The Pure Software Act: A Proposal for Mandatory Software Labeling

Simson L. Garfinkel <simsong@mit.edu>
MIT Computer Science and Artificial Intelligence Laboratory

Abstract

Spyware and adware are a scourge of desktop computing. Many of these programs appear to perform useful functions but have hidden purposes and code that are rarely in the user's interest. For example, Gator's eWallet program fills out web forms but also displays pop-up advertisements on a regular basis.[1] Some spyware programs go further by hiding the fact that they are running or by failing to provide or "uninstall" scripts.

Adware and spyware is developed and sold by legitimate companies. These activities do not violate the Computer Fraud and Abuse Act (18 U.S.C. 1030)[2] because users consent to be monitored when they agree to overly-broad and turgid click-through license agreements.

The problem that computer users face today with spyware is remarkably similar to the problem that they faced a century ago with patent medicines. Just as programs today have undocumented functions, patent medicines had undocumented ingredients such as cocaine and codeine. Many people became addicted to such potions without even realizing it.

The solution to patent medicines was the 1906 Pure Food and Drug Act[3] --- legislation that forced companies selling a food and drugs in the United States to disclose certain ingredients on product labels. With the knowledge of what they were about to ingest, consumers were able to identify and avoid (if they wished) consuming potions that were "habit forming." Equipped with the information from thousands of labels, lawmakers were empowered to pass additional legislation in the public interest.

A similar approach can be applied to software. Federal regulations could require mandatory disclosure accompanying any program sold or distributed in the US. The label could consist of icons that documented specific program behaviors. These icons would be displayed at the top of license agreements, on install screens, and in key places such as the Windows "Add or Remove Programs" control panel. Some sample icons are shown in Figure 1.

 **Hook** Hooks itself so that it runs at boot.	 **Modify** Modifies your computer's operating system.	 **Monitor** Monitors what you are doing even when not the active application	 **pop-up** Displays pop-up windows, even when not active application.
 **Self-updates** Downloads code from the net that could change its behavior.[4]	 **Dial** Can dial a phone (and spend your money!)	 **Sticky** Cannot be uninstalled.	 **Remove** Application allows others to remote-control your computer

Figure 1: A few icons that could be required by federal regulation.

Icons are not necessarily bad. For example, the Google's Toolbar, which is generally not regarded as a piece of spyware, would get the **Hook, Modify,** and **Self-updates** icons. With time, in fact, consumers might want to avoid programs that do not display the **Self-updates** icon, because these programs would not automatically patch themselves when new security flaws are discovered. The point of the icons is not to scare off all consumers, but to make visible functionality that is invisible today. Disclosure also helps academics, activists and lawmakers.

This 10-minute talk will discuss the history of the 1906 Act, show how similar justification can be used for software today, and make an initial proposal for icons and behaviors that would require disclosure.

---

[1] Barrett, Robertson, "Five Major Categories of Spyware," Special to Consumer WebWatch, October 21, 2002. http://www.consumerwebwatch.org/news/articles/spyware_categories.htm

[2] http://www.usdoj.gov/criminal/cybercrime/1030_new.html

[3] FDA Consumer, "The Story of the Laws Behind The Labels," Food and Drug Administration, June 1981. http://vm.cfsan.fda.gov/~lrd/history1.html

[4] Any update that added a new icon would presumably require explicit user approval.