Consumer Software Working Group

The Consumer Software Working Group is a diverse community of public interest groups, software companies, Internet service providers, hardware manufacturers, and others that are seeking consensus responses to the concerns raised by practices that harm consumers.

Over the past several years, a subset of computer software referred to as “spyware” has become the subject of growing public concern. Computer users increasingly find programs on their computers that they did not know were installed, that create risks to privacy, that open security holes, that impair the performance and stability of their systems, that frustrate their attempts to uninstall or disable the programs, or that lead them to mistakenly believe that these problems are the fault of another application or their Internet service provider.

There is agreement that these practices can raise serious concerns. At the same time, the wide range of and lack of clarity in attempted definitions for the types of software practices that most concern consumers hamper attempts at self-regulatory, technological and legislative responses. Many definitions of spyware in circulation today are either under-inclusive in important respects or, more commonly, overbroad so that they include practices that clearly benefit consumers, or both.[1]

The Center for Democracy and Technology convened the Consumer Software Working Group. Companies, public interest groups or academics interested in joining the Working Group should contact Ari Schwartz <ari@cdt.org>, Michael Steffen <msteffen@cdt.org>, or John Morris <jmorris@cdt.org> at the Center for Democracy and Technology.

Examples of Unfair, Deceptive or Devious Practices Involving Software
Version 1.0

The Consumer Software Working Group is concerned about a specific set of devious, deceptive or unfair practices that adversely affect consumers online. While the following list of examples is not nearly complete, it describes a series of activities and behaviors that the Group considers to be clearly objectionable.

Specifically, the Group identifies three broad types of practices where abuses occur today. Most of these practices may be illegal under current law, depending on the specific facts of the particular case. Within each area, we offer illustrative examples, based on real cases. We note that each of the objectionable behaviors we identify has constructive consumer-friendly counterparts when carried out with proper notice and consent and in ways that give consumers control. Automatic installation, personalization and tracking, and in some cases resistance to uninstallation can provide important benefits to consumers.

We hope that this list of objectionable practices will help to focus technical, self-regulatory, regulatory and law enforcement efforts to protect consumers from inappropriate activities in a more targeted and effective manner, while avoiding unintended negative consequences for good actors and consumers alike. The Working Group believes that this is an area that could be ripe for self-regulatory efforts to craft industry principles to protect consumers and the marketplace.

[1] For example, the Working Group observes that the current Utah law addresses practices involving software that most informed consumers would not consider unfair, deceptive or devious and fails to cover some practices that most informed consumers would consider unfair, deceptive or devious.

1) **Hijacking** — The practices described in this section are objectionable to the extent that they enable an unaffiliated person to use the user's computer in a way that ordinarily would not be expected. This may occur through an unnoticed program consuming the user's computing resources or resetting a user's existing configurations without the user's knowledge, or through coercion or deception.

Example: A computer user sees an Internet advertisement for Program A. The user clicks on the ad and is sent to a page that pops up a window asking if the user wants to download Program A. The user clicks “no,” but Program A is eventually downloaded and installed anyway.

Example: A computer user sees an Internet advertisement for Product B. The user clicks on the advertisement, and is sent to a page that informs the user that “Program C is needed to view this Web page.” This leads the user to believe that Program C is necessary to view the site about Product B, so the user clicks “yes” and the program is downloaded and installed. In fact, Program C is not necessary to view the website for Product B and the user is never informed of the actual reason why Program C was installed.

Example: A computer user sees an Internet advertisement for Program D. The user clicks on the ad, and she is sent to a page that immediately pops up a window asking if she wants to download Program D. The user clicks “no.” This happens repeatedly until the user gets frustrated and clicks “yes.”

Example: A computer user receives an Internet advertisement for Product E as part of a webpage he is looking at. Simply as a result of loading the ad, Software Program F wholly unrelated to Product E is downloaded onto the user’s computer. No notice or opportunity to consent to download Software Program F was provided.

Example: While browsing the Internet, a computer user is offered the opportunity to download and install Software Program G. Using a fraudulently obtained digital certificate, the download request falsely identifies Software Program G as being from the user’s trusted Internet Service Provider, H. In fact, the Program is not from Internet Service Provider H, and has no relation to the ISP. However, based on its claimed affiliation with H, the user agrees to let the program be downloaded and installed.

Example: A computer user loads Company I’s Web page. The Web page opens another page running a java script. When the user closes Company I’s Web page, the java script page covertly resets the user's homepage without obtaining consent.

Example: A computer user loads Company J's Web page. The Web page opens another page running a java script. When the user closes Company J's Web page, the java script page covertly resets the user's homepage. The java script is written such that any time the user attempts to reset his homepage, the program automatically resets it again so the user cannot reset his homepage to what it was before the hijacking took place.

Example: A computer user downloads Software Package K. Among the programs in Software Package K is a dialer application that was not mentioned in any advertisements, software licenses, or consumer notices associated with the package or in information provided in conjunction with the ongoing operations of the package. The dialer application is not an integral part of Software Package K. When the user opens her Web browser after installation of Software Package K, the dialer opens in a hidden window, turns off the sound of the user's computer, and calls a phone number without the user's permission.

Example: A computer user is sent Software Package L as an attachment to an unsolicited commercial email message. There is no documentation for Software Package L. Included in Software Package L is Program M that sends a message to Computer N. Computer N then uses Program M on the user's computer as a means to send out unsolicited commercial emails.

2) **Surreptitious surveillance** — The practices described in this section are objectionable to the extent that they involve intrusive and surreptitious collection and use of personally identifiable information about users that is wholly unrelated to the purpose of the software as described to the consumer.

Example: A computer user downloads Software Package P. Software Package P contains a keystroke logger unrelated to any functions described to the user. The keystroke logger records all information input on the user's computer and sends this information on to another computer user. The first user is not informed about the operation of the keystroke logger.

Example: Program Q advertises itself as a search tool bar. A user downloads Program Q to gain the search functionalities. Program Q installs a tool bar, but — once installed — also mines the user's registry and other programs for personally identifiable information about the user unrelated to the search functionality and without informing the user or obtaining consent. When the user connects to the Internet, Program Q sends this information back to the company that makes Program Q.

3) **Inhibiting termination** — The practices described in this section are objectionable to the extent that they frustrate consumers' efforts to remove a program, deactivate it or otherwise render it inoperative. Generally, these practices are intended to prevent the user from severing or terminating a relationship with the provider of the program.

Example: A computer user downloads Software Package S. Software Package S contains Advertising Program T. Advertising Program T sends the user pop-up ads while the user is surfing the Web even if no other programs in Software Package S are running. The pop-up ads are not labeled as related to Advertising Program T or Software Package S in any way and there is no other way to find the ads' origin. The user is concerned about the increase in pop-up ads, but does not know whether they are caused by Program T or are from the Web sites that he is visiting. The user has no means to find out the origin of the ads in order to make a decision about uninstalling Program T.

Example: A computer user downloads Software Package U. As initially disclosed to the user, Software Package U contains a mandatory program, Advertising Program V, which is bundled as a way to generate revenue and pay for the development of Software Package U only. When the user uninstalls Software Package U, the user is not given a clear opportunity to uninstall Program V at that time, and Advertising Program V stays on the user's computer.

Example: A computer user downloads Gaming Program W. The user wants to remove Gaming Program W from the computer. Gaming Program W does not have an uninstall program or instructions and does not show up in the standard feature in the user's operating system that removes unwanted programs (assuming this feature exists in the operating system). The user's attempts to otherwise delete Program W are met by confusing prompts from Program W with misrepresentative statements that deleting the program will make all future operations unstable.

Example: A computer user downloads Program X. The user wants to remove Program X from the computer. Program X appears in the standard feature in the user’s operating system that removes unwanted programs. However, when the user utilizes the “remove” option in the operating system, a component of Program X remains behind. The next time the user connects to the Internet, this component re-downloads the remainder of Program X and reinstalls it.

The following companies, organizations and individuals have worked to describe Examples of Unfair, Deceptive and Devious Practices Involving Software. These descriptions can be used to help focus technical, self-regulatory, regulatory and law enforcement efforts to protect consumers from inappropriate activities.

America Online
Business Software Alliance
Center for Democracy and Technology
Claria Corporation
Consortium of Anti-Spyware Technology Vendors
Consumer Action
CryptoRights Foundation
Dell, Inc.
Distributed Computing Industry Association
EarthLink
eBay
Electronic Frontier Foundation
Google
Information Technology Industry Council
Internet Commerce Coalition
Lavasoft
Microsoft
Network Advertising Initiative
Privacilla.org
Sharman Networks
Peter Swire, Moritz College of Law of the Ohio State University[2]
TRUSTe
Webroot Software
WhenU
Yahoo!

[2] Individuals are listed with their affiliation for identification purposes only.