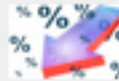




Gallery: Tech's Most Powerful Women




Gallery: 28 Dirt-Cheap ETFs



Gallery: 10 Health Care Stocks To Buy



America's Best Small Companies



Free Issue >

Editor's Picks

Live Stream | Topics | Contributors | **Headline Grabs**

# Firesheep Users May Be Breaking the Law

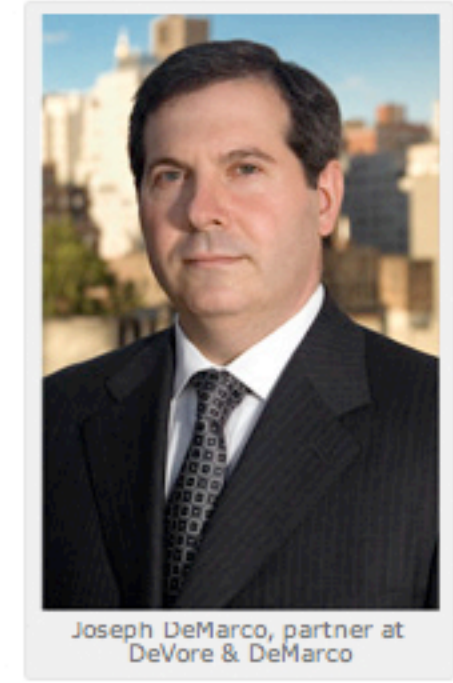
Oct. 28 2010 - 12:45 pm | 1,283 views | 0 recommendations | 0 comments

When the media report on some wild new privacy-invading tool, it's tempting to rush out and try it. This week brought reports of two such tools: [Firesheep](#), a WiFi hacking tool, and the Secret SMS Replicator, an Android app for secretly forwarding texts from someone else's phone.

After the [New York Times Bits](#) blog reported on the Android app, I wondered about the legality of such an application given that it sounded quite a lot like wiretapping. Hours after the Bits post went up, Android quickly [pulled the app](#) from its market.

Firesheep, has not been pulled down, though. Created by a freelance software developer to help expose a major security flaw on most social networking websites, it's a Firefox extension that you can download and use to tap into the unencrypted browsing sessions of other surfers on an open WiFi network. So if you and a Firesheep user are in a coffee shop together taking advantage of free wireless and you visit a non-encrypted version of Facebook, the Firesheep user can hop into your account and take a look around.

This has intrigued many Internetters. The extension has been downloaded over [380,000 times](#). Many of my friends have pinged me saying they've tried it out and can't believe such a thing exists. My response to them: "Don't use it; you may be breaking the law."



communications in real-time — it's unclear if that law applies to computer communications. "Whether the Wiretap Act is violated largely depends on whether the captured cookie is considered a 'communication' — an issue which is unclear under existing federal case law," says DeMarco.

The legality of using Firesheep is less woolly when it comes to the Computer Fraud and Abuse Act, which criminalizes accessing computer systems without authorization.

"The actual use of Firesheep may or may not be unlawful, depending on the facts. For example, many system administrators may have legitimate reasons to use the software," says DeMarco. "However, individuals who use the extension to access the accounts of others without those persons' knowledge or consent are almost certainly violating the computer trespass provisions of the Computer Fraud and Abuse Act and are also potentially engaging in an unlawful data tap."

So, to those 300,000 newly anointed [amateur hackers](#) out there, just because you can easily hack into people's Web browsing with Firesheep doesn't mean you should, and doesn't make it legal.

As for why Butler may not get into trouble for initiating all these new hackers, DeMarco says his intent matters. "If the author intends that the software will be used for illicit purposes, his conduct may be criminal under broad and well-established principles of accomplice and/or conspiratorial liability," says DeMarco. That was not Butler's stated intent.

As for why there's no law directly applicable to the distribution of hacking tools, like the Web with its security flaws, the law has technology flaws.

"It is unlikely that Congress will enact an express prohibition against the creation or distribution of computer hacking tools for two reasons. First, there is no well-settled definition of what constitutes a 'hacking tool.' Software which is used by network administrators in the course of their jobs may be used for nefarious purposes by those with the desire to abuse them," says DeMarco. David Barksdale, the Google engineer canned for abusing his access to users' accounts, is an [example of that](#).

"Second, the rapid evolution of security threats would likely render such a law obsolete almost as soon as it is adopted," DeMarco continues. "Experience has shown that legislation has had tremendous difficulty keeping up with emerging technology on the Internet; indeed, although they have from time to time been amended, the two most salient pieces of federal legislation in this area — the Computer Fraud and Abuse Act and the Wiretap Act — were passed decades ago."

In the meantime, [Boing Boing](#) has advice for how to avoid having a herd of Firesheep users silently sneaking into your open WiFi surfing.



Just because hacking is made easy doesn't make it legal

submit

5

Share

27

tweets

retweet

## MY ACTIVITY FEED

Show all activity

☒

KASHMIR RECOMMENDS

2 minutes ago

The Politics Of Stewart's Rally: It's The Money, Stupid

by JEFF BERCOVICI

☒

KASHMIR RECOMMENDS

4 minutes ago

How To Screw With Firesheep Snoops? Try FireShepherd

by ANDY GREENBERG

☐

KASHMIR'S HEADLINE GRAB

Yesterday

Americans Maximize Social Network Security

INFORMATIONWEEK.COM

☒

KASHMIR RECOMMENDS

Yesterday

Behind The O'Donnell 'One-Night Stand' Story

by JEFF BERCOVICI

☐

KASHMIR CALLED OUT

Yesterday



## MOST POPULAR

MY POSTS	All Posts Last 24 Hours	
1.	The Privacy Landmine That is Duke Graduate Karen Owen's 'Senior Thesis'	92,626 views
2.	How Karen Owen and Tyler Clementi Lost Control	55,284 views
3.	Tyler Clementi Turned To A Gay Message Forum For Help Before His Suicide	24,941 views
4.	The Geek Squad Becomes the Porn Squad	17,989 views
5.	The Dirty Refuses To Give Erin Andrews Her Privacy	17,531 views

## ABOUT ME

I'm a privacy pragmatist, writing about the intersection of law, technology, social media and our personal information. If you have story ideas or tips, e-mail me at [khill@forbes.com](mailto:khill@forbes.com). I've hung out in quite a few newsrooms over the last few years. Most recently, I was an editor at Above the Law, a legal blog. In the past, I've been found in midtown Manhattan at The Week Magazine, in Hong Kong at the International Herald Tribune, and in D.C. at the National Press Foundation and the Washington Examiner. I have few illusions about privacy — feel free to follow me on Twitter: [kashhill](#). Or friend me on Facebook... though I might put you on limited profile. [See my profile »](#)

Followers: 92

Contributor Since: August 2010

Location: New York, NY

MY PROFILE

MY RSS FEED

MY HEADLINE GRABS

EMAIL ME TIPS

+ FOLLOW ME

## WHAT I'M UP TO

### Past Work

You can check out my digital dossier here at Forbes or previously at Above The Law. In addition, these are some of the magazines and newspapers that I've written for:

- The Washington Post
- Washingtonian Magazine
- Time Out New York
- The Orange County Register
- The Washington Examiner
- Assembly Journal
- Next American City