MIGNOLET

BUSINESS RESEARCH CONSULTANTS, INC.

Cybercrime, Ferraris, and On Star Bugging

Cybercrime & Ferraris

Are you being bugged in your car?

For more than three decades Jean Mignolet has served in law enforcement and private investigation, managing all aspects of general investigative business. She specializes in in-depth background investigations, and is the top choice of attorneys, corporations, small business owners and individuals who require all types of investigative services.

For further information visit: www.Mignolet.com

Contact us at: investigators@Mignolet.com or call us at: 954-523-8737

Quick Links

Jean,

What do Cybercrimes, Ferraris, Cellphones and On Star Bugging of our conversations have to do with one another? It's basically called no privacy for us and the cyber-criminals are out in full force.

You can read more here in this month's issue of our newsletter and believe me, it's an eyeopener.

Imagine being offered a huge bonus for finding ways to steal from the company you work for, or a prize for the best detriment to society that you can think of...it's not hypothetical anymore. It's real.

Likewise you believe your conversations in your car that has On Star is a safe haven to talk about anything you want without anyone listening in. Incorrect! Wrong again. Even that is gone. Read on and learn about the newest and most sophisticated ways that the FBI and the government know whether or not you are heading out to buy shoes or destroy a building.

Something to think about.

Cybercrime boss offers a Ferrari for best online scam

The head of the European Cybercrime Centre (EC3) found out that a top cybercrime boss offered a Ferrari to the person who came up with the best online scam. Yes, go ahead; read it again because we know it's unbelievable.

A bit like "employee of the month" promotions this one featured a Ferrari and a Porsche. They added a couple of leggy blondes in the mix and this clip was off and running. The guy in the clip says: those who make the most money can get this car".

Mr. Oerting, who is currently acting Head of Europol's Counter Terrorism and Financial Intelligence Centre, said that 85% of cybercrime now originates in Russian-speaking countries - an area where law enforcement has typically found it

Jean Mignolet

A reminder that prior issues of the newsletter are view-able from my website.

Cellphones & On Star Bugging our Conversations

You may be familiar with the interview of Edward Snowden by Brian Williams in which Snowden said that this cell phone bug was brought up as one of the techniques used by the NSA for intruding upon our privacy.

Two alleged mobsters, John Ardito and his attorney Peter Peluso, had Nextel cell phones and the FBI listened in on their nearby conversations. Ardito is considered one of the most powerful figureheads in the National Mafia so in this case maybe that's a good thing but is it good for us?

U.S. District Judge Lewis Kaplan ruled the ***roving bug*** legal because federal wiretapping laws are broad enough to permit such eavesdropping.Judge Kaplan's opinion said that the eavesdropping technique "functioned whether the phone was powered on or off."This is the first time this technology has been used but there were conversations for a long time before this actually happened.

The U.S. Commerce Department's security office warned that **"a cellular telephone can be turned into a microphone and transmitter for the purpose of listening to conversations in**

challenging to prosecute those responsible for attacking Western targets. That's not only annoying it's frightening.

Mr. Oerting spoke of the difficulties of bringing booking cyber criminals:

"They are very, very good at locating themselves in jurisdictions that are difficult for us. If we can pursue them to arrest, we will have to prosecute by handing over the case. Even if they will do it, it's a very cumbersome and slow process. You can wait until they leave the country, then get them. That's a comparatively small volume. The police ability stops at the border. We are also seeing signs of movement to African countries when the broadband is getting bigger. We will probably see more from places we don't want to engage with."

He also warned of a two-tier Europe in which the wealthy can pay to protect themselves, while the less fortunate are unable to afford protection. This makes them vulnerable to identity theft and other online crimes.

"We have 28 different legislations but we

the vicinity of the phone."

Additionally, cell phone providers can "remotely install a piece of software on to any handset, without the owner's knowledge, which will activate the microphone even when its owner is not making a call". There is no privacy as Edward Snowden mentioned in his interview, while most of us believe that we have nothing to hide, the collection of such data, if misread, may lead to unfair consequences.

It seems that Nextel and Samsung handsets and the Motorola Razr (is that still out there) are most vulnerable to such software downloads. James Atkinson, a counter-surveillance consultant who worked very closely with the government agencies stated:

"They can be remotely accessed and made to transmit room audio all the time," he said. "You can do that without having physical access to the phone."

Let's face it, modern phones are miniature computers, and downloaded software could modify the usual interface that always displays when a call is in progress. The spyware can easily place a call to the FBI and activate the microphone without the owner knowing it happened. Unfortunately the FBI is not commenting on this.

Big corporate heads often remove their batteries from their cell phones and those aware of this do the same.

"In July 2003, Ardito and his crew discovered bugs in three restaurants, and the FBI quietly removed the rest. Conversations recounted in FBI affidavits show the men were also highly suspicious of being tailed by police and avoided conversations on cell phones whenever possible."

Snowden lives in Russia because he can't come home, and the reason as we know it, is because he wanted the public to know that their information can be, has been, and is being and will probably always be "captured" for *intelligence reasons.* The laws that relate to this are so broad that the public basically has nothing to stand on.

The bugs work anywhere in the United States. Intelligence agencies employ the remote-activation method and have done

have one new crime phenomenon. If you're rich you live in a nice place with a fence around it with CCTV, but if you're poor. ... On the internet, some will be able to protect, some will not", said Oerting.

Online criminal gangs recruit very seriously. They source young programmers from universities so they get the top of the crop. With the offerings of flashy cars who knows how far global cybercrime bosses will go to get the best techies out there.

There was a case in which five debit cards were purchased for $500. Each had a fixed withdrawal limit, however; the gang was able to convert them into credit cards which had no blocks on them. They then cloned the cards and over a few hours stole approximately $45 million from card machines all around the world, with Britain losing billions of pounds yearly.

"In real cybercrime, [we're going after] the people who develop and distribute the malware. We are trying to find them and identify them. It's like cutting the snake's head off. But

so since 2004. "A mobile sitting on the desk of a politician or businessman can act as a powerful, undetectable bug...enabling them to be activated at a later date to pick up sounds even when the receiver is down."

In his interview, Snowden was adamant about the amount of data that can be taken in this manner and says it is equal to other techniques and intrusions upon the privacy of the American People and our Constitution.

The FBI can also set key loggers onto a computer so they can detect each and every stroke on the keyboard that one makes." *Roving bugs"* are legally permitted to capture hundreds of hours of conversations when law enforcement obtains a court order when alternative methods have either been attempted or aren't possible. Private investigators may NOT obtain these orders.There is "no law that would allow me as a private investigator to use that type of technique," ..... it is not legal in the private sector."

This isn't new but Snowden brought it out to the public . There was even a lawsuit in 2003 in which the FBI was able to surreptitiously turn on the built-in microphones in automotive systems like

General Motors' OnStar to snoop on passengers' conversations and the passengers were unaware!

Malicious hackers have followed suit, and Snowden referred to this as well, there have been cases before today. A man who wrote a Trojan horse that secretly activated a computer's video camera and forwarded him the recordings was arrested in Spain. TIP: WHEN YOU HAVE A CAMERA ON YOUR LAPTOP OR PC COVER IT WITH BLACK TAPE FOR EXTRA SECURITY. Often we use our equipment when at home and we are in very "casual situations".

As we always say. BE DILIGENT...at least as diligent as is allowed.

there are a lot of heads, and they grow back very quickly. Organized crime has not just embraced this but integrated cybercrime into its business."