ACCOUNTING

Reining in The Internet

Online Exclusive Column

Feb. 18, 2011

Not since the automobile has any technology so confounded law enforcement officials that they resorted to full-scale assaults on the constitution in order to keep pace with the bad guys.

When the automobile first appeared at the beginning of the last century, law enforcement agencies could not keep pace with their horse-drawn wagons, and could not afford to invest in the new-fangled machines. So they resorted instead to attempts to have automobiles banned. Or limited in speed. Or otherwise crippled so they could not outrun the sheriff.

They are in the same bind today with the Internet. The tools that helped to thwart organized crime 60 years ago don't work with the Internet. Virtual Private Networks shield data from investigation. Services like Skype automatically encrypt phone conversations, rendering them immune to wire taps. Emails can be easily encrypted, as can hard drives, folders and documents.

I am sympathetic to the plight of our officers. They are caught between the bad guys, a desire to protect the public and a technology deck that seems stacked against them. But I am not willing to level the playing field by allowing local, state and federal officers to toss the Fourth Amendment to the Constitution into the scrap heap. You know, the part about being secure in our persons, houses, papers and effects.

In the past two years, the U.S. Department of Justice (DOJ) has mounted a concerted campaign to force Internet Service Providers to retain everything about everyone online for a period of two years, just in case they might ever want to sift through this data looking for a crime. There are lots of things wrong with this scheme, not the least of which is that it doesn't work. That's the judgment of the European Union, which tried this scheme and found that it didn't have much impact on crime fighting.

Nonetheless, the DOJ is back before Congress this year, asking for a data retention law for Internet Service Providers. And also an ability to hack into encrypted phone calls. The White House, even more ambitiously, wants the ability to shut down the Internet entirely if it deems a national emergency so requires.

I would be less skeptical of giving the government such powers if they had a good record of responsibility when it comes to the Internet. But they don't. In fact, the record is one of blunders, bad information and worse intentions.

It's not just the infamous "SunDevil" operation, in which the FBI arrested the wrong people. Or the dozens of "National Security Letters" illegally issued in the past few years to pry into Internet records. It stretches right up to this month, when the Department of Homeland Security (DHS) acted to shut down 84,000 websites it claimed were violating copyright and child pornography laws. Oops ... no, they were not.

The DHS seized control of the 84,000 websites, most of them belonging to small business, and replaced them with the notice that the operators of the sites were child pornographers. Even though they seized the sites with no evidence whatsoever.

I am a law-and-order kind of guy. And as I have often stated, any law enforcement officer who taps my phone calls or views what I browse online would be at serious risk of being bored to death. My emails lean toward corny jokes and tech news, not high crimes and misdemeanors.

But I am also mindful of Ben Franklin's adage that "Those who would sacrifice freedom for security deserve neither."

This isn't some theoretical or philosophical discussion. Any accountant who is using hosted accounting solutions, stores data in the "cloud"

or communicates without encrypting their data risks having that data misused. Or worse, having their clients falsely accused of vile crimes.

So what is the balance we should seek between security and freedom? In my mind, it begins with better technology for law enforcement. The fact that the FBI last year scrapped and wrote off its brand-new, $150 million computer system as a failure is a good indication that something is awry with IT for law enforcement. It also begins with more education and training for law enforcement officers at every level. If the criminals are trading horses for automobiles, so should our peace officers. Same with computer systems and the Internet.

And it ends precisely at the point where the needs of law enforcement conflict with the Fourth Amendment.

Reality Check

A compendium of ideas, products, rants and raves from the viewpoint of the author. Not that the author has no financial interests in any of the products mentioned. Feel free to disagree, or to share your ideas by sending them to davemcclure@cpata.com.

Internet Site of the Month: Internet Explorer 9. (http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/home).
If you have not yet upgraded to this new version, now is the time — even if it is still in beta. The version offered here is stable, interesting, faster and better ... and will be automatically updated when the final version is released.

> **Internet Explorer 9.** Microsoft is in the process of releasing this most recent version of its popular browser, designed to be the fastest and easiest browser to date. It offers support for the new HTML5 language, which enhances security because of the ability to turn off Active-X support — long the source of hacks of the browser.
>
> **Phony**
> **Broadband Use Rates.** According to the U.S. government, use of broadband grew by a whopping 5 percent last year — a near-miraculous feat in a year of galloping recession. How did this happen? Well, mostly by fudging the numbers. By including the decidedly not high-speed mobile phone data

use
in the mix, they are able to show growth when virtually none occurred. Broadband
over a cell phone is still not of sufficient speed or quality to make a meaningful
browsing experience, and the data should not be mixed.

**Watson's
Win On Jeopardy.** So a computer wins over a human at answering questions
on Jeopardy ... what did you expect? Answering trivia questions is really not much of an achievement, even with the bells and whistles of adapting to
a human interface. It was fun to watch, but the outcome was never really in doubt. Now show me a computer that appreciates a sunset, and I'll be impressed.

High-Tech Toilets. The Japanese are different from Americans, if
in no other way than their love of high-tech gadgets in the toilet. Their toilet bowls include such features as ion-odor control sprays, remote controls,
music, and video games you can play with your urine! Last year a musical tribute
to clean toilets hit the Japanese best-seller lists. Sigh! There are some tech trends I can live without experiencing.

Gaming consoles. I love video games on the PC. Doom, Quake,
Halo and Duke Nuke'm are all favorites, though I don't have the
time I once did to indulge in them. Game consoles have been of lesser interest,
due to the additional cost of both the equipment and games. That's changing,
though, as the Wii, X-Box and Play Station evolve out of mere gaming and into
the realms of Internet browsing and movie downloads. I'm not yet ready to shell out the better part of $500 for one, but I am thinking about it.

Portals • Practice Management • Product & Service Guide • SaaS Accounting • Technology • Skype • News • Internet Security

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.