Applying the Fourth Amendment in the Age of Technology

By Eric Nemecek

Advancements in technology present a double-edged sword; they provide users with greater resources while exposing sensitive, personal information to others, including the government. Recent court decisions suggest a shift in the struggle between individual privacy and the investigative functioning of law enforcement.

Warrantless Search of Cell Phones

In *Riley v. California*, the U.S. Supreme Court confronted the parameters of the Fourth Amendment's privacy protections within the context of warrantless cellular telephone searches incident to arrest. The Court determined that law enforcement was required to obtain a warrant prior to conducting a search of an arrestee's cell phone. The Court's rationale was predicated, in large part, on the advancements of technology, including the type and quantity of information stored on modern electronic devices. As the Court explained, "Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read …. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant … " *Id*. at 2489.

The Court also relied upon the ability of modern devices to collect information that reveals much more in combination than any isolated record an individual could conceivably carry on their person. In essence, the "sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Id*. Furthermore, a cell phone's ability to access the Internet renders the device a treasure trove for information regarding its user's private interests or concerns.

The Court reasoned that a search of one's cell phone would typically expose far more than the most exhaustive search of a house. "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id*. at 2495. Thus, the Court's answer was simple – before searching a cell phone incident to arrest, law enforcement must obtain a warrant.

Search of Electronic Devices Pursuant to a Warrant

Although *Riley* implies a search warrant would insulate law enforcement from Fourth Amendment violations, a recent decision from the Ohio Supreme Court suggests otherwise. *See State v. Castagnola*, 2015-Ohio-1565 (Ohio 2015). Therein, the defendant was initially charged with selling alcohol to a minor. During the course of those proceedings, the prosecutor's vehicles were vandalized. The police were provided with text messages the defendant sent to a third party claiming responsibility for the vandalism. Thereafter, law enforcement obtained a recording of the defendant admitting he had committed the offense by "looking up" the prosecutor's home address.

The police obtained a warrant to search the defendant's electronic devices for a broad array of information relevant to their retaliation investigation. The forensic analysis of the seized devices revealed child pornography. The defendant was subsequently indicted with numerous child pornography offenses as well as charges related to his retaliation against the prosecutor. After he was unable to suppress the evidence, the matter proceeded to trial and the defendant was convicted of all charges.

The case was appealed to the Ohio Supreme Court, which considered two interrelated issues – whether the search warrant affidavit established probable cause and whether the warrant sufficiently limited the scope of the search of any seized devices. The court found in favor of the defendant on each issue, holding the evidence in the case should have been suppressed. As the court acknowledged, "[t]he modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement much more important." *Id*. at 74.

The impact of the case is notable because it limits law enforcement's efforts to use warrants as a mechanism to seize electronic evidence without establishing any significant nexus between those devices and the nature of the investigation. Secondly, it imposes an affirmative duty on an officer to provide details in the affidavit that could limit the scope of the warrant to guide and control the searcher and to narrow the category of records or documents subject to seizure. Finally, the case establishes that a showing of probable cause does not provide law enforcement with unfettered authorization to conduct a search of electronic devices.

Common Theme

Riley and *Castagnola* provide insight into how the Fourth Amendment is applied within the context of electronic evidence. Both cases serve as an important acknowledgment that the primary focus of the Fourth Amendment is protecting the privacy of citizens. Likewise, the cases confirm an individual's right to be secure from unreasonable intrusion is inalienable, even where the defendant is arrested or an affidavit establishes probable cause to search devices for *certain* evidence.

Eric Nemecek is a partner at Friedman & Nemecek L.L.C. He has represented clients at all stages of criminal proceedings with a primary focus on complex litigation, post-conviction representation and issues involving cyber-crimes. He has represented corporations and clients in state and federal courts throughout Ohio and the United States. He is the past chair of the criminal law section for the Cleveland Metropolitan Bar Association and has co-chaired the cyber-crime committee for the American Bar Association since 2011.