# Encrypted evidence is increasingly hampering criminal investigations, police say

Not even search warrants make a difference

**BY:** Mark Greenblatt, Scripps News, and Robert Cribb, The Toronto Star
**POSTED:** 3:58 PM, Nov 4, 2015
**UPDATED:** 4:54 AM, Nov 6, 2015

WASHINGTON, D.C. - Barbara Mills, a retired nurse in Baton Rouge, has been tormented for seven months by questions no mother should have to ask: Who killed her 29-year-old daughter Brittney in cold blood, and why is new privacy technology allowed to potentially stop the police from finding out?

Brittney's murder is only one of many serious crimes in the United States and Canada that could go unsolved because Apple and Google are deploying strong encryption on cell phones and messaging applications that even the cops can't break through. The advanced privacy technology, introduced after Edward Snowden revealed the NSA's warrantless surveillance, is designed to keep all prying eyes away from files or messages if the correct password is not used.

In a joint investigation, Scripps News and The Toronto Star have found the very encryption that has become so prized by technology firms and many consumers is also becoming a critical tool for child molesters, drug dealers and other criminals who can hide evidence the authorities say they can no longer access, even with a search warrant. Even a law-abiding citizen who loses a loved one, like Barbara Mills, is now unable to recover files stored on the fully encrypted phones if they didn't obtain their relative's password in advance.

It's a battle being waged between law enforcement in the U.S., Canada and other countries and privacy advocates, with both sides claiming they're trying to protect your safety.  Police agencies contend they are losing critical tools to track and arrest criminals. Privacy

advocates argue that governments around the world have lost the trust of the public, while arguing encryption protects vulnerable groups. They often say that investigators have other tools at their disposal to solve crimes and do not need access to text messages or stored data.

At this stage of the battle, law enforcement is losing. Scripps and the Toronto Star made numerous requests over several months across all levels of government asking for specific cases where investigations were thwarted because of encryption. Law enforcement agencies had many anecdotes, but are just now starting to collect data.

But in Baton Rouge, local authorities have no hesitation blaming Apple's latest encryption for bringing their search for the person who shot Brittney Mills to a near halt. Mills, a single mother who was eight months pregnant with her second child, opened her apartment door late one evening last April. Police believe she knew the killer. She refused to let the still unknown person borrow her car, they believe, and was shot shortly after. Her unborn but nearly full-term baby boy clung to life for a week before dying. Mills leaves behind a daughter, now 10 years old.

Police are convinced clues to the murderer's identity lie inside the victim's Apple iPhone. "She did say she had a diary in her phone and that everything negative that happened to her was in that diary," her mom Barbara said. "If that phone could help solve that case then I think law enforcement and law enforcement alone should be able to go into those phones and access whatever it is they need to access. You have two murders here. Not one, but two."

But like many consumers, Brittney Mills never shared her phone's password with anyone. Baton Rouge authorities obtained her family's permission to look inside of it but could not get past Apple's encryption even after reaching out to the FBI and the Secret Service for help.

"I'm at a dead end right now and I need that information to make sure we fully investigate this case and try to bring justice to this family and our community," East Baton Rouge District Attorney Hillar Moore said.

Compounding the problem, if police or any user enters the wrong password in to an iOS device six times in a row, a message will display saying the device is disabled.

So with the Mills murder case going cold, Baton Rouge authorities obtained a search warrant this September in an attempt to force Apple to help them break through the company's encryption. But two days after receiving the court-ordered search warrant, Apple's Privacy & Law Enforcement Compliance team delivered the bad news to homicide investigators, concluding in a brief email that stated, "Since the device is running iOS version 8 or a later version, the iOS extraction cannot be completed."

Investigators were able to successfully retrieve a trove of information from Brittney's Apple iCloud account, but they say the last time a backup of her phone occurred was months before the crime, meaning her most recent communications and activities remain unknown to police, and her personal diary was not included in any of the files recovered from the iCloud backup.

"This encryption just tells you, tells drug dealers, tells killers, (to) do what you want with impunity because law enforcement can't get into your phone," Moore said.

Apple declined repeated requests to comment on the record about the Mills murders, or any related issues.

But in an open letter to customers that addresses the topic more broadly, Apple's CEO Tim Cook explains on the company's Website (http://www.apple.com/privacy/approach-to-privacy/) "we respect your privacy and protect it with strong encryption."

Google has announced full-disk encryption in its newest Android 6.0 Marhshmallow operating system, which was launched in late October. Law enforcement officials remain in early stages of collecting information about the impact of Apple's iOS8, released one year ago, but in some jurisdictions the numbers are beginning to trickle out.

In Manhattan, the office of District Attorney Cyrus R. Vance Jr. says that in less than 12 months "roughly 111 iPhones running iOS 8 or newer were inaccessible" to its staffers. Joan Vallero, a spokesperson for Vance, says the time period tracked was from last October 2014 to this September.

Vallero says the lack of access disrupted active investigations into the attempted murder of three individuals, the repeated sexual abuse of a child, an ongoing sex trafficking ring, and numerous assaults and robberies, among other everyday crimes. She said not every disrupted crime will be unsolvable, but says the delays experienced by investigators can keep criminals in communities for longer periods.

The battle over encryption crosses international borders. The Toronto Police Service revealed to Scripps News and The Star how pedophiles are catching on and even coaching each other on how to use the latest encryption advances to conceal evidence from authorities. Toronto Detective Paul Krawczyk of the child exploitation division entered one of the "boy love" online communities he regularly monitors that he says is one of many virtual meetup spots for pedophiles.

From his desk, he located a conversation taking place that explained how American "boy lovers" have an advantage over those in some other nations, noting how no U.S. laws exist that compel criminals to hand over their private passwords that police would use to decode their files. The online user wrote, "in the U.S. (not turning over passwords) won't get you jail time. It will get the cops to abandon the investigation against you without filing charges. Just invoke the 5$^{th}$ Amendment and that's the end of it."

Another user provided advice to another "boy lover," instructing him to begin using a specific text messaging service that encrypts text messages, so that if police ever come knocking with a search warrant "they won't get anything off of your phone when it comes to chat."

The Federal Bureau of Investigation has been trying to raise the alarm in the United States with repeated trips to Capitol Hill, but has so far been rebuffed. Technology firms and privacy advocates pushed back strongly, launching a number of campaigns, such as SaveCrypto (https://savecrypto.org/). The initiatives petitioned the White House to side against groups advocating for a key for law enforcement to unlock encrypted devices if officers have a search warrant. In September, Twitter signed on to the petition, joining Dropbox and others. Last month, the White House signaled it would not, for now, push for the legislation.

Privacy advocates such as the Silicon Valley-based Electronic Frontier Foundation declared victory.

“You can’t make a back door in a house that only law enforcement can enter,” said EFF staff attorney Nate Cardozo. “If Apple were to compromise the encryption on the behest of the FBI for instance, and I was travelling in China or France or Israel or Russia or Brazil, I would no longer be secure in knowing that my iPhone wasn’t being intercepted by the local authorities there.”

Cardozo says that domestically businesses also could face an increased risk of corporate espionage if a back door were built in.

A research paper (http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8) published this July by the Massachusetts Institute of Technology and co-written by 15 of the world’s top cryptographers and computer scientists concluded that requiring a back door for  law enforcement would be akin to “mandating insecurity.”

Investigators, left to deal with encrypted operating systems on cell phones, face other mounting challenges. Popular new messaging applications such as Apple’s iMessage and Facebook’s WhatsApp also automatically encrypt messages by default.

“I think encryption is a good thing. I think it provides security for the public in their online behaviors,” said Scott Tod, deputy commissioner of the Ontario Provincial Police.  “I also think that there’s an issue in regards to building a wall too high and a moat too deep.”

Tod says about 80 percent of the digital communications officials in his Ontario office now obtain as evidence after a court-issued search warrant are “as good as garbage.”

The Royal Canadian Mounted Police cites another case in which it attempted to intercept and read encrypted e-mails among a group of high-level drug traffickers. Other law enforcement agencies wanted the Canadian police agency to either dismantle the communication network or decrypt the messages.

“With judicial authorization in hand, the RCMP dedicated thousands of hours to this effort, but was ultimately not successful because of various technical and jurisdictional challenges,” Sgt. Harold Pfleiderer, a spokesperson for the RCMP, wrote in an email.

Last week, a working group of local, state and federal officials formed that will begin to collect statistics across the nation, said David Matthews, the chair of the technology and digital evidence committee of the Association of State Criminal Investigative Agencies. Matthews admits the law enforcement community as a whole has not prioritized collecting the statistics needed to communicate what they are seeing on the ground.

*If you have a tip or an update about encryption’s impact on criminal investigations, email* mark.greenblatt@scripps.com (mailto:mark.greenblatt@scripps.com?subject=About%20Under%20the%20Radar) *and* rcribb@thestar.ca.

*Angela M. Hill (@AngelaMHill), Scripps National Investigative Producer, contributed to this report.*

*(This project was jointly reported by Scripps News and The Toronto Star.)*