

<http://writ.findlaw.com/ramasastry/20040601.html>



-----  
**Can Utah's New Anti-Spyware Law Work?  
Why the Law is More Promising than Some Critics Claim**  
**By ANITA RAMASASTRY**  
-----

Tuesday, Jun. 01, 2004

In March of this year, Utah became the first state to enact new legislation addressing certain types of "spyware" - with its [Spyware Control Act](#). (Spyware is software that tracks a consumer's online activities, and uses the data it collects to choose targeted pop-up advertisements and other promotional messages, which are then displayed to the user.)

Then, in May, a suit was brought pursuant to Utah's new act. Overstock.com sued Massachusetts-based online retailer SmartBargains, Inc. in the Third District Court in Salt Lake City, claiming that SmartBargains used spyware to display pop-up ads over the Overstock.com Web site. Overstock.com is seeking injunctive relief, damages, attorney's fees and other costs.

Meanwhile, other states are also considering legislation on this topic, and several bills on this issue have been introduced in Congress. In addition, the Federal Trade Commission recently hosted a spyware workshop in an attempt to craft useful policy solutions.

The Utah law has been the subject of criticism from industry as well as from privacy advocates alike. But on closer examination, many of these criticisms are without merit.

All the Utah law requires is that spyware creators or issuers must give consumers notice, obtain their consent, and give them a means to uninstall the spyware. That is not too much to ask of companies that, until now, have been installing software on users' computer without doing these very basic things.

### **Spyware: What It Does, How It Works, and Why It's Controversial**

Such messages are annoying to users. But what is more disturbing, to many users, is that spyware also tracks and/or transmits their personal information - for instance, the websites they visit - without their knowledge or permission.

Businesses are also annoyed by spyware that may mean that customers who visit a given business's site, are exposed instead to its [competitor's](#) advertisements - and indeed, that these ads obscured the site itself. Lawsuits have ensued -- filed by companies that allege that popup ads give rise to various copyright, trademark, and unfair competition claims.

Where does spyware come from? Typically, it is installed on users' computers, without their knowledge or consent. That might happen when a user downloads free software programs from the Internet -- such as email software, web browsers and digital music file-sharing programs.

These programs may bundle spyware alongside the other software, so that in order to download the programs they want, users must download spyware as well.

### **The Utah Spyware Control Act: What It Prohibits**

The Utah bill originated after 1800contacts.com, an online contact lens distributor (located in Utah), discovered that some of its customers received targeted pop-up advertisements while visiting its website.

The Spyware Control Act prohibits persons from installing spyware -- or causing it to be installed -- on another person's computer. But it makes clear "spyware" does not include software designed and installed solely to diagnose or resolve technical difficulties; software or data that solely report to an Internet website information previously stored by the Internet website on the user's computer, including cookies, HTML code; or Java Scripts; or an operating system.

The Act also prohibits persons from using a "context based triggering mechanism to display an advertisement that partially or wholly covers or obscures paid advertising or other content on an Internet website in a way that interferes with a user's ability to view" the site. (In other words, it prohibits targeted pop up ads that cover others' sites.)

It also prohibits software that records and reports a users' online actions, sends personal data to other companies, or serves pop-up ads without the user's permission unless three conditions are met. The software provider must give consumers notice of such data transmissions in a license agreement, obtained the user's consent through the license agreement, and provide an uninstall feature.

The law provides for substantial penalties of \$10,000 per violation, as well as other judicial remedies.

### **Industry Criticism: The Law is too Broad**

In early March 2004, American Online, Amazon.com, Cnet, eBay, Google, Microsoft Corp., and Yahoo! [sent a letter](#) to the sponsors of the Utah legislation, arguing that the legislation was flawed.

They complained that the definition of "spyware" - even despite the exceptions noted above -- is still too broad or overinclusive. They claim that "spyware," as defined in the Act, encompasses several types of important and beneficial Internet communications software, and even routine network communications. They fear, for instance, that the Act prohibits information technology and security companies from collecting data to analyze and prevent virus attacks.

### **Ben Edelman's Persuasive Response to Industry Criticism**

However, Harvard graduate student and spyware expert Ben Edelman offers a [persuasive rebuttal to these industry critiques](#).

Edelman grants that programs such as virus definition updaters "might be taken to monitor a computer's usage" But he responds: So what?

"[I]t's hard," Edelman notes, "to imagine a legitimate, mainstream antivirus software that lacks a license agreement presented to the user, that fails to tell the user what information it will transmit to remote servers, or that lacks an uninstall program." Thus, any virus definition updater ought to comply with the three-pronged requirements of the Act anyway - and thus be permitted.

Edelman also grants that Search engine toolbars "often need information about the web sites users visit; for example, the [Google Toolbar](#) obtains and transmits this information so that it can offer users related sites, site rankings, and the like." But again he responds: So what?

As Edelman points out, as with virus definition updaters, the law only prohibits toolbars when there has been no notice to the user, no consent or where the program cannot be uninstalled readily. Put another way, like virus definition updaters, toolbars may fall within the Act, but they will still be permitted based on its three pronged requirements.

### **Is the Utah Act's Notice Provision Too Much? Or Not Enough?**

Another typical critique focuses on the Act's requirement that consumers be provided with proper notice about spyware in the form of a license agreement.

Industry advocates say such notice should not be required - but that's hard to stomach. Why should we allow secret installation of unwanted software on our computers - software that can reap our personal data?

Meanwhile, privacy advocates say the notice the Act requires is not enough. The Center for Democracy and Technology, for example noted that "the specific requirements for presentation of notice in [the Spyware Control Act] are weak, and could set a bad precedent for what constitutes acceptable notice for consumers".

But on closer examination, the Act's requirements don't seem as "weak" as the CDT claims. The Act requires that the notice be written "[in plain language](#)," and that it include "a clear and representative full-size example of each type of advertisement that may be delivered; [and] a truthful statement of the frequency with which each type of advertisement may be delivered . . . ."

That makes a lot of sense: The user can see firsthand what he or she might be getting on a regular basis if she agrees to the license agreement.

### **Another Critique: Will Enforcement Provisions Lead to Frivolous Litigation?**

Another critique claims that the Utah law will lead to too much frivolous litigation - as plaintiffs' lawyers sue innocent companies on behalf of websites or trademark owners.

However, this fear alone seems a very poor reason for Utah to fail to take action to address spyware that was violating consumers' privacy, violating business's rights to their own websites, and annoying many (if not virtually all) who were exposed to it.

Whether this fear will be realized, remains to be seen. But even now, it's important to note that the Act doesn't exactly open the floodgates to litigation. Rather, web site owners, trademark or copyright owners, or web site advertisers who are adversely affected by a violation under the Act are the only parties who may file a suit. Consumers cannot bring suit - they may only lodge complaints.

Finally, the requirement that websites demonstrate the harm caused to them by a given violation of the Act further reduces the risk of frivolous lawsuits.

For all these reasons, a close examination of industry and other critiques of Utah's new Spyware Control Act shows them to be unpersuasive. Utah should be lauded for leading the country in an important new area of legislation on a topic that has crucial consumer privacy implications.

---

*Anita Ramasastry is an Associate Professor of Law at the University of Washington School of Law in Seattle and a Director of the Shidler Center for Law, Commerce & Technology.*