

For FTC, e-commerce means managing 'mice'

Only on the Internet could a site hawking dancing hamster animations, accompanied by hamster-sung harmonies, be paid advertising royalties from corporate giants like Wal-Mart and American Express. But the future earning power of the darlings on Hamsterdance.com could be slowed by a few bad "mice."

To Peter Swire's eye, the Internet's problem of consumer confidence is zoological. The senior fellow at the Center for American Progress breaks down e-players as either elephants -- hulking powerhouses like Amazon.com and eBay -- or mice -- disparate, small-scale and barely visible.

Swire was among a group of experts who spoke earlier this week at the Center for American Progress on the Internet and consumer protection.

According to a bevy of experts including a veritable Who's Who of past FTC leaders, it's creative solutions to harness these mice that the Federal Trade Commission needs to create when it convenes in November for a series of hearings on the future of consumer protection and the Internet.

"I call them Rodents of Unusual Size because they hide under the radar screen," said Ari Schwartz, deputy director for the Center for Democracy and Technology. Schwartz cited CoolWebSearch, a particularly obnoxious form of browser-hijacking spyware, as one example of the "multi-multi-million dollar business" that is Internet fraud.

CoolWebSearch is a particularly good example of Swire's mice-run-amuck because it is as prevalent (it may exist on half of the PCs over six months old) as it is insidious (the code changes daily, making it nearly impossible to block by programming methods alone.)

What the experts don't agree on is how to combat these malevolent mice. Several themes, however, do appear to be gaining traction four months before the hearings.

For Federal Trade Commissioner Jon Leibowitz, breaking down walls between the FTC and other government agencies would go a long way toward attacking fraudulent operations that often originate -- like 75 percent of the spam in one's inbox -- outside the United States.

"The world is getting smaller, and that's a good thing to be sure, but it's not unusual for a scammer living in Canada to have a bank account in Cypress and sending spam through servers in the Dominican Republic. We've got to be able to work with our sister agencies in order to share information, but an anomaly in the law prevents us from sharing that confidential information," Leibowitz said.

These concerns would be rectified under the Safe Web Act, Leibowitz added, which has already passed the Senate and will soon be taken before the House.

While information may lead to more accurate targeting of "fraudsters" or, in their data-collecting iteration, "phishers" -- such as the Nigerian check-cashing scandal or fake e-mails from one's bank -- government officials want the ability to levy civil penalties without giving up speedy punishment. And because the FTC often surrenders its fining capabilities for rapid prosecution, "we can go fast or we can get penalties, but we can't do both at the same time," Leibowitz said.

But for civil penalties to be even remotely effective, the language of the current law would need to be altered considerably.

"One of my core complaints with civil penalties is that one of the statutory criteria that a court must consider in civil penalties is to preserve the companies' ability to continue in business. If you caught a phisher that is exactly the wrong thing to do," said Howard Beales, former director of the FTC Bureau of Consumer Protection.

While prosecuting malevolent actors is important, one former FTC official felt that empowering individuals would go just as far.

"We need legislation that mandates notice and consent. I'm not sure what it's all about, but when people buy on the Internet they should know what's going to happen to the information that they provide and they should be able one way or another to opt out. I'll never forget Senator McCain saying at a hearing that 'I spent all day yesterday trying to opt out of Yahoo! and I never could find it,'" said former FTC Chairman Robert Pitofsky.

Interestingly, some consumers have taken awareness of the problem to a new level by hunting the programs themselves.

"I follow a dozen spyware blogs and there are people who hunt these things. The zealots are there. I don't know when these people eat, but they are already spending their full time researching the ills of big companies and small companies alike," said Jules Polonetsky, vice president of integrity assurance at America Online.

Calling privacy statements, at least currently, "worthless," Beales stressed the importance of authentication and information exchange in buttressing consumer confidence.

"The core problem is anonymity," Beales said. "We need to think of better ways to authenticate who you're dealing with or this is going to be an online market limited to large players who can put something at stake."

"The way to avoid the fraud problem is exchange of information. There's very sophisticated analytical tools to do that, but they depend on getting information that in any strict sense isn't a part of the transaction but that they determine" that neither party to a transaction is a bad apple, Beales said.

Every expert felt that any regulation would need to be weighed against inflicting rules upon all parties that would stymie the explosive growth of e-commerce.

"Very strict legislation to put the elephants and mice in the cage and put the zookeeper there with a whip. The other side is to let the elephants and the mice work it out and clearly there's murder and mayhem in between there. It's an interesting balance," to be struck, Polonetsky said.

The FTC's hearings will be held Nov. 6-9, with the first three days devoted to the public and the last day reserved for government and law-enforcement officials. The forum will be held at George Washington University.

Copyright 2006 by United Press International

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.