Software License Agreements: Ignore at Your Own Risk

Edward Desautels

Summary

By now you've heard all about computer viruses, Trojan horses, worms, identity theft, and phishing scams, and you're taking the necessary steps to secure your computer and privacy when using the internet. One boring little item, however, can undo your good work—if you're not careful. That item is the end user license agreement (EULA) covering the software you use.

These agreements themselves can't harm you or your computer. In fact, EULAs can do just the opposite: they highlight things that can put you at risk. The harm comes from ignoring EULAs—and the subtle warnings they might contain—by blindly agreeing to their terms:

- Ignoring EULAs can expose your computer to security risks.
- Ignoring EULAs can put your privacy at risk.

For instance, a EULA might require you to allow the software publisher or a third party to collect information about your internet activity in exchange for use of the software. This information could include not only the web sites you visit, but also information you supply in online transactions, such as your name, address, credit card number, and items purchased. Once collected, the security of this information is out of your control (a fact highlighted by the number of recent, high-profile database attacks).

By carefully reading and understanding the EULA covering software *before* you install it, you can make an informed decision that takes into account any privacy and security issues.

What is a EULA?

A EULA is a legal contract between you and the software publisher. It spells out the terms and conditions for using the software. For instance, it might say you can only install the software on one computer for your personal use, a fairly common stipulation. However, it might also say that by using the software you agree to third-party monitoring or to allowing other users to access parts of your computer.

You can agree to the EULA's terms in several ways, depending on the publisher and how it distributes its software. Some of the ways you can "agree" may surprise you, however, because they don't look or feel anything like signing a contract. You might agree by

- clicking an "I accept" button during the installation process
- opening the shrink wrap software packaging
- breaking the seal on the software CD
- mailing a registration card to the software publisher
- installing the application
- using the application

You can refuse to accept the terms and conditions of the EULA, but then you can't legally use the software.

Why EULAs are Important

EULAs can include a number of items you should seriously consider before installing the software. In general, you should note the following facts about EULAs:

- **EULAs are legally binding**. Some consumer advocates have challenged the legality of EULAs, especially long agreements clouded in complicated "legalese." The advocates argue these EULAs are a strategy for discouraging careful review and hiding controversial terms and conditions. However, a number of influential court decisions have upheld the legality of EULAs, so you need to assume you're entering into legal agreements when you accept their terms.
- **EULAs restrict how you can use the software**. EULAs often include clauses that limit the number of computers you can load the software on. They sometimes also prohibit reverse engineering for the purpose of creating compatible software. In some cases they prohibit software testing and even publishing the results of this testing.
- **EULAs may force you to agree to certain conditions when using the software**. Many software bundles force you to use all bundled components, including software produced by third-party publishers. They may also require you to agree to monitoring of your internet activity and/or sharing your computer's resources.
- **EULAs can limit your ability to sue for damages**. Most EULAs include a clause that says you cannot sue the publisher for any damages caused by using the software.

The above items are detailed in the section "A Closer Look: EULAs, Security, and Privacy."

What to Look Out For

Because software EULAs can impose terms and conditions that affect your online security and privacy, you should carefully consider what you're willing to allow in exchange for the use of the software. You should be particularly concerned about EULAs that

- allow the software publisher or third parties to monitor your internet activity
- allow the software publisher or third parties to collect your personal information
- allow the software publisher or third parties to use your computing resources
- hold you to the terms of EULAs governing third-party software components

What You Should Do

The following list presents recommendations for protecting yourself from the security and privacy problems associated with EULAs. These recommendations are explained in detail in the section "What You Can Do to Protect Yourself."

- **Read the EULA *before* you install the software.** It can be painfully boring reading, but this is the only way to know exactly what privacy and security risks you might be taking by agreeing to the EULA's terms.
- **Consider the software publisher**. If you don't know about the publisher or if you have any question about its integrity, review the EULA covering its software with extra care.
- **Beware of firewall prompts when installing software**. Firewall prompts asking you to allow certain traffic to pass may be cause for concern. Review the EULA to find out why this traffic must be allowed and whether you wish to allow it.
- **Beware of "free" software, especially peer-to-peer (P2P) file-sharing software**. Rarely is anything truly free. Review the EULA to find out what you need to do or allow in exchange for using the software, and evaluate what impact this might have on the security of your computer and personal information.

A Closer Look: EULAs, Security, and Privacy

The following sections provide real-world examples of the privacy and security issues that resulted from ignoring EULAs or agreeing to EULA terms that opened users to risk. This risk can also result from poorly managed software partnership situations in which the primary software publisher fails to check its partners' software for bugs, security issues, and compliance with its EULA. What's more, the risk you sign onto when agreeing to certain EULA terms is not limited to your own computer or information, but can extend to other computers and data connected to your network.

Monitoring Software EULAs

An interesting episode highlights the way EULAs and bundled software can combine to create security dilemmas. The IT department of a major university noticed many users on its network running a troublesome piece of software packaged as a tool for speeding internet downloads and protecting email from viruses. Bundled with it, however, was adware that collected a great deal of sensitive information about the users, including information from encrypted, secure socket layer (SSL) sessions. The EULA for this software included the following:

> …[this software] monitors all of your Internet behavior, including both the normal web browsing you perform, and also the activity you may have through secure sessions, such as when filling a shopping basket or filling out an application form that may contain personal financial and health information.

You should scrutinize and evaluate any EULA that requires you to allow monitoring of your online activity. You need to determine how comfortable you are placing personal information in the hands of a third party.

Even if you are comfortable surrendering this kind of information to a third party, you should understand that monitoring software can create wider privacy and security problems. In this case, the university IT department was particularly concerned about SSL-protected data accessible on its network. Because the monitoring software could collect data from SSL-encrypted sessions, the following data was at risk:

- critical university information
- personal information
- network IDs and passwords
- federally regulated data

Because of this threat, the IT department blocked all connections attempted by the software and redirected users to a web page that explained the problem and provided instructions for removing the software from their computers. So, when evaluating the effect of a EULA on security and privacy, consider your duty as a "good citizen" of your network: Think about the wider privacy and security problems your software might create.

File-Sharing EULAs

Peer-to-peer (P2P) file-sharing programs have become popular, but they create numerous headaches for those concerned about privacy and security. By agreeing to the EULAs covering this software, you're allowing third parties to monitor your internet activity and share this information with advertisers. You're also agreeing to open up directories on your computer for access by others. One popular P2P program even requires you to install bundled software designed to transform your computer into a distribution channel for third-party software and content publishers.

When evaluating the EULAs for P2P file-sharing programs, you should seriously consider whether you're comfortable surrendering control over directories on your computer, allowing others to access these directories, and, in some cases, allowing others to upload content to your computer. You should also consider whether you're comfortable allowing a third party to monitor your internet activity. Can you trust that those accessing your computer will not try to gain access beyond the designated directories? Can you trust the files uploaded to your computer do not contain viruses or illicit content? Can you trust assurances that the information gathered through monitoring will be encrypted or that personally identifiable information will not be collected (see "Third-Party Software and Cascading EULAs" below)?

The Australian Computer Emergency Response Team lists the following dangers associated with P2P file-sharing software:

- enhanced vulnerability to Trojan horses and viruses
- enhanced risk to your personal data
- enhanced exposure to software flaws that can harm your computer
- enhanced exposure to security workarounds that can leave your computer open to abuse

Resource Sharing EULAs

In a noted case, a free internet service provider changed the terms of its EULA to support its move into the arena of supercomputing. The revised agreement required users to allow the

installation of software that would support the provider's supercomputing venture. The agreement also required users to leave their computers on at all times so their resources would be available when needed. The EULA prohibited removal of this software and required users to allow it to make modem connections as needed to the provider's servers.

You should approach any request to surrender even partial control of your computer to a third party with extreme caution. Surrendering this control may enable the third party to reconfigure your computer in ways that weaken its security, such as by creating holes in personal firewalls or communications channels that bypass existing security mechanisms. Also, in the example of the internet service provider mentioned above, those agreeing to the revised EULA could have become accustomed to their computers connecting to the internet independently. Would these users know if a connection was the result of a virus or spyware and not the resource sharing software?

Third-Party Software and Cascading EULAs

In many cases, the software you purchase or download is bundled with third-party software. Sometimes, the EULA covering the primary software (for instance, a file-sharing program) says that you must also install the third-party software bundled with it (for instance, adware) and that you cannot disable or alter the third-party software. Normally, these third-party components have their own EULA which can, in turn, include "downstream" third-party components also covered by their own EULAs. This can make it hard for you to determine what you're agreeing to when you install the software and what affect all these EULAs have on your security and privacy.

The following diagram illustrates the problem.

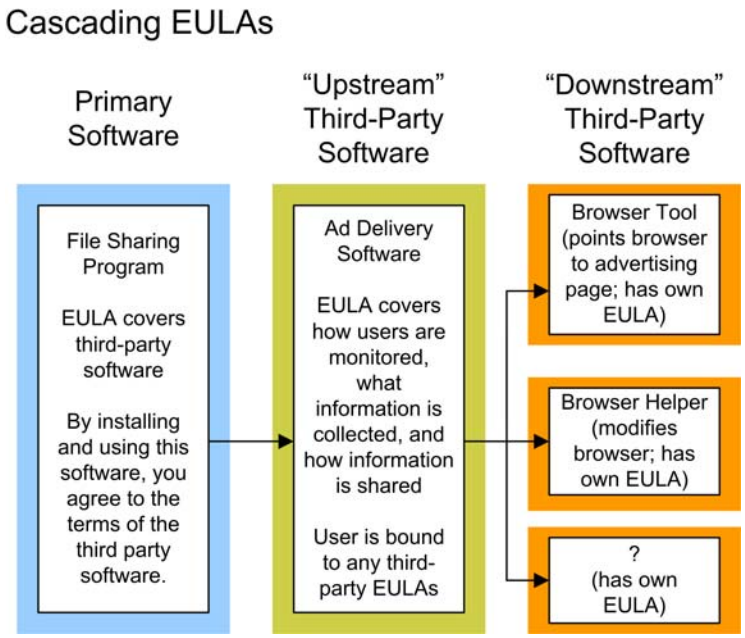

Figure 1, Cascading EULAs. "Downstream" third-party software EULAs can become numerous, making it hard for you to completely understand the terms and conditions under which you will use the software. It also raises concern over how much the primary software publisher knows about the downstream third-party software components and their license agreements.

In 2002, four popular file-sharing programs were affected by a Trojan horse bundled into their releases. The Trojan horse was introduced by a third-party advertising software partner. The advertising partner failed to recognize one of its components—itself supplied by a third-party further downstream—as a bogus application. The application presented itself as an online contest but actually contained the Trojan horse W32.Dlder.Trojan. When unsuspecting users clicked a link hoping to win a prize, the Trojan horse quietly installed itself on the users' computers. It then logged web sites visited by the users, posted them to a web site, and opened a security hole in the users' systems.

Responding to this incident, the chief technical officer for one of the file-sharing companies involved stated, "We rely on [the advertising partner] to deal with our ad deals and bundled software. We assumed that they did their homework on this package but that does not seem to be the case." The public relations manager for one of the other file-sharing companies involved admitted, "We were unaware of what this program did when we added it to our installs …."

This case demonstrates why you should exercise caution when presented with a EULA that holds you to the terms of all third-party software EULAs. You cannot assume that the primary software publisher has evaluated third-party EULAs and software.

What You Can Do to Protect Yourself

While EULAs rarely attract the kind of attention lavished on viruses or phishing schemes, they are an important consideration when managing the security of your computer and private information. The following sections present recommendations for protecting yourself from the security and privacy problems associated with EULAs.

Read the EULA

This is the most important step you can take: Before installing any software, take the time to read its EULA. While you might incur a half hour of boring reading, doing so can spare you security and privacy headaches.

If the EULA is lengthy or you find it difficult to read in the installation interface, copy it into a word processing document, quit the installation, and carefully read the agreement before proceeding. Make sure you understand the agreement's terms and conditions, and that you agree with them. Contact the software publisher with any questions you might have or if you need clarification about any specific points.

Packaged software purchased off the shelf can present something of a catch-22: How can you agree to the terms and conditions of the EULA when the package states that breaking the shrink wrap constitutes agreement? To get around this problem, consult the software publisher's web site. Software publishers often make their EULAs available online. Note the version ID or number and other pertinent information from the packaging to help ensure you read the EULA for the specific version of the software. Contact the publisher directly if you cannot locate the EULA for the software you're interested in.

Consider the Software Publisher

While there is no guarantee you will agree to the terms of any given EULA, established software publishers that have built strong business reputations are less likely to engage in questionable business practices. This includes unusual, misleading, or camouflaged terms and conditions in the EULAs governing the use of their software. You should not, however, use a company's strong business reputation as an excuse for not reading its EULA. A company's good corporate reputation does not mean you will necessarily agree with the terms and conditions of its software.

When dealing with software published by a company or organization with which you're not familiar, you may want to review its software EULAs with added scrutiny. Particular vigilance is recommended when the software is bundled with other software from third-party publishers. Be prepared to read the EULAs for third-party components when necessary.

Beware of Firewall Prompts When Installing Software

During installation, if your personal firewall generates a prompt asking whether you want to allow certain inbound or outbound connections, proceed with caution. You should verify that the software requires changes to your firewall settings for normal operation, and that you are comfortable with this operation. For instance, the EULA may require you to allow monitoring of your activity, access to specified directories (as in file-sharing programs), or use of your computer's resources. These provisions may require the opening of holes in your personal firewall.

Note, however, that in the case of bundled software, EULAs requiring you to allow monitoring, directory access, etc. may not be in the primary software's EULA. These EULA requirements may be in the third-party software EULAs.

Firewall prompts may also be a sign that rogue software has been bundled into the software package you're installing. This was the case in the file-sharing Trojan horse discussed earlier.

If you're in doubt about whether to change your firewall settings based on prompts received during software installation, consult the software's user or installation guide. If no guide is available, or if you are still unsure about allowing the traffic through your firewall after consulting it, contact the software publisher before making any changes.

Note that some personal firewalls include options to allow one-time or case-by-case connections. This option may be useful if you are reasonably certain about the legitimacy of a request. For instance, some software attempts to connect to a server during the registration process. If you are comfortable with this request, you can approve the connection for the purposes of registration, but deny all future connections.

Beware of "Free" Software

The old saying tells us "there is no free lunch." This applies to software. Many "free" software programs, such as the file-sharing programs discussed earlier, often exact a non-monetary charge for their use. This non-monetary charge is detailed in the EULA and specifies what you must allow or provide in exchange for use of the software. This may include mandatory installation of components that compromise your security and/or privacy.

Glossary

Adware:	A software application that displays advertising when the program is running. The software may display ads in pop-up windows or a bar in the frame of the application window.
Back door:	A back door is a means of access to a computer program that bypasses security mechanisms.
P2P	An internet network in which a group of computer users, each equipped with the same networking program, can connect to each other and directly access files from one another's computers.
PGP:	(Pretty Good Privacy) is a program used to encrypt and decrypt data, primarily e-mail, over the internet.
SSL	(Secure Sockets Layer) is a method for securing information exchange on the internet. SSL uses data encryption and digital certificate authentication to secure the information exchange.
Spyware	Adware that tracks user activity and passes it to third parties without the user's knowledge or consent.
Super-computing	Computing systems or schemes designed to handle extremely large databases or to perform a great deal of computation. Some supercomputing schemes involve clustering, in which many PC processors and drawn on to perform the supercomputing tasks.
Trojan horse	A program in which malicious or harmful code is packaged inside apparently harmless software or data.
Zombie	A compromised web server on which an attacker has placed code that, when triggered, will launch with other zombies a denial-of-service attack.

Further Reading

AusCERT. "File-Sharing Activity Part 1 of 2 - Security implications of using peer-to-peer file sharing software." May 20, 2002.
http://www.auscert.org.au/render.html?it=2228&template=1.

Brandt, Andrew. "Click With Caution: User Licenses Get Tough." *PC World*. April 9, 2001.
http://www.pcworld.com/news/article/0,aid,46764,00.asp.

Delio, Michelle. "What They Know Could Hurt You." *Wired News*. January 3, 2002.
http://www.wired.com/news/privacy/0,1848,49430,00.html.

Garfinkle, Simson. "Software that can spy on you." *Salon.Com*.
http://dir.salon.com/tech/col/garf/2000/06/15/brodcast/index.html.

McDowell, Mindi. "Reviewing End-User License Agreements." US-CERT. March 2, 2005.
http://www.us-cert.gov/cas/tips/ST05-005.html.

Newitz, Annalee. "A User's Guide to EULAs." Electric Frontier Foundation.
http://www.eff.org/wp/eula.php.

Rasch, Mark. "Is Deleting Spyware a Crime?" SecurityFocus. May 24, 2005.
http://www.securityfocus.com/columnists/329

Produced 2005 by US-CERT, a government organization. Updated 2008.