

Pop-up foe targeting trespassers ; Attorney Shawn Collins employs novel legal twist in federal lawsuits attempting to block spyware from infesting personal computers

[Chicagoand Final Edition]

Chicago Tribune - Chicago, Ill.

Author: Eric Benderoff, Tribune staff reporter

Date: May 7, 2006

Start Page: 1

Section: Business

Text Word Count: 1513

Document Text

He's been using a computer for only a year, but 48-year-old Shawn Collins wants to accomplish what the software industry has failed to do: stop annoying pop-up ads and spyware from intruding into personal computers.

The Naperville attorney considers spyware to be akin to cyberwaste.

"The Internet is being polluted," he said. "I look at spyware companies as industrial polluters."

So with his background in environmental issues, Collins is applying to the Internet the same kinds of laws he used against groundwater polluters. In a case settled in February, he successfully argued that spyware companies were trespassing on personal property, a tactic lifted from environmental law.

Because spyware companies typically bundle spyware with other programs, such as games or a screensaver, users often do not realize they have agreed to download the software. Spyware code can create numerous problems, ranging from incessant pop-up ads that clog a computer to programs that monitor a user's keystrokes, providing thieves a way to steal personal information.

"We attacked it as if someone was coming on your property without your permission," Collins said. And they were "staying there without your permission and doing surveillance on you without your permission."

So far, the computing industry has not been very aggressive in battling spyware.

"The way we've gone after spyware companies is by complaining to the Federal Trade Commission by saying they are using unfair and deceptive practices. Basically, that they are committing fraud," said David McGuire, a spokesman with the Center for Democracy and Technology, a Washington-based industry group that coordinates anti-spyware campaigns. "In some cases the FTC has gotten some favorable settlements."

In the meantime, Collins is helping to shape Internet case law.

"There's nothing charted in these waters," he said. And he is getting some kudos for his efforts.

"I like his [Collins'] approach. I think it is novel," said Michael Overing, an adjunct professor at the University of Southern California and a lawyer specializing in Internet issues.

On Friday, Collins filed his third suit in federal court in Chicago using trespassing laws. He claimed that Ebates Shopping.com Inc. downloaded software onto a client's computer to track his Internet behavior. Ebates is an Internet company that refers people to online retailers in exchange for a commission. Ebates did not respond to questions on Friday.

How did Collins go from fighting polluters to fighting pop-up ads?

Collins, a father of three who graduated from the University of Chicago Law School in 1986, acknowledged that he is often the butt of jokes at his firm because of how little he knows about technology. "I'm a very unlikely pioneer, to say the least."

But the computer newbie said David Fish, an associate at The Collins Law Firm, urged him to take a close look at how

problematic spyware had become.

"I did a Google search for some cases and started getting all these pop-ups," Collins said. "I started to see what Fish was talking about, how this stuff can slow down computers."

And he began to see the clutter gathering on his computer like contamination of a resource like groundwater.

"I saw the Internet as a common resource that everyone had access to, and this common resource was being polluted," he said.

Old English law

In the February settlement of the case *Sotelo vs. Direct Revenue*, Collins dipped into law history books to argue spyware providers were trespassers. The trespass-to-personal-property argument is based on "a 1,000-year-old law we inherited from the English," he said.

Collins has used that law in six pollution cases since 2000. He won three and lost one; two are pending. Even in the case he lost, Collins obtained a \$2 million settlement for his clients.

"But the main thing that changed" in each case, he said, "is that the people have clean water. Similarly, we're looking for a clean Internet."

Attorneys for Direct Revenue tried to have the trespass approach thrown out, but U.S. District Judge Robert W. Gettleman allowed the argument. He wrote in an opinion that "elements of trespass to personal property—interference and damage— ... may be asserted by an individual computer user."

In the settlement, Direct Revenue did not admit to wrongdoing. However, it agreed not to install software on a computer without a user's consent, not to collect personal information on users and that it will help users remove the software.

"To date, it is the most comprehensive prohibitions anyone agreed to in a federal court," Collins said. If Direct Revenue violates the agreement, it can be found in contempt of court.

In an e-mail, Direct Revenue called the settlement "fair and reasonable." The agreement, the e-mail stated, embraces "the basic tenets of Direct Revenue's current consumer policies."

The company "absolutely does not promote spyware," and "we support the efforts of those who seek to eliminate spyware from the Internet," the e-mail said.

One aspect of the settlement should make Internet advertisers nervous.

"Advertisers can be sued if they know what the spyware companies are doing," Collins said. "You have to prove the advertisers have knowledge, but it's difficult for me to believe they would not know."

Collins' firm is researching companies to target.

"It's the real pressure point" of spyware cases, he said. "Spyware people live in the shadows. They don't have a reputation they care about.

"So we'll go after the big companies. Advertisers can't bury their head in the sand," he said. "If legitimate advertisers refuse to play with the spyware companies, then the jig is up. We want to go after the biggest companies we can find. The point needs to be made."

Companies have several options when it comes to advertising online. They can buy ads on Web sites or use search engine queries to target customers, among other things.

But many firms also buy ad placements from companies that track a user's online activities, sending ads that pop up on a computer when certain Web sites are visited. There are legitimate companies in this area and others that implant spyware on a computer to aggressively generate pop-ups. The reason: The more ad impressions, the more money for the company that facilitated the ad.

"You have highly motivated people behind this problem," said Dave Cole, director of security response for Symantec Inc. "They are making a lot of money installing this on computers."

Deals between a spyware company and an advertiser can be difficult to unravel. In general, an advertiser makes an arrangement with a marketing company to place ads across the Internet. The marketing company, which could be a spyware provider, gets paid when a user clicks on an ad.

Affiliate deals

But a marketing company can make additional agreements with software distributors and affiliate companies, which could include firms that place spyware on a computer. Those additional companies also get a percentage of money if an ad is clicked.

It is conceivable advertisers do not know about those other agreements, according to security experts, who say spyware has escalated because affiliate programs have gotten out of hand.

While spyware can be installed on a computer without a user's consent, users often click on a licensing agreement before the software is downloaded. Critics claim the agreements can be misleading and don't include instructions for removing the software.

Indeed, in the Sotelo case, it was difficult to prove how much plaintiff Stephen Sotelo of Lemont knew about the user agreement he accepted. That was one reason it was settled without monetary damages.

Overing, the USC Internet law professor, said he was surprised Judge Gettleman allowed the argument.

"It works to a point," he said. "The argument on the other side is that you left your doors and windows open and let me peek in," referring to the notion that people regularly allow companies to put "cookies" on their computers. Cookies are small files that hold personal information about the user that are used to speed up the loading process when a person visits a Web site frequently.

Nonetheless, Collins is using the trespass argument in a case filed in September that could be another first for the law firm: determining whether victims of spyware can band together as a class.

The suit against 180solutions Inc. is in the discovery stages.

"With Gettleman approving the theories, you can win a case," Collins said. "But can people sue collectively? If the court says yes, anyone can be part of the class."

In the suit, Collins alleges 180solutions infected more than "20 million computers and has business relationships with more than 6,000 advertisers, including dozens of Fortune 1000 companies."

Steve Stratz, a spokesman for 180solutions, agreed the company's software is found on 20 million computers, but said it is not a spyware firm because customers have allowed the software to be downloaded.

"We have gone through rigorous testing to make sure our customers know what they are downloading," he said. "We believe the case is completely off base."

ebenderoff@tribune.com

Reproduced with permission of the copyright owner. Further reproduction or distribution is prohibited without permission.

Abstract (Document Summary)

"It works to a point," he said. "The argument on the other side is that you left your doors and windows open and let me peek in," referring to the notion that people regularly allow companies to put "cookies" on their computers. Cookies are small files that hold personal information about the user that are used to speed up the loading process when a person visits a Web site frequently.

