



Harvard Lunch Club with Todd Feinburg, Mike Stopa

DAs: Locked phones hamper local cases

Waiting for a bite of the Apple

Antonio Planas Friday, March 04, 2016



Credit: Jim Michaud

EVIDENCE: Local prosecutors, including Plymouth District Attorney Timothy J. Cruz, above, say unlocking smartphones could be the key to unlocking local investigations such as homicides and sex assaults. Tech giant Apple is locked in a legal battle with the FBI, which has obtained a court order directing the iPhone maker to hack into the encrypted phone of a suspected terrorist after a mass shooting in San Bernardino, Calif.

[Facebook] Share [Twitter] Tweet [Google+] G+ [RSS] 802 11 COMMENTS



Hundreds of encrypted smartphones seized by Bay State cops could crack homicides, sex assaults and other criminal cases if the FBI wins its epic legal battle with Apple, according to local prosecutors.

Police and district attorneys from Suffolk to Berkshire counties say their inability to look into phones is cutting them off from key evidence, including one case in which a homicide might have been video-recorded on a cellphone.

That's why, as Suffolk District Attorney's Office spokesman Jake Wark told the Herald, "Like prosecutors across the country, we're watching the San Bernardino case closely."

Suffolk has 45 ongoing cases dating to last year, including murders, shootings and sex assaults, in which investigators have been unable to retrieve evidence from iPhones and Android phones, Wark said. Prosecutors, he said, have been "literally locked out" of evidence.

"The encryption technology makes the evidence within them inaccessible to police or prosecutors, even with a search warrant signed by a judge," Wark said. "With sufficient probable cause, detectives can obtain a search warrant to get a suspect's DNA sample through a cheek swab," he said. "Warrant-proof phone encryption means that an inanimate object has a greater privacy interest than the human body."

Although a customer's phone numbers and texts can be retrieved from a cell service provider with a warrant, photos, videos and notes are locked behind the encryption firewall. Berkshire District Attorney David F. Capeless said his office was locked out of at least 80 smartphones in cases last year, hampering investigations.

"This is a problem," Capeless said. "We needed a phone to get certain information that might lead us to get a search warrant and we were not able to."

In the San Bernardino, Calif., mass-killing terrorism case, the FBI has obtained a court order directing tech giant and iPhone creator Apple to create software to hack into the encrypted iPhone 5c of slain terrorist Syed Farook. But Apple is fighting it, its lawyer telling a congressional hearing this week that unlocking Farook's phone "would set a dangerous precedent for government intrusion on the privacy and safety of its citizens."

District attorneys declined to identify specific cases. But Essex District Attorney Jonathan W. Blodgett's spokeswoman said prosecutors have four ongoing cases dating to 2014 — including two homicides — in which investigators have been unable to break into encrypted phones. One of the phones holds particular interest.

"We have reason to believe that this particular phone may contain a video that would show part of a murder, or the end of a murder, but certainly would help to corroborate witnesses who were present," said Essex spokeswoman Carrie Kimball Monahan.

"We're not seeking broad authority to go trolling around for information willy-nilly," Monahan said. "We're looking for evidence based on specific crimes and specific information."

Plymouth County District Attorney Timothy J. Cruz said, "I am frustrated. I can certainly foresee dealing with our own congressional district and talking to them about it. Hopefully, we can get some law that we can all live with, that would allow us to get the information we need at the time we need it. And at the same time, maintain the privacy of people who own the phones."

Defense Attorney Martin Weinberg said he and other local lawyers also are monitoring the Apple case.

"The real risk is not a single, dramatic terrorist case," Weinberg said. "Once one court allows it, the government will predictably go back to the case. The precedent will be applied in ordinary criminal law cases to the detriment of people's expectations of privacy."

In a potentially related case, criminal defense attorney Drew Segadelli is defending a Coast Guard petty officer who was accused of drunken driving. Cops claim they found child pornography on his phone after he handed it to them.

"This issue with Apple is going to bear a lot of potential arguments which can help me in my success in suppressing what the police officers purportedly found," Segadelli said.