WILENTZ
—ATTORNEYS AT LAW—
WILENTZ, GOLDMAN & SPITZER, P.A.

Danger - "General" Search Warrants in the Digital Age

06/01/15

If you knew that there was a chance—maybe even a good chance—that a law enforcement officer could gain access to every single text, email, photograph and voice mail on your smartphone, going back years, because you were suspected of criminal activity, would you change your behavior? Say less? Save less? As the law struggles to keep pace with rapid advancements in technology, the threat to individual privacy rights is rising just as quickly. More and more, law enforcement officers investigating criminal activity are securing warrants to search the smartphone contents of the targets of their criminal investigations. The justification for these searches is often if there is probable cause to believe that an individual is involved in criminal activity, it follows automatically that probable cause exists that the target's smartphone is being used to facilitate that criminal activity--or at least communicate about it. And judges are approving search warrants in these cases, without any competent, specific evidence to establish that a particular smartphone is likely to contain evidence of a crime. This dangerous trend has yet to be checked under New Jersey law.

Additionally, such search warrants run the risk of beings overly-broad, generalized search warrants that do not identify with any particularity the evidence the officer is permitted to search for and seize. In a recent case, a search warrant was issued permitting investigators to seize and search cellular telephones without specifying or particularizing the evidence permitted to be searched and seized. The warrant provided that:

An Investigator from the **** County Prosecutors Office or any other law enforcement agency is authorized to activate the cell phone to access *all information contained within the cellular telephone* bearing phone number ***-***-****, including, but not limited to the assigned cellular number, cellular billing number, address book/contact(s) information, all recent calls, to include dialed, received, missed, erased calls, duration of said calls, incoming and outgoing text messages, text message content, any stored pictures and calendar information, and any other stored information on said cellular telephone *that will assist in the continuation of this investigation* . . .

This type of warrant basically allowed the officers to look through everything on the phone, going back years before the crime that was being investigated. Based on this warrant, officers were able to read text messages between family members that had nothing at all to do with the crime that prompted the investigation in the first place. Imagine the following hypothetical, non-digital situation - the police are investigating a murder accomplished with a handgun. Although they have no information that leads them to believe that the suspect's car was used, they know that frequently people leave things in their cars. Based on that fact alone, with no specific information tying the car to the crime, police seek and obtain a search warrant. Then, when they search the car, they locate love letters between the suspect and the suspect's wife that date back 5 years before the murder. Should police be able to read the letters? If the answer is no, then why should a search warrant allow the police to review evidence on someone's smart phone that is completely unconnected with the crime being investigated?

A search warrant that provides no guidelines to the officer as to what kind of items are permitted to be seized, delegating to the officer the function of deciding whether evidence is subject to seizure, is constitutionally intolerable because it strikes at the foundation of the Fourth Amendment's requirement that warrants describe the items to be seized with particularity. State v. Muldowney, 60 N.J. 594, 600 (1972); Marcus v. Search

Warrants, 367 U.S. 717 (1961). The warrant described above is the digital equivalent of a general warrant permitting officers to rummage through an entire house, and look for and seize any item they wish.

When federal agents obtain a wiretap order, which is basically a warrant that allows agents to listen in on phone conversations that are in progress, the law imposes what is known as a "minimization" requirement. The minimization requirement requires agents to stop listening to a call once it becomes apparent that the call is irrelevant to the specific crime being investigated. For example, if agents obtain a wiretap order in a narcotics investigation and start eavesdropping on the suspect's phone, once they hear that the call is between the suspect and his child's teacher and concerns the child's progress in school, the agents must stop listening and recording. The federal wiretap statute contains this minimization requirement to protect individual privacy rights.

Our courts in New Jersey must revisit the process of granting search warrants permitting investigators to rummage through smartphones without restriction. Before an investigator obtains a search warrant for a smartphone, there must be some evidence that the smartphone was actually used to help commit the crime, or that evidence about the crime is likely to be found on the phone. Simply saying generally that people use their smartphones all the time to do everything should not be enough to obtain a warrant. If a warrant is justified, it must be limited by date and topic to specific items of information, and investigators should not be permitted to rummage around the contents of the smartphone, looking at whatever they want.

Attorney

- Darren M. Gelber

Practice

- Criminal Defense