

# Exhibit G

Sponsored by:

**NETWORKWORLD**

This story appeared on Network World at  
<http://www.networkworld.com/columnists/2007/053107-backspin.html>



## Ameritrade leaks and more Wi-Fi theft

[Backspin](#) By [Mark Gibbs](#), Network World, 05/31/07

First of all, there is something that I meant to discuss a few weeks ago that surprisingly has not gotten much coverage. Art Medlar, a fellow inhabitant of a mail list I subscribe to explained that he is a client of [TD Ameritrade](#), and being a cautious kind of guy he used unique primary and alternate e-mail aliases for his account.

He wasn't happy when "[within] a month, both of these addresses were receiving stock-pumping spam. I called [Ameritrade] and had a nice heart-to-heart with a clueless and unconcerned [customer service representative] and changed the addresses [to different e-mail aliases]."

Medlar was even less happy when "[last] week, these two began getting stock spam. None of them have ever received any other sort. They have never been used except where entered on the Ameritrade profile form. The Ameritrade guy this morning says that it's obviously a dictionary spam at all possible addresses [like those I used]."

To say that this was disingenuous on Ameritrade's part would be kind. Medlar commented that "it looks like the people running these scams are pretty serious and have connections of one sort or another inside at least one business which should be very secure but is not."

A recent [Slashdot](#) article discussed more or less the same experiences of Bennett Hazelton, a well-known privacy and anticensorship activist. The implications of this for Ameritrade are . . . what is the word I'm looking for? Ah yes. Huge. This is a story that has, as we say, "got legs." Stay tuned.

My other topic this week is a follow-up regarding last week's column on things legal and the issue of unauthorized Wi-Fi access stirred up some interesting comments.

Reader Peter Quirk in Hopkinton, Mass., asked: "Thanks for highlighting this unintended consequence of security legislation. I wonder whether we will soon be subject to power theft suits for plugging laptops or cell phone chargers into the very few available power outlets in airport lounges."

I've wondered about this for years. We all go into Starbucks or we're waiting in the airport lounge for our flight to be cancelled and the first thing we do is plug in to the first power outlet we can find with nary a care in the world. Why is it that using AC power (which has an easily quantified and real cost) without explicit permission is apparently OK while using an unsecured, uncontrolled Wi-Fi access point at a cost that could be measured in nanocents — no, femtocents — is something that is worthy of arrest and prosecution?

Reader Vinny Fasano of Huntington Station, N.Y., was amazed when he read about the case I discussed in BackSpin: "Perhaps I'm missing something here, but I seem to remember during the course of my studies that the airwaves are owned by 'the

people' — if you choose to put something out for broadcast (and yes, I would certainly consider a non-point to point, non-encrypted radio transmitter 'broadcast'), how can you possibly be prosecuted for using it?"

Fasano continued: "Since I apparently don't have the moral compass of a number of your bloggers, when I'm traveling with my PDA I'll routinely search for a Wi-Fi hot spot to check my e-mail."

I suspect the blogger Fasano was referring to was Anonymous writing on Gibbsblog who declared that: "what bothers me most about the alleged action mentioned in the second-to-last paragraph of your article -- you or anyone finding '... an open access point we would probably use it...!' I would not use it! It is just plain wrong, no matter how you justify it!"

Another blog contributor, Lawson, pointed out that if "... [you] use your laptop in a part of the house or property where the neighbor's unsecured Wi-Fi with same router setup is the stronger signal [you could unknowingly] connect to their setup rather than your own. By the logic of the current law you are now hacking and liable for prosecution." I love that!

I was discussing the whole unauthorized Wi-Fi issue with Mrs. Gibbs, who raised a very interesting question: What if a teenager were to use an unsecured wireless access point to browse porn? Could the access point owner not be considered to be liable in a similar way that Amero was found guilty of four counts of risk of injury to a minor and impairing the morals of a child?

All contents copyright 1995-2007 Network World, Inc. <http://www.networkworld.com>