Simson L. Garfinkel

April 7, 2004

To: FTC Spyware Workshop
From: Simson L. Garfinkel
Subject: Public Comments on Spyware

To the FTC Spyware Workshop:

Spyware is one of the most pressing problems facing computer users today. Unlike computer worms and viruses, spyware is authored by paid programmers at legitimate companies. This means that there is considerable resources at the disposal of spyware creators, there are systems in place to distribute spyware, and there is a profit motive to make spyware as nefarious, as covert, and as lucrative as possible.

On Wednesday, April 7, 2004, I published an article on *Technology Review's* website, technologyreview.com. The article, entitled "The Pure Software Act of 2006," proposes a mandatory labeling regime as a solution to the spyware problem.

The State of Utah recently passed an Act regarding spyware, and two bills have been proposed in the US Senate. These legislative approaches all attempt to ban spyware outright. My concern with this approach is twofold.

> First, the activities of spyware are similar to the activities of many legitimate programs. These acts are crafted so that they will only apply to spyware, but in so doing they create exemptions for non-spyware programs. It is my fear that these exemptions could be utilized by spyware programs as well.
>
> Second, I believe that we can use spyware as an opportunity to pass legislations or regulations that would benefit consumers of many kinds of programs. If we carefully craft our regulations so that they only apply to spyware, we will have missed an opportunity to increase consumer knowledge over non-spyware programs.

Instead of banning spyware, my approach is to force the makers of all programs to reveal when particular behaviors have been coded into their systems. Whether or not these behaviors are "good" or "bad" will depend on many things, such as the company's data protection policies. This is not my

concern. Instead, my concern is to make sure that consumers are aware of what their software might to.

Attached to this letter is the text of my article as well as comments that have been publicly posted on the TechnologyReview.com website. If you have another workshop, I would welcome the chance to come down and address your group.

Sincerely,

Simson L. Garfinkel

<< Return to article

The Pure Software Act of 2006

100 years ago, Congress passed a law requiring honest labeling of food and drugs. Now the time has come to do the same for software.

By Simson Garfinkel
The Net Effect
April 7, 2004

Spyware is the scourge of desktop computing. Yes, computer worms and viruses cause billions of dollars in damage every year. But spyware—programs that either record your actions for later retrieval or that automatically report on your actions over the Internet—combines commerce and deception in ways that most of us find morally repugnant.

Worms and viruses are obviously up to no good: these programs are written by miscreants and released into the wild for no purpose other than wreaking havoc. But most spyware is authored by law-abiding companies, which trick people into installing the programs onto their own computers. Some spyware is also sold for the explicit purpose of helping spouses to spy on their partners, parents to spy on their children, and employers to spy on their workers. Such programs cause computers to betray the trust of their users.

Until now, the computer industry has focused on technical means to control the plague of spyware. Search-and-destroy programs such as Ad-Aware will scan your computer for known spyware, tracking cookies, and other items that might compromise your privacy. Once identified, the offending items can be quarantined or destroyed. Firewall programs like ZoneAlarm takes a different approach: they don't stop the spyware from collecting data, but they prevent the programs from transmitting your personal information out over the Internet.

But there is another way to fight spyware—an approach that would work because the authors are legitimate organizations. Congress could pass legislation requiring that software distributed in the United States come with product labels that would reveal to consumers specific functions built into the programs. Such legislation would likely have the same kind of pro-consumer results as the Pure Food and Drug Act of 1906—the legislation that is responsible for today's

labels on food and drugs.

The Art of Deception

Mandatory software labeling is a good idea because the fundamental problem with spyware is not the data collection itself, but the act of deception. Indeed, many of the things that spyware does are done also by non-spyware programs. Google's Toolbar for Internet Explorer, for example, reports back to Google which website you are looking at so that the toolbar can display the site's "page rank." But Google goes out of its way to disclose this feature—when you install the program, Google makes you decide whether you want to have your data sent back or not. "Please read this carefully," says the Toolbar's license agreement, "it's not the usual yada yada."

Spyware, on the other hand, goes out of its way to hide its true purpose. One spyware program claims to automatically set your computer's clock from the atomic clock operated by the U.S. Naval Observatory. Another program displays weather reports customized for your area. Alas, both of these programs also display pop-up advertisements when you go to particular websites. (Some software vendors insist that programs that only display advertisements are not spyware, per se, but rather something called adware, because they display advertisements. Most users don't care about this distinction.)

Some of these programs hide themselves by not displaying icons when they run and even removing themselves from the list of programs that are running on your computer. I've heard of programs that list themselves in the Microsoft Windows Add/Remove control panel—but when you go to remove them, they don't actually remove themselves, they just make themselves invisible. Sneaky.

Yet despite this duplicity, most spyware and adware programs aren't breaking any U.S. law. That's because many of these programs disclose what they do and then get the user's explicit consent. They do this with something that's called a click-wrap license agreement—one of those boxes full of legal mumbo-jumbo that appears when you install a program or run it for the first time. The text more-or-less spells out all of the covert tricks that these hostile programs might play on your system. Of course, hardly anybody reads these agreements. Nevertheless, the agreements effectively shield purveyors of spyware and adware from liability. After all, you can't claim that the spyware was monitoring your actions without your permission if you gave the program permission by clicking on that "I agree" button.

Uniform standards for labeling software wouldn't replace the need for license agreements, but they would make it harder for companies to bury a program's functions. Such legislation—call it the Pure Software Act of 2006—would call for the Federal Trade Commission to establish standards for the mandatory labeling of all computer programs that are distributed within the United States. A labeling requirement would force makers of spyware to reveal their program's hidden features.

The Historical Precedent

As I hinted above, we've been down this road before. The Pure Food and Drug Act of 1906 was passed by Congress to deal with a remarkably similar set of deceptive business practices. The problem back in 1906 was foods and drugs that were sold with misleading labels, or without labels at all.

The 1906 Act required that every drug sold in the United States be delivered to the consumer in a package that states the strength, quality, and purity of the drug if they differed from accepted standards. The dose of the drug had to be clearly printed on the outside of the package. A number of ingredients that tended to accompany nineteenth century patent medicines—substances like alcohol, codeine, and cannabis—had to be clearly disclosed as well.

In the case of food, the Act required that labels explicitly mention any artificial colors and flavors—after 1906, you couldn't sell something called "orange soda" unless it had flavoring that came from genuine oranges. Otherwise you were selling "imitation" or "artificial" orange soda. And every bottle, box, and bag of food needed to clearly indicate the precise weight of the food that

was inside the container.

The Pure Food and Drug Act was successful for many reasons. Forcing manufacturers to disclose what was in their products allowed consumers to avoid products that contained things they didn't want to ingest. For example, many of the snake-oil tonics distributed at the end of the nineteenth century contained significant doses of addictive drugs like codeine or cocaine. Forcing to disclose these drugs on the product's label, along with a warning that said "may be habit forming," made it possible for consumers to make informed decisions. Labeling also empowered scientists and eventually consumer groups to check the product makers' claims. Mandatory labeling put pressure on manufacturers to remove the most objectionable ingredients —a process that continues to this day. Finally, the labels provided additional evidence to lawmakers that was used to justify the crafting of additional legislation.

The parallels between nineteenth century adulterated food products and twenty-first century adulterated software is uncanny. Just as some tonics claimed to do one thing (like grow hair) when they actually did another (made the user intoxicated and chemically dependent on codeine), today we have software that claims to do one thing (set the time of your PC) and actually does another thing (displays ads when you visit particular websites).

So what would a Pure Software Act look like? Judging from 1906 legislation, the best results are likely to come from requiring labels that would directly address the issue of deception. The new law would therefore require that software identify itself as such: no more hidden programs that silently install themselves and then run without any visible evidence. The Pure Software Act would make it illegal for programs to run without revealing themselves though the standard means used by the host operating system. And the Act would require that programs have an "uninstall" feature—or else make it very plain that they do not.

Documenting a program's installation and providing for its removal is just the start. The Pure Software Act would require that the Federal Trade Commission identify specific practices of software that would have to be explicitly revealed when the programs are distributed and run. Instead of letting companies hide the features of their software with obscurely written legalese buried in click-through license agreements, the legislation would require that the disclosure be made in the form of easy-to-understand icons that could be clicked on for additional information. Clicking on the icon would bring up further explanatory text—perhaps from a website maintained by the Federal Trade Commission. The icons could also be displayed in other places. Under Windows, for example, the Task Manager and the Add/Remove control panel could both display the mandated behavior icons alongside the program's application icon.

A Modest Proposal

To make my proposal more concrete, I've come up with a list of program behaviors that would have to be disclosed, and some representative icons. These icons (created by TechnologyReview.com senior graphic designer Matthew Bouchard) are just samples to illustrate the concept. Actual government-mandated icons would be developed by a team of professionals with expertise in human computer interface, tested on focus groups, and put up for public comment. But these icons are useful to convey the general idea and to start discussion.

Hook: Runs at Boot
Some programs hook themselves in to your computer's operating system so that they automatically run whenever the computer is rebooted or a user logs in. Other programs don't. Today there's no way to tell except by performing a detailed analysis of the computer's configuration files before and after the program is installed and noting the changes. Any program that installs itself so that it automatically runs would have to display this Hook icon.

Dial: Places a Phone Call
One common spyware scam involves programs that cause your computer to call phone numbers that cost you money. For example, a few years ago some pornographic websites distributed a program called david.exe that caused the victim's computer to make a long-distance phone call to an Internet service provider in Eastern Europe; the porn company got to keep half of the (exorbitantly high) long distance revenues. Other kinds of scam software might dial 900-numbers or even use your computer to send junk faxes without your knowledge. Documenting that the software has code that could make it dial your phone would be a good way to address this problem.

Modify: Alters Your Computer's Operating System
Some programs do more than simply install themselves to run at boot —they alter your computer's operating system. Seeing this icon would give you a reason to ask questions. More likely, forcing this kind of disclosure would simply end the practice on the part of developers.

Monitor: Keeps Track of What You're Doing
Most programs mind their own business. But some software watches your keystrokes and monitors the Web pages you are viewing even as other programs run in the foreground. Programs can watch as you create files, make copies of every document that's printed, or simply note when your computer is idle and when it's in use. The key here is that personal information is being captured by a program when you think that it's not listening. Perhaps this icon might incorporate a lightening bolt to indicate that the monitored information is reported back over the Internet to someone else.

Displays Pop-Ups
A well-mannered program speaks only when spoken to. Some programs, on the other hand, demand your attention. I was astonished the other day when Microsoft Word 2003 popped a window up on my computer inviting me to participate in some kind of survey. A few years ago I noticed that an electronic wallet program called Gator was opening up windows to competing websites whenever I visited certain online merchants.

Remote Control: Lets Other Programs Take Over Your Computer
In theory, any program that's running on your computer can take it over and execute commands on the part of others. In practice, only very few programs have the ability to offer others such remote control. Programs that do so should be labeled.

Self-Updates: This Program May Change Its Behavior
One of the most important techniques for software vendors to deal with persistent computer security problems is to have their programs automatically update themselves with code downloaded from the Internet. Programs that have this feature should advertise that capability, because they can change their behavior without any input from the user.

Stuck: Cannot be Uninstalled
Some programs, once installed in your computer, are impossible to dislodge. These programs are typically operating system updates, but it is easy for a clever programmer to make uninstallable spyware as well. Consumers should be informed that there are some programs for which there is no going back.

Rules of Engagement

With the icons would come rules for their use. For instance, many of today's click-through license agreements say that the user implicitly agrees to any changes in the license agreement unless those changes are "substantive." But what is substantive? Once a label regime was in

place, a substantive change could be legally defined as a change that results in a change of icons—for example, if a self-updating program downloaded a remote-control feature. The law could then require that this sort of change would require new consent on the part of the user.

One tension inherent with any labeling regime is in deciding what gets put on the label and what gets left out. The more information required on the label, the more expensive it will be to produce, and the less likely that consumers would be to actually pay attention to the information. Any regulatory body implementing this policy will need to avoid icon creep—having 23 different icons on each piece of software won't serve the needs of consumers, it will just cause confusion.

Personally, I'd like my software labels to distinguish between information that's collected and used in aggregate form and personally identifiable information that's stockpiled in a large data warehouse. But fundamentally this isn't about what the program does—it's about what the company does after the program has reported its information. That is, this is a business practice that should be protected by the company's privacy policy. Perhaps we need icons there, too. (Years ago, the trade organization TRUSTe tried to have three icons for three different kinds of standard privacy policies; TRUSTe gave up when its member companies balked.)

Another tension is between voluntary and mandatory labeling. I think that mandatory is the way to go. We're living in a voluntary regime today: Google has done a great job explaining what the Google Toolbar does, but other companies are not so forthcoming. Nearly 100 years' experience with The Pure Food and Drug Act of 1906 shows that labeling requirements need not be onerous, but they do need to be mandatory—otherwise the good companies label and the bad companies don't. What's needed now is to extend this principle to the world of software.

Acknowledgements
I've been discussing this proposal for software labeling for several months with associates in Cambridge. At Harvard Law School, Jonathan Zittrain offered very helpful comments; at MIT's Computer Science and Artificial Intelligence Laboratory, I had useful discussions and comments with my thesis advisors, Rob Miller and David Clark, and with my fellow student, Steven Bauer.

Simson Garfinkel is an incurable gadgeteer, an entrepreneur, and the author of 12 books on information technology and its impact.

FORUMS

The Pure Software Act of 2006

Post A Message
View All Forums

100 years ago, Congress passed a law requiring honest labeling of food and drugs. Now the time has come to do the same for software. Read the article.

Posted 4/7/2004 2:55:13 PM by Jim Demers

Subject: Software regulations

It's already happening, at the state and federal levels.

Utah has recently enacted the "Spyware Control Act", which prohibits surreptitious installation of spyware on consumers' computers, and prohibits the use of "context-based triggering mechanisms" to display ads that obscure web pages. The law provides for up to $10,000 in damages for each violation, to be tripled in cases of willful violation.

For the gory details, see http://www.le.state.ut.us/~2004/bills/hbillenr/hb0323.htm

Anti-spyware legislation has also been introduced in Congress. S-2131 (the "Controlling Invasive and Unauthorized Software Act") would prohibit the unauthorized installation of software on a computer, and S-2145 ("Software Principles Yielding Better Levels of Consumer Knowledge Act"; aka the "SPY BLOCK" Act) would require disclosure and uninstall features on spyware programs, and would require disclosure of any advertising features in such programs.

The Utah law has the industry in bit of a lather, as you can imagine. I expect that the phrase "not intended for installation in Utah" will now be buried in the fine print of spyware click-through agreements.

Posted 4/7/2004 1:46:00 PM by Jon

Subject: The Pure Software Act of 2006

While there may be some merits to this The Pure Software Act of 2006 proposal. There is actually already in existence a much better set of protections and penalties. I was rereading some books and papers the other day when it suddenly hit me that all of this so called spyware is in direct violation of exiting federal law.
I refer you for starters to the 4th amendment of the United States Constitution which says,

"The rights of the People to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
The 14th amendment also applies here. To put some teeth behind this refer to Title 18 USC sections 241 and 242 for starters which have some nasty sharp teeth. There

are other sections of the USC as well as state and local laws which can and should be applied to this problem. Consider local Peeping Tom laws as another source of protection.
The point is that we have the right to be secure with only the exceptions mentioned in the 4th, this means that not one private person nor company has the authority to spy upon us unless they have applied for and recieved a warrant, therefore they are in violation of the law everytime they enter, invade your computer which falls under the protection of being one of your effects, not to mention your papers, all the while being in your house [usually].
There are already plenty of laws on the books which need only be used; we don't need yet another layer of laws to further confuse everyone and make the lawyers more money.

Now there are some who will say well that sort of thing [the 4th etc.] applies only to government and police agencies and in no way applies to the private sector. I say they are wrong, read it again slowly. It says that you have the right to be secure with only extremely limited exceptions, like if you are under consideration for having committed a criminal act and there is great reason to believe that proof of such will be found within your protected envelope; the swag, the smoking gun etc. Which is the reason that a warrant must be specific, no fishing expeditions need apply.

I would love to see the Attorney Generals, both State and Federal take this argument to the wall starting with a few of the worst offenders.
I had no idea how bad this problem was until I got some software, like spystopper and Ad-aware which found hundreds of invasive programs on the first scan. It also let me know that everytime my "Free AOL IM" given to me by my ISP [Earthlink] fired up it was attempting to insert more spyware; AOL might be a good place to start with; take down a big fish the little fish won't be so brave.
Any thoughts on this from you out there in unsecured cyber space?

Posted 4/7/2004 12:57:36 PM by Robert L. Cox

Subject: Software labelling act

Senator O. Hatch, R. Utah, several years ago got a reloluction passed and made into law that essentially emasculated the FDA labelling requriements. As a result, Ephedra was allowed and many claims of medical, unsupported and un-peer reviewed, claims were made which has led to the deaths of many unsuspecting and gullible individuals.

Under R. Reagan, who did not like regulation in any form, Clarence Thomas, then head of the Equal Opportunity, Age Discrimination area, decided that they weould not enforce the age discrimination laws. As a result, I and many others in the 50 year old bracket were let go by corporations using the non-enforcement of existing laws to justify their actions. I could have, but did not have the finances to prosecute under the law as many did. As a result, Clarence Thomas was first made a Federal Judge then elevated to be an Associate Justice of the Supreme Court. He is the one who "Elected" GWBush by stopping the state-wide recount in Florida contrary to 1873 law requireing the Federal Government to stay out of State election procedures.

I think Ashcroft would not enforce such a law. He would be supported by Microsoft et al.

Incidentally, I wish my spell check program would work on this!

Posted 4/7/2004 10:58:40 AM by Peter Harter

Subject: semantic?

Seems a bit like UCC2B and that was a mess of lawyers and consumer rights lobbyists. So who is involved in this SG proposal is important.

Would this law require the declaration of software contents to be machine readable? This may assist the development of the semantic web and help bridge language barriers -- an increasingly significant policy issue in the WSIS area.

But if the Platform for Internet Content Selection (PICS) did not work because website operators and browser users (consumers) did not take the time to implement and if consumers don't read through click wrap, then....

But if people actually read through, use and benefit from Creative Commons licenses, then...

This is worth further discussion Simson. Thanks!

Posted 4/7/2004 10:11:28 AM by Chris

Subject: What effect could this have?

It seems to me that if this kind of labeling became mandatory, the major issue wouldn't be what labels to put on a piece of software, but what constitutes *one* piece of software. For instance, in the Norton Utilities suite, is it one application? Or a dozen? Does each piece need its own label?

The problem only gets worse when you consider free (libre) software or open source software. Putting requirements on the labeling of software that oftentimes is only available in source code form apart from third-party distributors (true for dozens of popular open source packages), or software that is being heavily developed by dozens or hundreds of people, seems to me to be impossible to really enforce, and any attempts would serve mainly to limit the freedom of people to produce good software without red-tape restrictions that could be leveraged by existing powerful proprietary software companies to smash free software competition.

Posted 4/7/2004 6:50:59 AM by Chris

Subject: Good Ideas

You did an excellent job in putting this article together. Right down to creating/finding the right icons to describe the specific enhancements that should be conveyed.

I agree very strongly with what you have mentioned here.

I would want a law like this to be thought out very carefully, however, I would hate such a law to put binding on an application that would require it to give away secrets inherent to its security structure or anything like that. The wording of the law would have to be careful.

Of course, this reminds me of one of my pet peeves.

What this article really makes me think about is the whole legal jargon issue to begin with. I have noticed that most end user agreements, as well as numerous other legal documents, and laws themselves, are so full of legal jargon and loopholes that they are very similar to the problems you describe with software here.

What if we had a law requiring legal documents to have an accompanying document that provided a natural language interpretation of the document, and, more importantly, a "spirit of the law/rule" document that outlines the intended purpose of the rule, law or agreement.

I think we often get so caught up in the "letter" of the law that we ignore the "spirit" of most laws, and are often required to break that spirit due to some legal loophole.

I think including such a document would actually help bind the hands of shifty legal document drafters (a.k.a. shady lawyers) that are intentionally creating agreements, rules and laws that were intended to have loopholes. They wouldn't likely say "The spirit of this rule is to allow us to do this while you think you're only allowing us to do that."

Instead, if the spirit of a law about clear cutting is to prevent deforestation, then

loopholes in the law that would allow deforestation under certain circumstances could potentially be seen as breaking the "spirit" of the law, and would instantly bring the "letter" of the law into question if such a thing happened.

Anyway, sorry to ramble, thanks for bringing this topic to light.

Page: 1

The Pure Software Act of 2006

Post A Message
View All Forums