PortlandTribune

When Apple vs. FBI becomes life vs. death

Peter Korn

March 17, 2016

Even district attorneys have nightmares. Ryan Lufkin, an assistant Multnomah County DA, has a new one. And it's the worst kind of nightmare, Lufkin says, one that you know will soon come true.

Lufkin is following more closely than most the fight between Apple Inc. and the FBI over a court order the FBI hopes will force Apple to help unlock the iPhone of Syed Farook. Farook and his wife killed 14 people in a December San Bernardino, Calif. Christmas Party massacre.

Farook is dead, but the FBI says data on his cell phone might lead them to contacts he had with other terrorists. However, the iPhone is encrypted so that it cannot be opened without the password. Not even Apple can open it — unless the company writes what is being called a backdoor program — a customized version of the phone's operating system downloaded as an update. Then the FBI could find and use the password.

Attorneys and technology enthusiasts concerned about a loss of civil liberties say providing government with that back door comes at too great a cost. Criminal justice officials say the stakes are too high to deny them access to the cell phone of a criminal — in this case, a dead terrorist.

For Lufkin, the issue is anything but abstract. Local prosecutors are already dealing with encrypted cell phones that they believe hold vital evidence. In some cases they've been able to unlock them. In others, their inability to unlock encrypted phones, they believe, has cost them convictions.

That nightmare of Lufkin's is about bigger stakes than a conviction.

“This is the scenario that keeps me up at night,” Lufkin says. “We have a kidnapped child. Law enforcement goes to the scene. We find the child’s phone in the dirt. Of course the parents would love us to be able to search the phone and figure out who she was communicating with and what locations she was at. But the phone will be encrypted and the parents won't know the password.

“What is the reason we can't unlock this phone?” Lufkin asks. “That's going to happen. It just hasn't happened yet.”

Slippery slope?

Here's the reason, says Julian Sanchez, a technology, privacy and national security expert at the Washington, D.C.-based Cato Institute. District attorneys throughout the country have been encountering encrypted cell phones they'd like to unlock, in cases ranging from murders to small-time drug deals. If Apple is forced to build that back door “skeleton key,” Sanchez says, every government agency, whether local or national, as well as foreign governments such as Russia and China, and individual hackers, will eventually get their hands on that key.

Even worse, Sanchez says, the precedent will be set that there are no barriers to government access to encrypted personal digital devices, and tech companies and software engineers can be “conscripted” by the government to hack into digital systems.

This year the issue is cell phones, Sanchez says, but a report issued by an expert panel convened by Harvard Law School predicted that without secure encryption, virtually any digital device with a sensor could be turned into a surveillance tool. Smart televisions and even the latest interactive Barbie doll, which records sounds through a microphone and sends them to the cloud so that Barbie can deliver an appropriate response, could become monitoring devices.

And that, in Sanchez's view, is simply too slippery a slope.

“We need some belief that we are able to have conversations and try out ideas that are unpopular in a private place if we are going to have a robust democracy,” Sanchez says.

Phones store vital evidence

The view from Lufkin's office looks substantially different. Lufkin is dealing with real cases on a daily basis. And criminal cases, he says, often come down to the word of one person against the word of another. In many of those cases, according to Lufkin, the only evidence that can corroborate the victim's story is on a cell phone.

Multnomah County prosecutors currently are working on just such a case. In January, Portland police arrested Sergio Zambrano, who has been accused of rape, sodomy, kidnapping and sex abuse of a young girl. Zambrano was also charged with taking pornographic pictures of the girl.

Police took Zambrano's cell pone and had a search warrant to search the phone for evidence. It's common for sex offenders, especially those with an interest in children, to keep evidence on their phones, says Portland Police spokesman Pete Simpson.

Simpson says in another recent case, a local man convicted of sex offenses against children was found to have on his phone information that tied him to another child victim in another state, which opened a door to a whole new group of child victims who had never come forward.

Without access to that phone's information, Simpson says, all those other children and their families would never have been put in contact with authorities.

But Zambrano's phone was encrypted. The case, still in court, could very well turn into a case of the child's version of events against Zambrano's.

Why non-encrypted phones are different

Lufkin says before some cell phones included encryption, police regularly found GPS information that placed suspects at crime scenes and text messages that provided motives. And that's one of the legal pieces that has Lufkin scratching his head. If the DA can get a judge to sign off on a search warrant and police recover a cell phone, as long as that phone isn't encrypted they can access its data, he says. So it's not as if cell phone information itself is off limits to police.

“The legal principles are in place right now,” Lufkin says. “What Apple has decided to do is create a system that prevents us from accessing what we are already able to access with other cell phones.”

But that access bumps up against people's Fourth Amendment rights forbidding unreasonable searches and seizures, says Lewis & Clark law professor Tung Yin. The FBI has chosen to fight encryption in a case involving terrorists, and local district attorneys are talking about cases involving child pornography because the public will be sympathetic to law enforcement's need for access in those cases.

That's precisely why the Fourth Amendment exists, according to Yin. “The Fourth Amendment was written with the idea that we would have trouble case by case drawing guidelines,” he says. “We would always find some crime so heinous that we should do what we can to put those folks away. We don't evaluate the Fourth Amendment on a case-by-case basis.”

Lufkin isn't buying the idea that, if the FBI wins its case, people will become afraid to speak or text their minds. He points out that until recently phones haven't been encrypted, and free expression doesn't appear to have been stifled.

Lufkin and dos Mathew dos Santos, legal director of ACLU Oregon, agree that the issues surrounding cell phone privacy are too important and far-reaching to be decided by one court case. The real issue, they agree, is that technology has outpaced the privacy rules we have in place. Those rules were not set up to deal with encrypted cell phones.

Laws not keeping up with digital advances

Lufkin says he'd like government authorities and the public to decide when judges should give warrants ordering back doors to encrypted cell phones and when they shouldn't. Terrorism cases,

probably? Murder or child kidnapping, maybe? Drug cases, possibly not? “I want that conversation,” he says.

Dos Santos favors the type of legislative process Lufkin says he wants. But that conversation could become irrelevant if the FBI wins the San Bernardino case and establishes a legal precedent and gains a backdoor key, he says.

“This action by the FBI in the Apple case feels like an end run around that legislative process,” he says. And dos Santos isn't buying the idea that the FBI can win this case, use its victory to gain access to Farook's cell phone, and not use the technology to access other encrypted devices.

“The government has shown time and time again that it can't be trusted with too much power to access people's private information,” he says.

Still, Lufkin hopes the FBI/Apple case serves as a starting point.

“The big picture is we are increasingly creating digital lives and our laws have not yet caught up to how we are going to approach those digital lives,” Lufkin says. “We have a constitution and a framework that have worked well for us in investigating criminal cases for regular human beings. But we don't yet have the framework in place to comprehensively deal with the digital lives we are creating.”

Backdoor key could be used to unlock other peoples’ phones

The iPhone used by San Bernardino shooter Syed Farook erases data if someone tries to open it up with ten wrong password attempts. The password is set by the phone's owner — not even Apple knows the correct combination of letters and/or numbers.

So the FBI isn't asking Apple to simply unlock Farook's phone so it can see if he had contact with other terrorists. The FBI is asking the courts to force Apple to write new code that would represent a back door into Farook's cell phone.

That new software architecture would be sent in the form of an automatic update to Farook's phone, so there's no need to authorize it. This new architecture would allow the FBI to use what is called a “brute force attack,” with supercomputers trying an unlimited number of passwords to open the phone.

That backdoor software Apple engineers would write could be used to unlock other phones, says Julian Sanchez, senior fellow at the libertarian Cato Institute and an expert on technology, privacy and national security.

Warrants aren't enough of a safeguard, in Sanchez's view. “The difference is when police execute a warrant to search my house, it doesn't really affect the security of everyone else's house,” he says. “They don’t have to make everyone else's door unlock to get into my home.”

Sanchez thinks that making Apple write new code to break into its own security systems is asking too much of the company. And it could force Apple executives to reconsider product policy.

Does the company want its engineers to write better security code for its future products, knowing it may have to pay engineers to work harder to unlock those new products if courts require it? Or, Sanchez says, maybe companies like Apple, if the FBI wins its case, will respond by creating security systems even they won't be able to unlock the next time a prosecutor comes calling.

Technology can work both ways, Multnomah County prosecutor Lufkin admits. Occasionally, he says, police get lucky when a suspect isn't quite as tech savvy as his or her devices require. One local carjacker was convicted, Lufkin recalls, because he thought he was using the flashlight feature on his smart phone but instead ended up filming himself stealing a car.

Cops can’t get passwords, but can use fingerprints to unlock phones

Washington County prosecutors know they can't force a suspect with an encrypted phone to provide the phone’s password. But sometimes, they don't have to.

Iphones have two security options: a password known only to the phone's owner, and a biometric system that opens to the owner's fingerprint. And in Washington County, police can and do get warrants to force defendants to put their fingers on their phones' biometric sensors.

“We basically say that we want to seize that person's fingerprint,” says Paul Maloney, Washington County deputy district attorney.

So why will judges force people to provide their fingerprints to unlock phones but not require them to give up their passwords?

It has to do with the Fifth Amendment and the act of production, says Lewis & Clark law professor Tung Yin. The Fifth Amendment protects citizens from incriminating themselves. But search warrants signed by judges give police access to people and their possessions. So, for instance, police can require you to take a blood alcohol test. They can force you to be part of a witness lineup. But they can’t force you to say anything while you are in the lineup.

“The distinction the courts are trying to draw is, if you are forced to think and respond to a question, then that is making you testify,” Yin says. So if a police officer asks for your password, that’s making you testify. And you can't be forced to testify because that could be self-incriminating.

Washington County prosecutors write warrants to seize fingerprints “all the time,” Maloney points out.

Portland police don't execute biometric search warrants, according to Multnomah County prosecutor Ryan Lufkin. Lufkin says his office is still concerned that some high court will rule it illegal to require a suspect to provide his or her fingerprint. And if that happens, cases that were won using fingerprints to unlock cell phones might be reversed on appeal

Evidence out of reach in sex abuse case

Washington County prosecutors convicted Steven Rockett on child sex abuse and child pornography charges last year. Three girls told detectives that Rockett had abused them and made them pose for pictures, but prosecutors didn't have a key piece of evidence connecting Rockett to the crimes.

“We couldn’t find the actual photos or videos or whatever he was taking,” says Paul Maloney, Washington County Deputy District Attorney.

Detectives were fairly certain, Maloney says, that the illegal video was on the home computer they took after executing a search warrant. But the computer was encrypted, just like a cell phone. And Rockett could not be forced to give up the password.

“We'll never know what is on that computer,” Maloney says.

Rocket was sentenced to 52 years in prison on the sex abuse charges, mainly on the basis of the testimony of the children, Maloney says. But, he adds, if detectives had been able to introduce pornography he had shot of the children, Rockett might have accepted a plea bargain rather than go to trial. And that, Maloney says, would have spared the children the trauma of having to testify in court.

Locked phone prevented conviction

Last year, Multnomah County prosecutors lost a case of a high- profile gang shooting in Laurelhurst Park that they might have won if they'd been able to get into the suspects' phones. The alleged shooter was arrested in a car with three others. Police recovered four cell phones from the car's occupants.

According to police, one of the men in that car, Damajio Louis, posted multiple videos and pictures from his phone onto Instagram that directly related to him hunting down rival gang members, and even showed the gun used in the shooting. But the social network posts did not tie Louis to the Laurehlhurst Park shooting clearly enough for prosecutors to get the conviction they sought. That information might have been found on the cell phones, authorities speculate.

All four cell phones were encrypted. Louis was convicted of illegal gun possession, but found not guilty of the shooting.