iPhone makes great snitch for savvy cops

September 1 2010, By Amber Hunt

Got an iPhone in your pocket? Then you might be storing even more personal information than you realize. And some of it could be used against you if you're ever charged with a crime.

A burgeoning field of forensic study deals with iPhones specifically because of their popularity, the demographics of those who own them and what the phone's technology records during its use.

Law-enforcement experts said iPhone technology records a wealth of

information that can be tapped more easily than BlackBerry and Droid devices to help police learn where you've been, what you were doing there and whether you've got something to hide.

"Very, very few people have any idea how to actually remove data from their phone," said Sam Brothers, a cell-phone forensic researcher with U.S. Customs and Border Protection who teaches law-enforcement agents how to retrieve information from iPhones in criminal cases.

"It may look like everything's gone," he said. "But for anybody who's got a clue, retrieving that information is easy."

Two years ago, as iPhone sales skyrocketed, former hacker Jonathan Zdziarski decided law-enforcement agencies might need help retrieving data from the devices.

So he set out to write a 15-page, how-to manual that turned into a 144-page book ("iPhone Forensics," O'Reilly Media). That, in turn, led to Zdziarski being tapped by law-enforcement agencies nationwide to teach them just how much information is stored in iPhones -- and how that data can be gathered for evidence in criminal cases.

"These devices are people's companions today," said Zdziarski, 34, who lives in Maine. "They're not mobile phones anymore. They organize people's lives. And if you're doing something criminal, something about it is probably going to go through that phone."

It's an area of forensic science that's just beginning to explode, law-enforcement and cell phone experts said. Zdziarski said the focus of forensics recovery has been on the iPhone over other smartphones in large part because of its popularity.

An estimated 1.7 million people rushed to buy the latest iPhone version

released in June. Before that, Apple had sold more than 50 million iPhones, according to company figures.

Although some high-stakes criminal cases have used cell phone towers to estimate a suspect or victim's whereabouts, few have laid out the information that iPhones have to offer. For example:

• Every time an iPhone user closes out of the built-in mapping application, the phone snaps a screenshot and stores it. Savvy law-enforcement agents armed with search warrants could use those snapshots to see if a suspect is lying about whereabouts during a crime.

• iPhone photos are embedded with GEO tags and identifying information, meaning that photos posted online might not only include GPS coordinates of where the picture was taken, but also the serial number of the phone that took it.

• Even more information is stored by the applications themselves, including the user's browser history. That data is meant in part to direct custom-tailored advertisements to the user, but experts said that some of it could prove useful to police.

Clearing out user histories isn't enough to clean the device of that data, said John B. Minor, a communications expert and member of the International Society of Forensic Computer Examiners who has written articles for law enforcement about iPhone evidence.

"With the iPhone, even if it's in the deleted bin, it may still be in the database," Minor said. "Much is contained deep within the phone."

Some of that usable data is in screenshots.

Just as users can take and store a picture of their iPhone's screen, the

phone itself automatically shoots and stores hundreds of such images as people close out one application to use another.

"Those screen snapshots can contain images of e-mails or proof of activities that might be inculpatory, or exculpatory," Minor said.

Most iPhone users agree to let the device locate them so they can use fully the phone's mapping functions, as well as various global positioning system applications.

The free application Urbanspoon is primarily designed to help users locate nearby restaurants. Yet the data stored there might not only help police pinpoint where a victim was shortly before dying, but it also might lead to the restaurant that served the victim's last meal.

"Most people enable the location services because they want the benefits of the applications," Minor said. "What they don't know is that it's recording your GPS coordinates."

Bill Cataldo, an assistant Macomb County, Mich., prosecutor who heads the office's homicide unit, said iPhones are treated more like small computers than mobile phones.

"People are keeping a tremendous amount of information on there," he said.

Cataldo said he has found phone call histories and text messages most useful in homicide cases. But Zdziarski, who has helped federal and state law-enforcement agencies gather evidence, said those elements are just scratching the surface when it comes to the information police and prosecutors soon will start pulling from iPhones.

"There are some terrorists out there who obtained some information

about a network from an iPhone," he said.

Sam Brothers, who works for U.S. Customs and Border Protection and helps train law-enforcement agencies about cell phone forensics, said he also has testified in state and federal cases about data he has retrieved from iPhones.

Although he can't comment about specific cases, he provided a hypothetical case:

"Let's say you have a gang and somebody's killed a gang member on the street," he said. "The killer takes a picture on his iPhone. ... We as law enforcement may retrieve that image and might have proof not only of the death, but the time of death."

Even people who don't take pictures or leave GPS coordinates behind often unwittingly leave other trails, Zdziarski said.

"Like the keyboard cache," he said. "The iPhone logs everything that you type in to learn autocorrect" so that it can correct a user's typing mistakes.

Apple doesn't store that cache very securely, Zdziarski contended, so someone with know-how could recover months of typing in the order in which it was typed, even if the e-mail or text it was part of has long since been deleted.

Apple did not return phone calls or an e-mail seeking comment for this story.

Adam Gershowitz, who teaches criminal procedure at the University of Houston Law Center, said the new technology brings with it concerns about privacy -- especially when it comes to whether investigators have

the right to search someone's iPhone after an arrest.

So far, the courts have treated mobile phones like a within-reach container that police can search the same way they can check items in a glove box or cigarette pack, Gershowitz said, though the Ohio Supreme Court in 2009 ruled to bar warrantless searches of cell phone data.

That case is being appealed to the U.S. Supreme Court.

"Phones are regular tools of the drug trade," Gershowitz said. As police become more familiar with iPhones, they become more adept at flipping through photos, map searches and text messages as they look for evidence.

Zdziarski said some examiners are afraid to touch iPhones because of privacy concerns.

"I personally will never work on civil cases," he said, adding that when he advises law-enforcement agencies about obtaining search warrants for iPhones, he instructs them to add iPhone-specific language to the warrant.

But, he said, as iPhones appear to keep selling in record numbers, law enforcement appears poised to keep up.

"It's no longer about a list of phone numbers and maybe a couple of pictures," Zdziarski said. "You're talking about data that can travel back a year or longer. That's useful to law enforcement."