# Cell Phone Surveillance: US Law Enforcement Can Intercept Apple iMessages

By Clarence Walker
Global Research, April 17, 2013
Stop the Drug War

Region: USA
Theme: Law and Justice, Police State & Civil Rights

*When the tech world news web site CNET published excerpts of a leaked DEA memo [7] explaining how, during an investigation, the agency was unable to access the messages of drug dealers using the Apple iMessage system built into a Verizon cell phone, it ignited a media frenzy. "It is impossible to intercept iMessages between two Apple devices," even with a court order approved by a judge, DEA complained.*

The DEA's warning, marked "law enforcement sensitive," was the most detailed example yet of the technological obstacles law enforcement faces when attempting to conduct court-authorized surveillance [8]on non-traditional forms of communication. Federal law enforcers have coined the catchy phrase "Going Dark" to illustrate the problem.News stories and tech blogs nationwide highlighted the effectiveness of Apple's encryption protection from privacy invaders, particularly law enforcement. (See, for example, stories here [9] and here [10].) Amidst the frenzy, what went little noted was that no one's private messages held by Apple's iMessage or any other cell phone service are actually immune from federal government snooping. Under the Stored Communications Act (SCA), if the DEA wants access to someone's messaging communications, all it has to do is get a warrant to review those messages.

Why most media accounts neglected to mention this basic fact is uncertain, but the failure to do so not only misled readers into believing their iMessage communications were secure from government spying, it also fed into and reinforced a narrative being constructed by federal law enforcement agencies — that rapid advances in telecommunications technologies are leaving the government in danger of "Going Dark" when it comes to its ability to surveil its citizens, and something needs to be done to fix the "problem."

"Apple iMessage users should be aware that regardless of what they heard last week, their messages can be easily obtained by law enforcement pursuant to a warrant under the

Electronic Communication Act [ECPA]," said Alan Butler, an in-house attorney with the Electronic Privacy Information Center [11] (EPIC). "The ECPA provides in Title 111, commonly referred to as the Stored Communication Act, that a government entity may require the disclosure of electronic communications held by a provider electronic storage," Butler told the Chronicle by email. Even though the messages are encrypted by the phone company as they are sent by iMessage, Apple can decrypt messages and hand them over to law enforcement with a warrant!"


"Nothing about the DEA memo says anything about trying to crack iMessage," Cato Institute [12]analyst Julian Sanchez told the Chronicle in an email. "All it really says is that an ordinary wiretap on a cellphone's text messages isn't going to pick up iMessages, which is a no brainer because iMessages go over the Internet and not over a cell carrier."The case that inspired the DEA memo centers around a drug investigation in Texas back in February where it was unable to intercept iMessages even though a federal judge had issued a court order approving the DEA's interception of the suspects' discussions about drug deals.

Although the Federal Wiretap Act allows real-time surveillance of a device or computer, the DEA discovered in the February case that most records obtained from Verizon — the carrier of the suspect's device — were incomplete.

Cell phone surveillance is a key tool for law enforcement in monitoring criminal activity. The New York Times [13] reported last June that federal, state, and local officials nationwide had requested assorted cell phone data 1.3 million times in the previous year. But iMessages can be sent through iPhones, iPads, and even Macs running the OS platform with the capability to bypass the text messaging services of a cell phone carrier. Apple revealed in January that it sees over 2 billion messages sent each day from a half-billion iOS and Mac devices that uses the iMessage to keep private conversations and text messages secure from snooping.

When iMessage was launched in 2011, company executives boasted about its "secure end-to-end" encryption, and some critics say the leaking of the DEA memo is a clever scheme by the feds to help convince lawmakers to mandate that all communication systems, including social media and internet messaging systems have a back-door mechanism to allow government access to the data.

Cato's Sanchez explained why he was leery of the DEA memo and the motives for its leaking.

> "If this leak came from law enforcement, and that's mostly who would have access to this memo, I wonder why someone would leak it," he said. "One reason might be to support the larger 'Going Dark' campaign by the Department of Justice. Another reason might be the hope that drug dealers will mistakenly assume iMessages are safe and get lazy. Those are two possibilities worth thinking about."

The DEA also complained "that iMessages between two Apple devices are considered encrypted communication and cannot be intercepted regardless of the cell phone service provider," even though in the same memo, it conceded that "sometimes the messages can be intercepted depending where the intercept is placed."

Was the DEA memo leak part of an ongoing campaign to revamp the federal laws governing surveillance of electronic communications? That's hard to prove, but showing that there is such a campaign is less difficult.

In February testimony [14] to the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security, FBI General Counsel Valerie Caproni coined the term "Going Dark" to describe what she called federal law enforcement's rapidly diminishing ability to monitor high-tech communications products as technologies advanced over the past 10 to 15 years. Caproni singled out "social-networking sites, web-based email and peer-to-peer communications."

Other federal officials have been making similar noises.

"The FBI simply can't keep up with criminals taking advantage of online communication to hide evidence of their actions," FBI lawyer Andrew Weissman said last month [15] during a meeting with American Bar Association.

The FBI and other federal law enforcers claim there is a growing gap between the legal authority of federal and other law enforcement agencies to intercept electronic communications pursuant to court order or direct warrant under the Communications Assistance Law Enforcement Act [16](CALEA) and their ability to actually do so. And they want new legislation to fix that.

Passed in 1994, CALEA law initially ordered phone companies to create a mechanism to have their systems conform to a wiretap in real-time surveillance. The Federal Communications Commission (FCC) extended CALEA in 2005 to apply to broadband providers, such as universities and Internet service providers, but messaging and social media services, such as Google Talk, Skype, Myspace, Yahoo and Facebook, as well as encrypted devices like Blackberry and Apple communications are not covered.

The FBI argues that "Going Dark" is a real and threatening possibility, with increased risk to national security and public safety. And the FCC has joined forces with the FBI by considering updating CALEA [17] to require that digital products equipped with video or voice chats over the Internet, including Skype and Google Box Live, to rejigger their systems to allow the feds to monitor criminal activity as it happens in real time.

"We have noticed a massive upstick in the amount of FCC-CALEA inquiries within the last year, most of which are intended to address 'Going Dark' issues," said Chris Canter, a lead compliance counsel at Marashlian & Donahue , a law firm specializing in CALEA law. "This generally means that the FCC is laying the groundwork for regulatory action," he told the Chronicle.

> "If we applied the FBI's logic to the cell phone carriers, it would state that every individual phone should be designed with built-in bugs," the Electronic Frontier Foundation said in a statement on CALEA [18]. "Consumers would simply have to trust law enforcement or the phone companies not to activate those bugs without just cause."

EFF filed a Freedom of Information Act (FOIA) request [19] with the FBI and other federal law enforcement agencies showing how the feds might try to justify forcing high-tech services to rewire their systems for expanded wiretapping purposes. The FOIA requested "information concerning the difficulties that the FBI and DOJ has encountered in conducting authorized electronic surveillance."

But so far, the Department of Justice has withheld the bulk of relevant information on the topic, provoking San Francisco US District Court Judge Richard Seeborg to order the feds to turn over the records [20]. No court date scheduled for the feds to comply.

While law enforcement is calling for legislative changes to aid its work, critics insist that even if Congress refuses to pass laws to tackle the "Going Dark" problem, investigators can still obtain a special warrant allowing them to sneak into private residences and businesses to install a keystroke-logging system onto a computer or other devices to record passwords to unlock data they need to make a case.

The DEA adopted this same technique [21] in the Texas case and another case where suspected drug dealers used PGP and the encrypted Web-email service identified in court records as Hushmail.com. Investigators can also send a malware to gain control of a targeted cell phone to extract the text messages, or as a last resort, obtain a warrant to seize the physical device and perform a traditional forensic analysis.

> "New technologies frequently create uncertainty and the law is slow to adapt while leaving us to fight over how much surveillance we can tolerate in a free society," noted EPIC attorney Butler. "No one has quite figured out how to strike that balance in every case. However, the Fourth Amendment requires that our persons, houses, papers, and effects be protected from unreasonable search and seizures."

The battle between the imperatives of law enforcement and the privacy rights of Americans is never definitively won. Instead, it is better viewed as a never-ending series of skirmishes. And the contested terrain of this particular skirmish is your iPad.

**Notes**

[1] http://stopthedrugwar.org/user/41139
[2] http://stopthedrugwar.org/taxonomy/term/159
[3] http://stopthedrugwar.org/taxonomy/term/243
[4] http://stopthedrugwar.org/taxonomy/term/92
[5] http://stopthedrugwar.org/taxonomy/term/178
[6] mailto:cwalkerinvestigates@gmail.com?subject=DEA%2FiPhone%20story
[7] http://news.yahoo.com/apple-s-imessage-encryption-trips-up-feds–surveillance-213946616.html
[8] http://news.cnet.com/8301-31921_3-20032518-281.html
[9] http://www.maclife.com/article/news/just_how_secure_apples_imessage_even_dea_cant_crack_it
[10] http://www.dailytech.com/Feds+Cant+Crack+Apples+iMessage+Encryption+for+Investigation+Purposes/article30280.htm
[11] http://epic.org/
[12] http://stopthedrugwar.org/cato.org
[13]

http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all&_r=0
[ 1 4 ]
http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies
[ 1 5 ]
http://www.slate.com/blogs/future_tense/2013/03/26/andrew_weissmann_fbi_wants_real_time_gmail_dropbox_spying_power.html
[16] http://transition.fcc.gov/calea/
[17] http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/
[18] https://www.eff.org/issues/calea
[19] https://www.eff.org/foia/foia-records-problems-electronic-surveillance
[ 2 0 ]
http://news.cnet.com/8301-13578_3-57544139-38/judge-prods-fbi-over-future-internet-surveillance-plans/
[21] http://news.cnet.com/8301-10784_3-9741357-7.html



---