## Anti-Virus Comparative


# Data transmission in Internet security products

Language: English
January 2014

Last Revision: 20th May 2014

*Commissioned by PCgo and PC Magazin Germany*

**www.av-comparatives.org**

## Management summary

Many Internet users are concerned about who has access to their personal information and what is done with it. After revelations by Edward Snowden regarding the extent of eavesdropping by the US-American NSA, users have become increasingly aware of privacy issues. Computer security software has legitimate grounds for sending its makers some information about the system it's running on; in particular, details of malware found on the machine have to be sent to the manufacturer in order to protect the user effectively. however, this does not mean that a program should have carte blanche to send any and all personal information found on a computer to the manufacturer (other than with the specific knowledge and agreement of the system's owner). This report gives some insight into data-sending by popular security programs.

Clearly, antivirus manufacturers have to comply with the laws of the countries in which they are established. In the event of e.g. a court order requiring the vendor to provide information about a customer, the company has no choice but to do this. However, this should be the only reason for providing user data to a third party. Some companies do not state that they will only pass on customer information in such circumstances.

This report was initially requested and commissioned by PCgo and PC Magazin Germany.

## How was the data collected?

The network traffic from a test machine running each of the products was collected and analysed. In some cases, this was encrypted, and so we were unable to read it. In general, it is much better if any data sent is encrypted first, to prevent it being intercepted and read in transmission.

We also looked at the End User License Agreement (EULA) and privacy statements of each product (***as at January 2014***), as these should state clearly which data may be sent to the respective manufacturer. Inevitably a number of things are dependent on the personal interpretation of the reader, and so our comments on AV-vendors' privacy statements are based on our own interpretation of them.

Finally, we sent each manufacturer a detailed questionnaire to fill out, requesting details of the data sent by their Internet security product versions. In some cases, the vendors chose not to disclose certain information. Reasons given for this included the need to keep the technology secret, and lack of knowledge of third-party components which have been integrated into the product (e.g. third-party antivirus engines).

We gave higher weighting to our own measurements and the EULA (as we understand it) than to the replies to our questionnaire. We cannot take any responsibility for the correctness of the data provided here.

We understand that too much openness and transparency might be useful for criminals, who could thus find out how to bypass some features of the security products. We thus accept that vendors cannot provide us with any information which could compromise security.

| | South Korea | Czech | Czech | Germany | Romania | UK | Austria | India | Slovakia | USA | Finland |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | **AhnLab** | **Avast** | **AVG** | **AVIRA** | **Bitdefender** | **BullGuard** | **Emsisoft** | **eScan** | **ESET** | **Fortinet** | **F-Secure** |
| **Product information** | | | | | | | | | | | |
| Is the product version and license information transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| Is a unique idenfication number transmitted? | YES | YES | YES | YES | YES | YES | YES | NO | YES | NO | YES |
| Are statistics for product usage transmitted? | NO | NO | YES | NO | YES | NO | YES | NO | YES | NO | YES |
| **Machine information** | | | | | | | | | | | |
| Is the version of the operating system transmitted? | YES | YES | YES | YES | YES | NO | NO | NO | YES | YES | YES |
| Is the Computername transmitted? | NO | YES | YES | NO | YES | YES | YES | NO | not disclosed | NO | YES |
| Is information (e.g. version numbers, etc.) about third party applications transmitted? | NO | YES | YES | NO | NO | NO | NO | NO | not disclosed | NO | YES |
| Is information about the hardware (RAM, CPU, ...) transmitted? | NO | YES | NO | NO | YES | NO | NO | NO | not disclosed | NO | YES |
| Is information about running processes transitted? | NO | NO | YES | NO | YES | NO | NO | NO | not disclosed | NO | NO |
| Is the local IP address transmitted? | NO | YES | NO | NO | NO | NO | NO | NO | NO | NO | NO |
| Are event- or errorlogs of the operating system transmitted? | NO | YES | NO | NO | NO | NO | NO | NO | not disclosed | NO | NO |
| Is the display resolution transmitted? | NO | YES | YES | NO | NO | NO | NO | NO | not disclosed | NO | NO |
| **Personal information** | | | | | | | | | | | |
| Are visited URLs (malicious and non-malicious URLs) transmitted? | NO | YES | YES | YES | YES | YES | NO | YES | YES | YES | YES |
| Is the Referer (previous page with link to malware-hosting site) transmitted? | NO | YES | NO | NO | NO | NO | NO | NO | not disclosed | NO | YES |
| Is the country / region of the settings of the operating system transmitted? | NO | YES | YES | YES | YES | NO | NO | NO | not disclosed | NO | NO |
| Is the language of the operating system transmitted? | NO | YES | YES | YES | NO | NO | NO | NO | YES | NO | YES |
| Is the windows username transmitted? | NO | NO | YES | NO | YES | NO | NO | NO | not disclosed | NO | NO |
| **File related information (clean and malicious)** | | | | | | | | | | | |
| Are hashes of files (or hashes of parts of files) transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | YES | NO | YES |
| Is the detection name (of malware detections) transmitted? | NO | YES | YES | NO | YES | YES | YES | NO | YES | YES | YES |
| Is the name and path of files transmitted? | NO | YES | YES | YES | YES | YES | YES | NO | YES | NO | YES |
| If "suspicious" files are transmitted: Are executable files transmitted? | NO | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| If "suspicious" files are transmitted: Are non-executable files (e.g. documents) transmitted? | NO | YES | not disclosed | NO | NO | NO | NO | NO | not disclosed | YES | NO |
| Can user opt out of sending files? | N/A | YES | NO | YES | NO | NO | YES | YES | YES | YES | YES |
| When potential malware collects and sends user data, is a sample of the collected data transmitted? | NO | NO | not disclosed | NO | NO | NO | NO | NO | not disclosed | NO | NO |
| **General** | | | | | | | | | | | |
| Do you make use of silent detections (e.g. for FP mitigation of new algorithms)? | YES | YES | not disclosed | YES | YES | NO | NO | NO | not disclosed | YES | YES |
| Are special updates delivered to users with specific IDs? | NO | NO | not disclosed | NO | NO | NO | NO | NO | not disclosed | NO | NO |
| In which jurisdiction is the data stored (EU, USA, worldwide/random, etc)? | South Korea | EU | not disclosed | EU | EU | EU | EU | not disclosed | EU | USA | EU |

| | Germany | Russia | USA | USA | Spain | UK | USA | USA | USA | USA |
|---|---|---|---|---|---|---|---|---|---|---|
| | **G DATA** | **Kaspersky Lab** | **McAfee** | **Microsoft** | **Panda** | **Sophos** | **Symantec** | **Trend Micro** | **Vipre** | **Webroot** |
| **Product information** | | | | | | | | | | |
| Is the product version and license information transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| Is a unique idenfication number transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| Are statistics for product usage transmitted? | NO | YES | YES | YES | NO | NO | YES | YES | YES | YES |
| **Machine information** | | | | | | | | | | |
| Is the version of the operating system transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| Is the Computername transmitted? | not disclosed | YES | not disclosed | YES | NO | not disclosed | YES | YES | YES | YES |
| Is information (e.g. version numbers, etc.) about third party applications transmitted? | YES | YES | YES | YES | NO | not disclosed | YES | not disclosed | YES | YES |
| Is information about the hardware (RAM, CPU, ...) transmitted? | not disclosed | YES | YES | YES | YES | not disclosed | YES | not disclosed | NO | not disclosed |
| Is information about running processes transitted? | YES | YES | not disclosed | NO | NO | not disclosed | YES | not disclosed | NO | YES |
| Is the local IP address transmitted? | NO | NO | YES | YES | NO | NO | NO | YES | YES | YES |
| Are event- or errorlogs of the operating system transmitted? | not disclosed | YES | not disclosed | YES | NO | not disclosed | YES | not disclosed | NO | YES |
| Is the display resolution transmitted? | NO | NO | not disclosed | YES | NO | not disclosed | NO | not disclosed | YES | not disclosed |
| **Personal information** | | | | | | | | | | |
| Are visited URLs (malicious and non-malicious URLs) transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | NO | YES |
| Is the Referer (previous page with link to malware-hosting site) transmitted? | NO | YES | YES | YES | NO | not disclosed | YES | not disclosed | NO | YES |
| Is the country / region of the settings of the operating system transmitted? | YES | NO | YES | YES | YES | NO | YES | YES | YES | YES |
| Is the language of the operating system transmitted? | YES | NO | YES | YES | NO | NO | YES | YES | YES | YES |
| Is the windows username transmitted? | NO | YES | YES | YES | NO | NO | YES* | YES | YES | YES |
| **File related information (clean and malicious)** | | | | | | | | | | |
| Are hashes of files (or hashes of parts of files) transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| Is the detection name (of malware detections) transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| Is the name and path of files transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| If "suspicious" files are transmitted: Are executable files transmitted? | YES | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| If "suspicious" files are transmitted: Are non-executable files (e.g. documents) transmitted? | NO | YES | not disclosed | not disclosed | NO | not disclosed | YES* | not disclosed | YES | not disclosed |
| Can user opt out of sending files? | YES | YES | NO | YES | YES | YES | YES | NO | YES | NO |
| When potential malware collects and sends user data, is a sample of the collected data transmitted? | not disclosed | NO | not disclosed | not disclosed | NO | not disclosed | YES* | not disclosed | NO | not disclosed |
| **General** | | | | | | | | | | |
| Do you make use of silent detections (e.g. for FP mitigation of new algorithms)? | not disclosed | YES | YES | YES | YES | not disclosed | YES | not disclosed | NO | YES |
| Are special updates delivered to users with specific IDs? | not disclosed | NO | not disclosed | not disclosed | NO | not disclosed | NO | not disclosed | NO | not disclosed |
| In which jurisdiction is the data stored (EU, USA, worldwide/random, etc)? | EU | Russia | USA | Safe Harbor | EU | EU | USA | USA | USA | USA |

** Symantec claim that they do not directly collect such data and do not intent to collect such data, but such data may be inadvertently sent to them. The last point is included in the EULA, presumably to be on the safe side legally. Furthermore, after receing the questionnaire, Symantec stated that they will release an update which will mean that the user name will no longer be collected.*

## Product version and license

Amongst manufactures who responded, all send the product version and license information. Sending the product version is obviously essential if it is to be updated to the latest version, which is of course recommended. Clearly license information also needs to be transmitted if there is to be any sense in having a license for a product. About half the vendors transmit product usage data; this could be very useful in improving the product, and so has a legitimate purpose. Almost all products send a unique identifying number (UID), which could fairly be used for licensing purposes; if one individual license is seen on a number of different PCs (different UIDs) , it could be pirated.

## Machine Information

It seems entirely reasonable that antivirus programs should send their manufacturers technical information about the machine they are running on, so that they can e.g. optimized for different operating systems and hardware specifications, and any conflicts with specific Windows updates/service packs and third-party software can be rectified. Sending product versions of third-party programs can be useful to warn of known vulnerabilities, e.g. for antivirus products that include a software updater. The information could also allow vendors to understand the use of exploits by malware authors. A majority of respondents state that their programs send operating system version, which is entirely legitimate. Sending the workgroup name, local IP address and hostname (computer name) might seem to be an invasion of privacy. Many programs do send the local hostname; the most common reason given for this is that it is necessary for license key mapping, although most of the programs that do this also submit a unique identification number as well. In some cases, it is surprising that relatively few manufacturers send technical data which would appear to be very useful. For example, most programs do not send the IP address of the DNS server used by the system, even though this could be relevant, as malware can attempt to change the computer's DNS configuration. Given that Windows 8 is now being used on screen sizes ranging from 8-inch (tablets) to 29-inch (monitors), it seems strange that very few products inform their makers about the display resolution of the device on which they are installed.

## Personal information

The most personal in the personal information category is the Windows username, which in many cases will be the user's full real name. About half of respondents stated that their products send the Windows username. Some claim that this is necessary for the parental control feature, and the username is only sent if the parental control feature is activated. However, not all of the programs that send the Windows hostname even have a parental control function.

Roughly half the respondents' programs send country, region and language settings. These could be used for a number of legitimate purposes, such as license control, providing the correct interface language, and noting the effect of regional settings on malware-hosting websites.

Sending information on URLs visited makes obvious sense if the product has a URL blocker. Sending details of the referrer (linking website) also seems relevant in blocking malware. IP addresses of web servers is also obviously important. Some vendors state that they remove any personal information such as email addresses and passwords before sending details of a URL, which strikes us as the right thing to do.

## File-related info

Sending information such as detection names, file hashes, names, paths and sizes of potentially malicious executable program files is obviously important in counteracting malware, and almost all respondents' programs do this. What is less easy to justify is sending personal data files (e.g. documents) or non-malicious executable program files. We feel that users should be able to decide on a file-by-file basis whether such files are sent. Several programs allow users to opt out of file-sending either completely or on a case-by-case basis, although a number send files without explicitly asking the user (there may be a warning in the EULA that this will happen).

If malware steals personal data, we do not feel there is justification for the AV program to send the same information to the manufacturer. Some products' EULAs or privacy statements note that the product might transmit such data to the product vendor, though this is for legal reasons, in case the product inadvertently sends personal data along with legitimate information about the malware itself.

## General

Sending of personal information/files should be pointed out/requested during setup. It's not reasonable to expect people to read license agreement in full.

Many products make use of silent detections. This involves sending to the vendor details of files that have triggered a detection, without the user being alerted in any way. This can be done e.g. to check whether the file is genuinely malicious or not.

Most (but not all) manufacturers answered the question as to the jurisdiction in which collected data is stored. In some cases, this is dependent on the country in which the software is first installed.

We asked whether special updates are delivered to users with specific IDs. This could theoretically allow authorities with a suitable court order to monitor e.g. specific terror suspects without the monitoring software being detected by the antivirus product. All updates would however be supplied to all other users, ensuring that their PCs were still fully protected. Most of the vendors responded that they do not do this, although a few (mostly from the USA and UK) did not reply to this question.

Some vendors allow big corporations or organizations to look inside their source code. Considering that a thorough code-review would take very long time and not give much real insight (cases of leaked source codes of AV products exist)[1] and that with every new update (which takes place several times a day) the product and its behaviour could change, the offer serves more to calm down some worried people.

Vendors tell us that the data gathered and transmitted by each product does not go to a single collection centre; rather, specific elements are transmitted separately to different isolated end points, without any connection between them. Thus e.g. licence-management data is sent separately from product-usage statistics. They say that as there is no connection between these systems, the data collected by one cannot be linked with the data collected by another. Consequently the privacy of the user should be safeguarded.

[1] http://www.huffingtonpost.com/2012/01/17/symantec-hack-norton-source-code_n_1211043.html

## Why are people often especially sceptical towards security vendors?

The Chief Research Officer of a major antivirus vendor cancelled his scheduled participation in the 2014 RSA Security Conference, in protest at collaboration by security company RSA with the United States NSA in the form of weakening security in its encryption systems. He stated that "*RSA is hardly the only vendor facing scrutiny. He said that the trustworthiness of U.S.-based security and technology companies is quickly eroding, pointing to a letter recently sent to 20 of the world's largest antivirus companies by Bits of Freedom, a Netherlands-based organization focused on digital rights. In that letter, the group asked whether the vendors had whitelisted government-authored malware. Most of those companies gave a prompt response in the negative, but U.S-based AV giants McAfee Inc. and Symantec Corp. never replied*".[2]

It is possible that intelligence/law-enforcement agencies in some countries prohibit vendors (security or otherwise) from revealing any co-operation with them.

Some people may ask why malware such as Stuxnet and R2D2 remained undetected for many years.[3]

In the past, there have been cases of security vendors removing (or not creating) detection for commercial spyware/keyloggers, due to issues of commercial law. Thus it is not far-fetched to assume that the same would be done for the software of law-enforcement agencies if instructed to do so.

Security vendors have an important duty to protect users' privacy. Equally, users need to trust the security products they use, as it would otherwise be better not to go onto the Internet at all. It is also important to remember that many other products and services also collect data from Internet users.

## Suggestions for users

Various information is transmitted, for a number of good reasons, which could potentially be misused by an unscrupulous vendor. It is thus advisable to install only products from reputable manufacturers, and check that the licence agreement does not permit any questionable practices such as allowing any and all user data to be collected. Users should also avoid being lured into using free products that require submitting personal data (data mining is a business model too, as well as the inclusion of third-party toolbars which collect information on their own).

Users should read the terms before buying/installing a product or signing up for a service ; this is why having the EULA accessible from outside of the programs is useful. This gives users the opportunity to make an informed decision as to whether to opt-out from data-collecting networks/features (e.g. toolbars) or not. In many cases an opt-out is offered, but in some cases this might decrease protection. In other cases (collection of data about malware) it is like vaccination – the more people participate, the more effective the protection for everyone.

---

[2] http://searchsecurity.techtarget.com/news/2240215264/TrustyCon-Hypponen-warns-of-government-malware-loss-of-vendor-trust

[3] http://www.wired.com/2012/06/internet-security-fail

## Wish list

In an ideal world, we would like to see data sending managed as follows:

- Users should be asked each time before a file is sent to the vendor, unless they have explicitly opted out of this by choosing either “always send” or “never send”.
- Users should be able to specify in detail what information is being sent.
- Users should be informed where the collected information is being sent and how long it will be stored.
- The path to files in a user profile can and should be sent as *%userprofile%* to avoid providing the user’s name.
- A single succinct, clear privacy statement should be easy to find on the vendor’s website and within the product itself.
- We would like to see vendors providing users with a short, clear explanation of which data is collected. This should be written in normal everyday language, not in legal jargon that only lawyers or technical specialists can understand.
- It should be possible to genuinely opt out of data sending without losing or compromising protection or usability.
- Security products should not include third-party toolbars or other add-ons that collect data separately from the AV vendor. We would find such add-ins especially inappropriate in paid-for products.
- Vendors claim that any data which could personally identify the user is anonymised after collection; we feel that it would be better to anonymise the data before sending.

## Links to terms and conditions, EULAs and privacy statements of the products

Below is a list of links to some terms and conditions, EULAs and/or privacy statements of various vendors. We advise users to take the time to read them. Most of the documents consist of about 1,000 to about 20,000 words. Some of them seem to do not have been updated for over 10 years.

Some few vendors currently do not provide this type of document on their website, but show them during or after the installation of their products.

**AhnLab**
https://global.ahnlab.com/en/site/etc/termsOfUse.do
http://global.ahnlab.com/en/site/etc/privacyPolicy.do

**Avast**
http://www.avast.com/privacy-policy

**AVG**
http://www.avg.com/eu-en/policies

**AVIRA**
https://www.avira.com/en/general-privacy

**Bitdefender**
http://www.bitdefender.com/site/view/legal_terms.html

**BullGuard**
http://www.bullguard.com/about/eula/is/en.aspx

**Emsisoft**
http://www.emsisoft.com/en/software/privacy/

**eScan**
http://escanav.com/english/content/company/privacy_policy/escan_privacy_policy.asp
http://www.escanav.com/english/escan_windows_eula/eula.html

**ESET**
http://www.eset.com/us/software-eula/

**Fortinet**
http://docs.forticare.com/eula/EULA.pdf

**F-Secure**
http://www.f-secure.com/en/web/home_global/rtpn-privacy-policy
http://www.f-secure.com/en/web/home_global/personal-data-policy
http://www.f-secure.com/en/web/home_global/license-terms

**Kaspersky Lab**
http://www.kaspersky.com/downloads/documentation/End-User-Licence_Agreement_for_Version_2014

**McAfee**
http://www.mcafee.com/common/privacy/english/index.htm

**Microsoft**
http://windows.microsoft.com/en-us/windows/security-essentials-privacy
http://technet.microsoft.com/library/hh508835.asp
http://windows.microsoft.com/en-US/windows-8/windows-8-privacy-statement?T1=supplement#T1=supplement
http://windows.microsoft.com/en-us/windows/windows-defender-offline-privacy
http://www.microsoft.com/security/pc-security/msrt-privacy.aspx

**Panda**
http://www.pandasecurity.com/usa/homeusers/media/legal-notice/#e10

**Symantec Norton**
http://www.symantec.com/about/profile/policies/ncwprivacy.jsp
http://www.symantec.com/content/en/us/about/media/eulas/2014/en_us/NAV_NIS_N360_21.0_USE_-EULA.pdf

**ThreatTrack Vipre**
http://www.threattracksecurity.com/privacy.aspx

**Trend Micro**
http://www.trendmicro.com/us/about-us/legal-policies/license-agreements/index.html

**Webroot**
https://www.webrootanywhere.com/eula.asp

## Copyright and Disclaimer



For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (May 2014)