TechNewsDaily™
Where technology meets daily life.

Apple iMessage Encryption Stymies Government Snoops

By: Paul Wagenseil – April 5, 2013

Apple's iMessage feature may be impossible for the U.S. government to spy on — and that seems to have at least one law-enforcement agency worried.

"Text messages sent via iMessages between Apple products (iPhone, iPad, iPod touch and iMac) are not captured," the Drug Enforcement Administration said in a recent unclassified memo addressed to other law-enforcement agencies and obtained by CNET.

"iMessages between two Apple devices are considered encrypted communication and cannot be intercepted, regardless of the cellphone service provider."

However, iMessage might still be able to be eavesdropped upon. It depends on whether iMessages are routed through Apple's own servers or, instead, depend upon totally peer-to-peer encryption with no intermediary.

Apple hasn't revealed whether it archives iMessages, but in a blog posting yesterday (April 4), the Cato Institute's Julian Sanchez said there's an easy way to tell.

"If you slip in a mud puddle, destroying your iPhone (along with any locally stored encryption keys) and forgetting your passwords as a result of the bump on the head, can you still recover your data?" wondered Sanchez. "If you can — and with Apple's iCloud services, you can — then the cloud provider must itself hold the keys to unlock that data."

The iMessage question is a small part of what the FBI calls the "going dark" problem. As electronic communications gradually move from relying mostly on hardware to relying mostly on software, and as software-based encryption becomes commonplace, law-enforcement agencies are losing their ability to listen to or read people's conversations. "It is critically important that we have the ability to intercept electronic communications with court approval," former FBI General Counsel Valerie Caproni told a House subcommittee in February 2011.

"A growing gap exists between the statutory authority of law enforcement to intercept electronic communications pursuant to court order and our practical ability to intercept those communications," FBI Director Robert Mueller told the Senate Judiciary Committee in December 2011.

"Those communications are being used for criminal conversations," current FBI General Counsel Andrew Weissmann told the American Bar Association last month.
A 1994 law, the Communications Assistance for Law Enforcement Act (CALEA), orders telecommunications companies such as AT&T, Sprint or Comcast, as well as networking-

device makers such as Cisco, to build backdoors into electronic communications hardware.

Using those backdoors, law-enforcement agencies can listen to anything crossing the telecom companies' networks — including Internet backbone infrastructure — as long as the telecoms can decrypt any encrypted communications. (A warrant, subpoena or National Security Letter is required in most cases.)
But there's no similar law covering email, messaging and Internet-based voice software owned by companies such as Apple, Facebook, Google, Microsoft or Yahoo.

The FBI has been pressing hard for a CALEA update or extension that would apply to software companies, and last year the bureau even sent draft amendments to the White House, according to CNET's Declan McCullagh.

There hasn't been much explicit progress on this issue since then, and, in any case, it's not clear whether a CALEA expansion would solve the "going dark" issue. Third-party peer-to-peer-encryption software for voice and text communications have been available for computers and smartphones for years and continue to be developed.
The best known smartphone peer-to-peer-encryption app may be Silent Circle, a company started last year by a team that includes former Navy SEALs as well as Phil Zimmerman, a renowned cryptographer who in the 1990s was threatened with federal prosecution for making his free Pretty Good Privacy (PGP) email-encryption software available to anyone in the world.

Silent Circle is based in Maryland, but houses its servers in Canada, out of the reach of U.S. subpoenas or National Security Letters. The company's executives insist they're not worried about government harassment, and count U.S. government agencies among their clients.

Of course, there's another way to view the DEA memo on iMessage.

A "possible motive is to spread the very false impression that the article creates: That iMessages are somehow more difficult, if not impossible, for law enforcement to intercept," Sanchez wrote. "Criminals might then switch to using the iMessage service, which is no more immune to interception in reality, and actually provides police with far more useful data than traditional text messages can."