Slate

# DEA Claims It Can't Snoop on iMessages Sent Between Apple Devices

By: Ryan Gallagher – April 5, 2013

The FBI has a hard time spying on Gmail in real time. And now the bureau's counterparts in the Drug Enforcement Administration are also in the grip of a surveillance dilemma—as they struggle to eavesdrop on Apple's iMessage chat service.

An internal memo published by CNET yesterday revealed that the DEA claims it can't monitor iMessages sent between two Apple devices because they are encrypted and "cannot be intercepted regardless of the cell phone service provider." iMessage allows users to send text messages, documents, and media files to other users of Apple devices, using what Apple has previously described as "secure end-to-end encryption."

The DEA note, labeled "law enforcement sensitive," says that the issue came to the attention of its office in San Jose in February. Agents there had been trying to conduct surveillance of a target but realized that not all of the messages the suspect was sending were being passed on to them by the wireless provider. The memo adds that while it is "impossible" to intercept iMessages sent between two Apple devices, "iMessages between an Apple device and a non-Apple device are transmitted as Short Message Service (SMS) messages and can sometimes be intercepted."

The DEA's difficulty eavesdropping on iMessages is an illustration of what the FBI describes as its "going dark" problem. The bureau says new ways of communicating have left it increasingly unable to successfully monitor communications between suspects. Indeed, last week I reported that Andrew Weissmann, the FBI's general counsel, said in a speech that the bureau has made it a "top priority" to work on crafting a proposal for new spy powers to help conduct surveillance of services like Gmail, Google Voice, and Dropbox in real time.

However, not everyone is convinced that iMessages should be considered a part of the "going dark" problem. Julian Sanchez at the CATO Institute has even gone as far as to propose a conspiracy theory that the DEA is in fact engaged in a disinformation plot to trick criminals into thinking iMessage is untappable when in fact it is secretly easy to spy on. "Criminals might then switch to using the iMessage service," Sanchez wrote in a blog post yesterday, "which is no more immune to interception in reality." That seems far-fetched, but it is certainly true that there are ways iMessages sent between Apple userscould be intercepted. The authorities could potentially infect a targeted device with a spy Trojan to bypass any encryption, for instance, which is not exactly easy—but nor is it impossible.

It's also worth noting that the DEA's difficulties are not unprecedented; surveillance and smartphones have a history of conflict. In 2010, the Indian government threatened to block BlackBerry (then known as Research in Motion) from operating in the country unless it helped spy agencies there decipher encrypted "BBM" messages sent between Indian users. The Canadian company eventually ceded to the demand and also assisted British government when it complained about snooping issues. If authorities in the United States continue to encounter problems monitoring iMessages, you can bet that Apple will come under similarly intense pressure to build in an eavesdropping capability.