privacy Information for Installation Features

Windows 7 Privacy Statement for Installation Features

Microsoft is committed to protecting your privacy, while delivering software that brings you the performance, power, and convenience you desire in your personal computing. This privacy statement explains data collection and use practices of some privacy-impacting features you can make decisions about while installing and setting up Windows 7 ("Installation Features"): Activation, Device Information Retrieval, Microsoft Error Reporting Service, SmartScreen Filter, Update Services, Windows Customer Experience Improvement Program, Windows Defender, and Windows Help.

With your consent, these features might send information to and from the Internet when you're installing and setting up Windows 7. This disclosure focuses on Windows 7 setup and installation features that communicate with the Internet. It does not apply to other online or offline Microsoft sites, products, or services.

Administrators can use Group Policy to modify many of the settings for the features described below. For more information about data collection and use practices of Windows 7 and how administrators can control these settings, see the white paper at:

http://go.microsoft.com/fwlink/?LinkId=148050

You are seeing this privacy statement because you might not have Internet access during Windows 7 installation. For a more comprehensive privacy statement for this software, see the online Windows 7 Privacy Statement at:

http://go.microsoft.com/fwlink/?LinkId=104288

Collection and use of your information

The personal information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to enable the features you use and provide the services or carry out the transactions you have requested or authorized. The information may also be used to analyze and improve Microsoft products and services.

Except as described in this statement, personal information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as performing statistical analysis. We will only provide those companies the personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Microsoft may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the software; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers, or the public.

Information collected by or sent to Microsoft by Windows 7 may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union.

Collection and use of information about your computer

When you use software with Internet-enabled features, information about your computer ("standard computer information") is sent to the websites you visit and online services you use. Standard computer information typically includes information, such as your IP address,

operating system version, browser version, and regional and language settings. In some cases, it may also include hardware ID, which indicates the device manufacturer, device name, and version. If a particular feature or service sends information to Microsoft, standard computer information will be sent as well.

The privacy details for each Windows 7 installation feature, software or service in the supplemental privacy information listed below describe what additional information is collected and how it is used.

Security of your information

Microsoft is committed to helping protect the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. For example, we store the information you provide on computer systems with limited access, which are located in controlled facilities. When we transmit highly confidential information (such as a credit card number or password) over the Internet, we protect it through the use of encryption, such as the Secure Socket Layer (SSL) protocol.

For more information

Microsoft welcomes your comments regarding this privacy statement. If you have questions about this privacy statement or believe that we have not adhered to it, please contact us by submitting your questions online to Privacy Feedback at:

http://go.microsoft.com/?LinkId=9634754

Windows 7 Privacy Statement for Installation Features
c/o Microsoft Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Installation Features

Activation

What this feature does

Activation helps reduce software counterfeiting, which helps ensure that Microsoft customers receive the software quality they expect. Once your software is activated, a specific product key becomes associated with the computer (the hardware) on which your software is installed. This association prevents the product key from being used to activate the same copy of the software on multiple computers. Some changes to your computer components or the software might require you to reactivate the software.

Information collected, processed, or transmitted

During activation, product key information is sent to Microsoft, such as:

* The Microsoft product code, which is a five-digit code that identifies the Windows 7 product you are activating.
* A channel ID or site code, which identifies where you obtained the Windows 7 product. For example, it identifies whether the product was sold at retail, is an evaluation copy, is subject to a volume licensing program, was pre-installed by the computer manufacturer, and so on.
* The date of installation.
* Information that helps confirm that the product key information has not been altered.

If you license Windows 7 on a subscription basis, information will also be sent about how your subscription works.

Activation also sends to Microsoft a number generated from the computer's hardware configuration. The number does not represent any personal information or information about the software. It cannot be used to determine the make or model of the computer and it cannot be calculated to determine any additional information about your computer. Along with standard computer information, some additional language settings are collected.

Use of information

Microsoft uses the information to confirm that you have a licensed copy of the software and to confirm whether you are eligible for certain support programs. It is also collected for statistical analysis. Microsoft does not use the information to identify you or contact you.

Choice and control

Activation is mandatory and must be completed within a predefined grace period. If you choose not to activate the software, you cannot use it after the grace period expires. If you do not have a valid license for the software, you will not be able to activate it.

Device Information Retrieval

What this feature does

Device Information Retrieval downloads information from Microsoft about your hardware devices, such as manufacturer, description, and a picture of the device, and then displays it to you.

Information collected, processed, or transmitted

In order to retrieve relevant device information, this feature sends data to Microsoft, including your Device ID (for example, Hardware ID or Model ID of the device you are using), your locale, and the date that device information was last updated. The device information downloaded to your computer might include model name, description, device manufacturer logo, and device-related tasks.

Use of information

The information collected is used to help download relevant device information. No information sent is used to identify or contact you.

Choice and control

If you choose the recommended settings during Windows 7 setup, you turn on Device Information Retrieval. You can turn this feature off by going to Devices and Printers in Control Panel, right-clicking the computer icon, and then clicking **Device installation settings**. Select “No, let me choose what to do,” and then clear the “Replace generic device icons with enhanced icons” check box.

Microsoft Error Reporting Service

What this feature does

The Microsoft Error Reporting Service helps Microsoft and Microsoft partners diagnose problems in the software you use and provide solutions. Not all problems have solutions, but when solutions are available, they are offered as steps to solve a problem you’ve reported or as updates to install. To help prevent problems and make software more reliable, some solutions are also included in service packs and future versions of the software.

The Microsoft Error Reporting Service also provides Setup Repair, an error reporting service that may run during Windows setup if a problem occurs.

Information collected, processed, or transmitted

Many Microsoft software programs, including Windows 7, are designed to work with the reporting service. If a problem occurs in one of these software programs, you might be asked

if you want to report it. If you host virtual machines using a Windows operating system, reports generated by the Windows operating system for the Microsoft Error Reporting Service might include information about virtual machines.

The reporting service collects information that is useful for diagnosing and solving the problem that has occurred, such as:

* Where the problem happened in the software or hardware
* The type or severity of the problem
* Files that help describe the problem
* Basic software and hardware information
* Possible software performance and compatibility problems

These reports might unintentionally contain personal information. For example, a report that contains a snapshot of computer memory might include your name, part of a document you were working on, or data that you recently submitted to a website.

If a report is likely to contain this type of information, Windows will ask if you want to send this information, even if you have enabled automatic reporting through the “Recommended settings” option in setup, or Control Panel. This gives you the opportunity to review the report before sending it to Microsoft. Reports including files and data might be stored on your computer until you have an opportunity to review and send them, or after they have been sent.

If an error report contains personal information, Microsoft does not use the information to identify you or contact you. In addition, if you enable automatic reporting through the "Recommended settings" option in setup, or in Control Panel, the reporting service will send basic information about where problems occur automatically, but these reports will not have the detail described above.

After you send a report, the reporting service might ask you for more information about the error you experienced. If you choose to provide your phone number or e-mail address in this information, your error report will be personally identifiable. Microsoft might contact you to request additional information to help solve the problem you reported.

The Microsoft Error Reporting Service generates a globally unique identifier (GUID) that is stored on your computer and sent with error reports to uniquely identify your computer. The GUID is a randomly generated number; it does not contain any personal information and is not used to identify you. We use the GUID to distinguish how widespread the feedback we receive is and how to prioritize it. For example, the GUID allows Microsoft to distinguish between one customer experiencing a problem one hundred times and one hundred customers experiencing the same problem once.

Use of information

Microsoft uses information about errors and problems to improve Microsoft products and services as well as third-party software and hardware designed for use with these products and services. Microsoft employees, contractors, vendors, and partners might be provided access to information collected by the reporting services. However, they will use the information only to repair or improve Microsoft products and services and third-party software and hardware designed for use with Microsoft products and services.

Microsoft might share aggregate information about errors and problems. Microsoft uses aggregate information for statistical analysis. Aggregate information does not contain specific information from individual reports, nor does it include any personal or confidential information that might have been collected from a report.

Choice and control

If you choose the recommended settings during Windows 7 setup, basic information about errors will be sent automatically to Microsoft. If a more detailed error report is required, you will be prompted to review it before it is sent. You can change this setting at any time by going to Action Center in Control Panel.

For more information, see the Microsoft Error Reporting Service privacy statement online at:

http://go.microsoft.com/fwlink/?LinkId=50163

SmartScreen Filter

What this feature does

SmartScreen Filter is a feature in Internet Explorer that is designed to help warn you about unsafe websites that impersonate trusted websites (phishing) or contain threats to your computer. If you opt in to SmartScreen Filter, it first checks the address of the website you are visiting against a list of high-traffic website addresses stored on your computer that are believed by Microsoft to be legitimate. Addresses that are not on the local list and the addresses of files you download will be sent to Microsoft and checked against a frequently updated list of websites and downloads that have been reported to Microsoft as unsafe or suspicious. You may also choose to use SmartScreen Filter manually to verify individual sites with Microsoft.

Information collected, processed, or transmitted

When you use SmartScreen Filter to check websites automatically or manually, the address of the website you are visiting will be sent to Microsoft, together with standard computer information and the SmartScreen Filter version number. To help protect your privacy, the information sent to Microsoft is encrypted.

Information that might be associated with the address, such as search terms or data you entered in forms, might be included. For example, if you visited the Microsoft.com search website at http://search.microsoft.com and entered "Seattle" as the search term, a full address such as http://search.microsoft.com/results.aspx?q=Seattle&qsc0=0&SearchBtn0=Search&FORM=QBMH1&l=1 will be sent. Address strings might unintentionally contain personal information, but this information, like the other information sent, is not used to identify, contact, or target advertising to you. In addition, Microsoft filters address strings to try to remove personal information wherever possible.

From time-to-time, information about your usage of SmartScreen Filter will be sent to Microsoft, such as the time and total number of websites browsed since an address was first sent to Microsoft for analysis. Some information about files that you download from the web, such as name and file path, may also be sent to Microsoft. Some website addresses that are sent to Microsoft may be stored along with additional information, including web browser version, operating system version, SmartScreen Filter version, the browser language, and information about whether Internet Explorer Compatibility View was enabled for the website. A unique identifier generated by Internet Explorer is also sent. The unique identifier is a randomly generated number that does not contain any personal information and is not used to identify you. This information, along with the information described above, is only used to analyze performance and improve the quality of our products and services.

You can also use SmartScreen Filter to report websites to Microsoft as unsafe. When you report a website as unsafe, some information will be sent to Microsoft including the address of the site you are reporting and the usage information described above.

Use of information

The information described above will be used to analyze performance and improve the quality of our products and services. Microsoft will not use any information collected to identify, contact or target advertising to you.

Choice and control

If you choose the recommended settings during Windows 7 setup, you turn on automatic website checking with SmartScreen Filter. You can also turn SmartScreen Filter on or off in Internet Explorer.

1. In Internet Explorer, click the **Safety** button, and then click **SmartScreen Filter**.
2. Click **Turn On SmartScreen Filter** or **Turn Off SmartScreen Filter**.

Update Services

What this feature does

Update Services for Windows include Windows Update and Microsoft Update:

* **Windows Update** is a service that provides you with software updates for Windows software and other supporting software, such as drivers supplied by device manufacturers.
* **Microsoft Update** is a service that provides you with software updates for Windows software, as well as other Microsoft software such as Microsoft Office.

The Update Services might periodically show you detailed notifications about new Microsoft software and specific updates that you can install manually. Some updates that are available through these update services can only be obtained by users who have validated that they are running a genuine copy of Windows 7. Genuine Microsoft software validation is covered by a separate privacy statement that you can read at:

http://go.microsoft.com/fwlink/?LinkID=83561

Information collected, processed, or transmitted

The Update Services collect information from your computer that allows us to operate and improve the services, such as:

* The Microsoft software and other supporting software (for example, drivers supplied by device manufacturers) installed on your computer for which the Update Services have updates available. This helps us determine which updates are appropriate for you.
* Your Windows Update and/or Microsoft Update configuration settings, such as whether you want updates automatically downloaded or installed.
* The successes, failures, and errors you experience when accessing and using the Update Services.
* Plug and Play ID numbers of hardware devices – a code assigned by the device manufacturer that identifies the device (for example, a particular type of keyboard).
* Globally Unique Identifier (GUID) – a randomly generated number that does not contain any personal information. GUIDs are used to identify individual machines without identifying the user.
* BIOS name, revision number, and revision date – information about the set of essential software routines that test your hardware, start the operating system on your computer, and transfer data among hardware devices connected to your computer.
* Product ID – the unique product license identifier that is included with every Microsoft product.
* Product Key – the string of numbers and characters that comes with every Microsoft product, typically entered by you during setup to successfully install a product.

You can use these Update Services by going to Windows Update in Control Panel and checking for updates or changing your settings to allow Windows to automatically install

updates as they become available (recommended). Within the Windows Update feature, you can choose whether to opt in for Microsoft Update.

Use of information

The data sent to Microsoft is used to operate and maintain the Update Services. It is also used to generate aggregate statistics that help us analyze trends and improve our products and services, including the Update Services.

To generate aggregate statistics, the Update Services use the GUID collected by the Update Services to track and record the number of individual computers that use the Update Services and whether the download and installation of specific updates succeeds or fails. The Update Services record the GUID of the computer that attempted the download and installation, the ID of the item that was requested, whether updates were available, and standard computer information.

Required Updates

If you turn on the Update Services, in order for them to properly function some software components on your system that make up or are directly related to the Update Services will need to be updated from time to time. These updates must be performed before the service can check for, download, or install other updates. These required updates fix errors, provide ongoing improvements, and maintain compatibility with the Microsoft servers that support the service. If the Update Services are turned off, you will not receive these updates.

Cookies/Tokens

A token is similar to a cookie. It stores information in a small file that is placed on your hard disk by the Update Services server, and is used when your computer connects to the Update Services server to maintain a valid connection. It is stored on your computer only, not on the server. This cookie/token contains information (such as last scan time) in order to find the most recently available updates. It contains information to manage what content should be downloaded to your computer, when that should happen, as well as a GUID to identify your computer to the server.

Information contained in the contents of the cookie/token is encrypted by the server (with the exception of the cookie/token expiration time). This cookie/token is not a browser cookie so it cannot be controlled with your browser settings. The cookie/token cannot be removed; however, if you do not use the Update Services, the cookie/token will not be used.

About surveys

Occasionally you might be invited to participate in a survey about the way you use the Windows Update or Microsoft Update Services. Each survey includes a privacy statement that details the way Microsoft will use the information submitted with that survey.

Choice and control

Update Services are turned on if you choose one of the following settings: (i) Install updates automatically; (ii) Download updates but let me choose whether to install them; or (iii) Check for updates but let me choose whether to download and install them. Windows Update service is turned on and set to "Install updates automatically" when you choose the recommended option during Windows setup.

If you turn on the Update Services, regardless of which setting you have chosen, required updates to some components of the service will be downloaded and installed automatically without further notice to you. If you would prefer not to receive required updates, turn off the Update Services.

You can also choose whether to check for or automatically install Important and Recommended updates for your computer or Important updates only. Optional or Featured updates are never installed automatically. To change your Update Services settings after

Windows setup, click **Start**, click **All Programs**, click **Windows Update**, and then click **Change settings**. To turn off the Update Services (including required updates), select **Never check for updates**.

Windows Customer Experience Improvement Program (CEIP)

What this feature does

If you choose to participate in Windows CEIP, Microsoft collects basic information about how you use your programs, your computer, connected devices, and Windows 7. We also collect information about how each is set up and performing. When you participate, CEIP will also periodically download a file to collect information about problems you might have with Windows. CEIP reports are sent to Microsoft to help improve the features our customers use most often and to create solutions to common problems. Microsoft does not use any collected information to identify you or contact you.

Information collected, processed, or transmitted

CEIP reports generally include information about:

* **Configuration**, such as how many processors are in your computer, the number of network connections in use, screen resolutions for display devices, and which version of Windows is running. Reports can also include configuration information, such as the strength of the signal between your computer and a wireless or Bluetooth enabled device, and if some features such as high-speed USB connections are turned on.
* **Performance and reliability**, such as how quickly a program responds when you click a button, how many problems you experience with a program or a device, and how quickly information is sent or received over a network connection.
* **Program use**, such as the features that you use most often, how frequently you open programs, how often you use Windows Help and Support, and how many folders you typically create on your desktop.

CEIP reports also contain information about events (event log data) on your computer from up to seven days prior to the time you decide to participate in CEIP. Since most users decide to participate in CEIP within several days of setting up Windows, Microsoft uses this information to analyze and improve the Windows 7 setup experience.

This information is sent to Microsoft when you are connected to the Internet. CEIP reports do not intentionally contain contact information, such as your name, address, or phone number; however, some reports might unintentionally contain individual identifiers, such as a serial number for a device that is connected to your computer. Microsoft filters the information contained in CEIP reports to try to remove any individual identifiers that they might contain. To the extent that individual identifiers are received, Microsoft does not use them to identify you or contact you.

CEIP generates a globally unique identifier (GUID) that is stored on your computer and sent with CEIP reports to uniquely identify your computer. The GUID is a randomly generated number; it does not contain any personal information and is not used to identify you.

CEIP will also periodically download a file to collect information about problems you might have with Windows. This file allows Windows to collect additional information to help create solutions for common problems.

Use of information

Microsoft uses CEIP information to improve our software. We might also share CEIP information with Microsoft partners so they can improve their software, but the information cannot be used to identify you. We use the GUID to distinguish how widespread the feedback we receive is and how to prioritize it. For example, the GUID allows Microsoft to distinguish between one customer experiencing a problem one hundred times and one hundred

customers experiencing the same problem once. Microsoft does not use the information collected by CEIP to identify you or contact you.

Choice and control

If you choose the recommended settings during Windows 7 setup, you turn on Windows CEIP. If you choose to participate, CEIP will collect the information described above for all users on your computer. Administrators can turn CEIP on or off by going to Action Center in Control Panel, clicking **Change Action Center settings**, and then clicking **Customer Experience Improvement Program settings**.

For more information, see these frequently asked questions about the Microsoft Customer Experience Improvement Program online at:

http://go.microsoft.com/fwlink/?LinkID=52095

Windows Defender

What this feature does

Windows Defender looks for malware and other potentially unwanted software on your computer. It offers two ways to help keep malware and other potentially unwanted software from infecting your computer:

* **Real-time protection**. Windows Defender alerts you when malware or potentially unwanted software attempts to install or run on your computer. It also alerts you when programs attempt to change important Windows settings.
* **Scanning options**. You can use Windows Defender to scan for malware and other potentially unwanted software that might be installed on your computer, to schedule scans on a regular basis, and to automatically remove any malicious software that is detected during a scan.

If you choose the recommended settings during Windows 7 setup, you turn on Windows Defender real-time protection and automatic scanning. Windows Defender will automatically download and install updated definitions before scanning, and then remove software that causes a severe or high alert level detected during the scan. You can change this setting at any time by using the options provided in Windows Defender.

Windows Defender – Microsoft SpyNet Feature

What this feature does

The Microsoft SpyNet anti-malware community is a voluntary, worldwide community of Windows Defender users. Through Microsoft SpyNet, users can report malware and other forms of potentially unwanted software to Microsoft. When you set up Windows 7, you can choose to join Microsoft SpyNet. If you choose to join, reports about malware and potentially unwanted software are sent to Microsoft. The type of information that is sent in reports depends on your level of Microsoft SpyNet membership.

Information collected, processed, or transmitted

Microsoft SpyNet reports include information about the files or programs in question, such as file names, cryptographic hashes, vendors, sizes, and date stamps. In addition, Microsoft SpyNet might collect full URLs to indicate the origin of the file, which might occasionally contain personal information such as search terms or data entered in forms. Reports might also include the actions that you applied when Windows Defender notified you that software was detected. Microsoft SpyNet reports include this information to help Microsoft gauge the effectiveness of Windows Defender’s ability to detect and remove malicious and potentially unwanted software.

Reports are automatically sent to Microsoft when:

* Windows Defender detects software or changes to your computer by software that has not yet been analyzed for risks.
* You apply actions to software that Windows Defender has detected.
* Windows Defender completes a scheduled scan and automatically applies actions to software that it detects, according to your settings.

SpyNet might unintentionally collect personal information. To the extent that SpyNet collects any personal information, Microsoft does not use the information to identify you or contact you.

You can join Microsoft SpyNet with a basic or an advanced membership. If you choose the recommended settings during Windows setup, you join with a basic membership. Basic member reports contain the information described above. Advanced member reports are more comprehensive and might occasionally contain personal information from, for example, file paths and partial memory dumps. These reports, along with reports from other Windows Defender users who are participating in Microsoft SpyNet, help our researchers discover new threats more rapidly. Malware definitions are then created for programs that meet the analysis criteria, and the updated definitions are made available to all users through Windows Update.

If you join Microsoft SpyNet with a basic or an advanced membership, Microsoft might request a Sample Submission report. This report contains specific files from your computer that Microsoft suspects might be potentially unwanted software. The report is used for further analysis. You will be asked each time if you want to send this Sample Submission report to Microsoft.

To help protect your privacy, reports that are sent to Microsoft are in encrypted form.

Use of information

Microsoft SpyNet reports are used to improve Microsoft software and services. The reports might also be used for statistical or other testing or analytical purposes, and for generating definitions. Only Microsoft employees, contractors, partners and vendors who have a business need to use the reports are provided access to them.

Choice and control

If you choose the recommended settings, you will join Microsoft SpyNet with a basic membership. You can join or leave Microsoft SpyNet or change your membership level at any time. You can turn automatic scanning on or off and change the frequency and type of scans. You can also choose which actions are automatically applied to software that Windows Defender detects during a scheduled scan.

You can change your Microsoft SpyNet membership or settings by using the Tools menu in Windows Defender.

Windows Defender – History Feature

What this feature does

This feature provides a list of all programs on your computer that Windows Defender detects and the actions that were taken when the programs were detected.

In addition, you can view a list of programs that Windows Defender does not monitor while they are running on your computer (Allowed items). You can also view programs that Windows Defender prevents from running until you choose to remove them or allow them to run again (Quarantined items).

Information collected, processed, or transmitted

The list of software that Windows Defender detects, the actions that you and other users

take, and the actions that Windows Defender takes automatically are stored on your computer. All users can view the history in Windows Defender to see malware and other potentially unwanted software that has attempted to install itself or run on the computer, or that has been allowed to run by another user. For example, if you learn about a new malware threat, you can check the history to see if Windows Defender has prevented it from infecting your computer. The History Feature does not send data to Microsoft.

Choice and control

History lists can be deleted by an administrator.

Windows Help – Windows Online Help and Support

What this feature does

Windows Online Help and Support, when turned on, allows you to search for online help content when you're connected to the Internet, giving you the most up to date content available.

Information collected, processed or transmitted

When you use Windows Online Help and Support, your search queries are sent to Microsoft, as well as any rating or feedback you choose to provide about the help topics presented to you. Windows Online Help and Support does not intentionally collect any information that could be used to personally identify you. If you type such information into the search or feedback boxes, the information will be sent, but Microsoft does not use the information to identify you or contact you.

Use of information

Microsoft uses the information to return help topics in response to your search queries, to return the most relevant results, to develop new content, and to improve existing content.

Choice and control

If you choose the recommended settings during Windows 7 setup, you turn on Windows Online Help and Support. If you do not choose recommended settings you are given the opportunity to select Windows Online Help and Support the first time that you use Windows Help and Support. To change your selection later, open Windows Help and Support, click the **Options** menu, and then click **Settings**; or select **Get online Help** from the menu at the bottom of the Help window.

Windows Help – Help Experience Improvement Program

What this feature does

The Help Experience Improvement Program helps Microsoft identify trends in the way our customers use Help so that we can improve our search results and the relevancy of our content. You may only participate in the Help Experience Improvement Program if you also choose to opt in to use Windows Online Help and Support.

Information collected, processed or transmitted

The Help Experience Improvement Program sends Microsoft information about the version of Windows that your computer is running and about how you use Windows Help and Support, including queries you enter when you search Windows Help and Support.

The Help Experience Improvement Program generates a globally unique identifier (GUID) that is stored on your computer and sent to Microsoft with the information described above to uniquely identify your computer. The GUID is a randomly generated number; it does not contain any personal information and is not used to identify you. The GUID is separate from the GUIDs created for the Microsoft Error Reporting Service and the Windows Customer Experience Improvement Program. We use the GUID to distinguish how widespread the

issues we receive are and how to prioritize them. For example, the GUID allows Microsoft to distinguish between one customer experiencing an issue one hundred times and one hundred customers experiencing the same issue once.

Use of information

The data collected is used to identify trends and usage patterns so that Microsoft can improve the quality of content we provide and the relevance of our search results. Microsoft does not use the information to contact you or identify you.

Choice and control

If you choose the recommended settings during Windows 7 setup, you enroll in the Help Experience Improvement Program. You can change your participation settings by opening Windows Help and Support, clicking the **Options** menu, and then clicking **Settings**; or selecting **Get online Help** from the menu at the bottom of the Help window. Note that selecting Get online help from this menu doesn’t automatically enroll you in the Help Experience Improvement Program; you must enroll through the Settings option. If you are not enrolled, you will also be given an opportunity to join after submitting feedback.