

Texting With An Informant: Lessons From Pa. Wiretap Ruling

Law360, New York (June 29, 2015, 1:31 PM ET) --

Last week, the Pennsylvania Superior Court issued an opinion in *Commonwealth v. Curtis Doval Diego*, in which the court addressed the scope of the Pennsylvania Wiretapping and Electronic Surveillance Control Act, and, specifically, whether text messages sent on an iPad were covered under the Wiretap Act. Although the case arose in the context of guns and drugs — suspected thefts of firearms and a setup heroin deal — the opinion nonetheless has implications for the use of informants and technology in a wide range of government investigations, including white collar crimes.

The problems for Diego started when an acquaintance, Gary Still, was confronted by police about his suspected theft of numerous firearms. Still quickly confessed to the thefts and became an informant against Diego. Still told the police that he exchanged two of the stolen guns for heroin from Diego. Sitting in police headquarters and surrounded by police officers, Still used his iPad to text with Diego to set up a drug transaction. Not surprisingly, when the police showed up at the arranged location, they found Diego with drugs and made an arrest. Diego then filed a motion to suppress claiming that by using an informant to send texts while the informant was at the police station the police engaged in an unlawful wiretap. The trial court granted the motion. The Superior Court reversed.

The Superior Court first rejected the commonwealth's argument that texting on an iPad somehow is the same thing as using a telephone. The Wiretap Act prohibits interception of "any wire, electronic or oral communication." 18 Pa.C.S. § 5702. The statute, however, excludes from the definition of "intercept" the use of any telephone. In *Commonwealth v. Spence*, the Pennsylvania Supreme Court confirmed that interceptions using a telephone are not prohibited by the Wiretap Act. Here, the Supreme Court didn't buy the commonwealth's argument that texting on an iPad was the functional equivalent of a telephone:

An iPad is not a telephone or telegraph instrument under a common understanding of the relevant terms, and no reasonable person familiar with the now ubiquitous technology of tablet computers would misidentify an iPad as a mere telephone. The fact that an iPad or any other tablet computer can perform functions similar or identical to a modern cellular phone is not dispositive, as the *Spence*



Lathrop B. Nelson III

Court's holding implies. The trend of convergence between modern computers and telephones aside, at this time the technologies in question remain different not only by degree, but also in kind.

Commonwealth v. Diego, 2015 PA Super 143, slip op. at 7-8 (Pa. Super. 2015). Take that, Commonwealth.

But not so fast. Just because an iPad is not a telephone — and therefore the text messages were not subject to the Wiretap Act's telephone exception — did not mean that the texting evidence should be suppressed. The court then turned to whether there was a reasonable expectation of privacy in the text messages and whether or not there was even an "intercept" in the first place. This is where things began to crumble for Diego.

The Superior Court held that the very nature of texting, much like sending an email or posting in a chatroom, recorded the text message for posterity and rendered it at least potentially capable of being shared by the recipient. Unlike an oral communication, for which one would expect no record of what was said, a text message, like an email message, is recorded for all time (or at least, for some time, until someone hits "delete"). As the court noted, "by the very act of engaging in the means of communication at-issue, Appellee risked that Gary Still would share the contents of that conversation with a third party." *Id.* at 10.

The Superior Court also rejected Diego's reliance on *Riley v. California*, which involved a cellphone that was seized and searched incident to an arrest for a firearms offense. The court distinguished between police searching a cellphone incident to arrest with the use of an informant to engage in a text conversation with a defendant.

The court concluded that there was no interception at all. The court noted that the informant voluntarily cooperated with the police and communicated with the defendant. Once the defendant sent the messages and the die was cast: what the informant did with the information received from the defendant was, according to the court, irrelevant. A government "interception" must occur either "during the transmission of the message or at least simultaneous to the receipt of the message." *Id.* at 19.

Ultimately, the court focused on the specific factual circumstances before it. Although the defendant was in a police station basement and the police were present during the transmission of the texts, the officers did not observe the actual texts. Had they done so, the court explained, "it would then be plausible to argue that the police may have observed the content of the text messages before Still had received them." The court explained in a lengthy footnote how this was not a circumstance involving police who saw and "intercepted" the text messages.

Just because the use of an informant in this case arose in the context of a drug investigation and prosecution does not preclude the use of a texting informant in a white collar prosecution. In an age where texting routinely has replaced telephone calls as a means of communication, one can certainly imagine circumstances involving a bid-rigging or other conspiracy investigation in which the state obtains the cooperation of an informant to text with a co-conspirator. And once the state has done so, and the target and the cooperator text as they had previously, all bets are off, even if that cooperator is sitting in a police station, surrounded by police officers and disclosing to them exactly what he or she is texting — so long as no police officer actually glances down to view the iPad screen and reads the text messages in real (or near) time.

This “real time” distinction draws a fine line between communications that are “intercepted” for purpose of the Wiretap Act and those that are not. In the end, this distinction provides authorities with broader freedom for how to use a cooperator in an investigation — whether involving guns, drugs or financial crimes.

—By Lathrop B. Nelson III, Montgomery McCracken Walker & Rhoads LLP

Lathrop Nelson is a partner in Montgomery McCracken's Philadelphia office. He is an editor of the firm's White Collar Alert blog.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2015, Portfolio Media, Inc.