The Brittney Mills murder case has put Baton Rouge in the middle of the national cellphone encryption debate

Slaying draws BR into national debate

By Danielle Maddox

dmaddox@theadvocate.com

Photo from Facebook -- Brittney Mills

Baton Rouge detectives can't get into murder victim Brittney Mills' iPhone, which they hope holds clues to a killing that so far has stumped them.

Why would a cellphone be encrypted in a way that thwarts local police investigating a homicide?

The answer lies in the fallout from Edward Snowden's disclosure that the National Security Agency was vacuuming up Internet data and information from the several billion phone calls Americans made each day. The revelation prompted Apple and Google to allow people to make it impossible to open their smartphones without a pass code — drawing Baton Rouge into a national debate.

If the owner of a phone dies, as in Mills' case, and hasn't told anyone the pass code, the manufacturers claim even they cannot access the device. And if the owner of a phone is a criminal who simply refuses to tell authorities the pass code, the same could hold true.

That can lock the contents — photos, text messages, voicemail, email, contacts, call history, iTunes material and notes — inside the phone for good.

If you don't put in the pass code, "you can't extract human readable data from the phone," said Jonathan Rajewski, associate professor of digital forensics at Champlain College in Vermont. "Even if you took the chip and hooked it up to another device, the information would still be encrypted."

Now, government and the tech industry are at loggerheads: Should companies guarantee the government, particularly law enforcement, access to these fully

encrypted devices, or will that weaken the encryption software, rendering it useless against hackers and foreign governments?

From FBI Director James Comey to East Baton Rouge Parish District Attorney Hillar Moore, law enforcement has told Congress that companies must find a way to give access to police agencies with a search warrant.

But tech industries have asked President Barack Obama to embrace encryption in its policies and resist regulating their security software.

In August 2013, Obama created an advisory committee on cybersecurity after Snowden, a former government contractor, publicized government programs that collect electronic data on Americans and foreign governments. The committee concluded the government and U.S. companies should not only embrace encryption but also should increase their use of it to better protect data.

Despite law enforcement and intelligence concerns, the committee further recommended the U.S. government should not "subvert, undermine, weaken, or make vulnerable" encryption software widely available on the market.

Those who support strong encryption claim it prevents crime, specifically hacking, and protects personal property. Apple and other players in the tech industry say the encryption upgrades made to their software mends the trust they had with international companies that was damaged during the Snowden leaks.

Critics of the upgraded encryption argue that while privacy is important, law enforcement needs legal access to encrypted phones when an investigation requires it. Criminals, like the one who shot Mills, go free when vital clues remain locked away on digital devices, they say.

The East Baton Rouge Parish Sheriff's Office said it has begun to see more encrypted phones during investigations, and Moore, the parish district attorney, recently wrote to Congress in opposition to Apple's latest encryption upgrade.

"Apple advertises this as a plus for people who buy their phones," Moore said, noting such encryption makes the phone ideal for criminals.

U.S. Sen. David Vitter, a Republican, said lawmakers are looking for a way to balance privacy with public safety but have not found a comprehensive solution.

The debate expanded well beyond individual privacy at a July hearing before the U.S. Senate Judiciary Committee, on which Vitter sits.

Peter Swire, a professor at the Georgia Institute of Technology, supports encryption. Swire argued at the committee hearing that secure communications play a vital role

in national security.

Jim Pasco, executive director of the National Fraternal Order of Police, says it's "convoluted logic" to believe that providing a way for police to open a cellphone could cause a national security problem, noting that encryption can stymie efforts to prevent terror attacks or investigate such crimes after they occur.

"It causes a much bigger national security issue when law enforcement can't get in," he said. "In making that technology available to criminals, you inadvertently make them harder to catch.??

Harley Geiger, senior councilman of the Center for Democracy and Technology, a nonprofit that advocates on Internet issues, argues that encryption makes us safer even though it can make information more difficult for law enforcement to access.

"Our smartphones and our Internet communications carry a great deal of sensitive content, and it's important to protect that content from unauthorized parties," he said. "There is a safety trade-out no matter which way you go."

Geiger said companies like Apple and Google are simply responding to market demand.

"Users, consumers and businesses that use digital service are demanding strong security," Geiger said.

Requiring U.S. companies to allow access for government surveillance would put them at a competitive disadvantage in an international industry, he said.

Manhattan District Attorney Cyrus R. Vance Jr. claims encryption has changed the dynamic between law enforcement and the public, and the change is for the worse, saying 74 investigations in his jurisdiction have been disrupted because of encryption.

"As it stands today, Apple and Google have decided who can access key evidence in criminal investigations," he told the Judiciary Committee hearing in July.

He added that he'd like Apple and Google to come to the table to discuss the problem, but as of now, they won't.

Pasco is on the same page.

"This is the kind of situation that tends to just simmer until there's some sort of horrible tragedy or we've reached our crisis stage in sheer numbers of crimes not solved because of a lack of available data," Pasco said.

Moore, Baton Rouge's district attorney, says the encryption problem "hits home

quickly with the Mills family."

Mills, 29, and eight months pregnant, was fatally shot April 24 at her Ship Drive apartment. Authorities believe Mills opened the door for someone who wanted to use her car and was shot when she refused. Doctors delivered her son, Brenton Mills, who died a week later .

Investigators said the shooter likely was someone Mills knew. They have looked to her cellphone for evidence, but her iPhone uses iOS8 software that blocks anyone without the pass code.

IPhone owners can choose to use Touch ID, which unlocks the phone with the owner's fingerprint, but Mills used only a pass code, Moore said.

Apple allows only a few consecutive pass code guesses before it returns the phone to factory settings — with none of the user's information on it.

Moore said investigators are increasingly encountering problems with encryption. On several occasions, police have tried to search for information about drug dealers from the phones of people who fatally overdosed but did not know the access codes, he said.

Sgt. Brian J. Blache, of the East Baton Rouge Sheriff's Office, said as more people use cellphones for everyday tasks, the information stored in them will be increasingly useful.

About 90 percent of the Sheriff's Office cases involves some type of cellphone or computer analysis, Blache said.

If nothing can be extracted from a cellphone, Blache said, the Sheriff's Office will lock it up in evidence with the hope that technology down the line will allow them to open it later.

Law enforcement officers can check other devices, including computers, to see if people backed up cellphone data there, or virtual platforms where people may store emails, call logs and, in some cases, old text messages from their phone. Often, information about where someone has been is available from cellphone service providers or from Internet app companies that serve up information based on the user's location.

Getting that information can be obtained with a warrant. But Blache noted some of that data depends on what location settings people select.

Also, Rajewski said Internet companies and mobile service providers keep such information for business purposes, not specifically for law enforcement's benefit,

and the retention period varies from company to company. He said the higher level of security will be more widespread moving forward as people buy new phones with the software needed to run the encryption programs.

Moore said a law should be passed prohibiting manufacturers from selling smartphones and mobile devices that the government cannot access.

Pasco, the director of the National Fraternal Order of Police, agrees that some sort of law needs to be put in place.

“Every day and week that we waste time means more crimes unsolved and more terrorist incidents unprevented,” he said.
