Garden State CLE Presents:

DIGI-Life
Protecting Your client's Digital Life From the Police

Instructor:
Robert Ramsey, Ed.D.
John Menzel, Esquire

Lesson Plan

I. The Legacy of Katz and the Expectation of Privacy

The Supreme Court's decision in Katz vs. United States, 389 U.S. 347(1967) marks the starting point for modern day 4th Amendment jurisprudence in the privacy protections accorded electronic communications and data storage.

According to the Court, the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.

With this as a starting point, both federal and New Jersey constitutional doctrine have based the reasonableness of a search for electronic data on the concept of a legitimate expectation of privacy in the place searched or the thing that has been seized by law enforcement.

Privacy in this context includes both a subjective and an objective expectation of privacy. That is to say, a legitimate expectation of privacy encompasses not only an individual's expectation but also society's willingness to recognize that expectation as reasonable.

Once a person can lawfully assert a reasonable expectation of privacy in a place or a thing, it is mandatory that law enforcement officers act reasonably when conducting a search or making a seizure.

Reasonableness in this context means that the officer either obtained a search warrant prior to effecting the search and seizure or was privileged to rely upon one of the recognized exceptions to the warrant requirement.

By contrast, in those instances where the defendant has no legitimate expectation of privacy, there is no requirement that law enforcement officers act reasonably when conducting a search or seizure.

These concepts provide the support for all of the following types of searches the police undertake in an effort to search and seize the electronic evidence.

a) No legitimate Expectation of Privacy – In General

In those instances where the subject has no legitimate expectation of privacy in the records that were searched or seized, there is no requirement that the police act in a reasonable manner. Essentially, the police can do whatever they want to obtain the records. Examples include:

1) A law enforcement review of on-file fingerprints, photographs or matters of public record - (Doe vs. Portiz, 142 N.J. 1, 28 n.8(1998).

2) Random police searches of license plates - (State vs. Donis, 157 N.J. 44(1998).

3) Records stored in the NCIC database - (State vs. Sloane, 193 N.J. 423(2008).

4) Workplace computers owned by the employer – (Doe vs. XYZ Corp., 382 N.J.Super 122, 138-39(App.Div.2005)). However, communications that are otherwise privileged may be subject to an expectation of privacy. By way of example, consider attorney and client communications on a workplace computer. See Stengart vs. Loving Care Agency, 201 N.J. 300(2010).

b) The Third-Party Doctrine

1) The Federal Rule

It has long been a matter of federal constitutional doctrine that people have no expectation of privacy in records they voluntarily turn over to a third party. In the case law, this rule of law has permitted these types of records to be subject to search and seizure based solely upon an administrative subpoena issued by a trial court or a grand jury. This federal rule of law has been applied to banking records (U.S. vs. Miller, 425 U.S. 435(1975)) and telephone usage (Smith vs. Maryland, 442 U.S. 735(1979)).

2) The New Jersey Rule

The foregoing principle is most decidedly not the law in New Jersey. Article I, paragraph 7 of the New Jersey Constitution of 1947 provides enhanced privacy protection to the electronic records. Over the decades, the Supreme Court has incrementally expanded the expectation of privacy that people in our state have for electronic records they voluntarily turn over to a third party. The trend is to require law enforcement to seek some measure of judicial or supervisory authority, usually based upon less than probable cause.

The chronology in the development of the law can be listed as follows:

1982 - State vs. Hunt, 91 N.J. 338, 450 A.2d 952(1982) (Telephone records—requiring a communications data warrant (the functional equivalent of a search warrant) to obtain telephone toll records)

1989 - State vs. Mollica, 114 N.J. 329, 554 A.2d 1315(1989) (Hotel room telephone records);

2005 - State vs. McAllister, 184 N.J. 17, 875 A.2d 866(2005) (Banking records - Grand jury subpoena *duces tecum* for banking records authorized)

2006 - State vs. Domicz, 188 N.J. 285, 907 A.2d 395(2006), (Public Utility records of usage requires grand jury subpoena *duces tecum)*

2008 - State vs. Reid, 194 N.J. 386, 945 A.2d 26(2008) (Internet subscriber information—may be obtained by grand jury subpoena *duces tecum*)

2013 - State vs. Earls, 214 N.J. 564, 70 A.3d 630(2013) (Cell phone location—Search warrant or exigent circumstances required to secure cell phone location and tracking data)

In State vs. Lunsford, 226 N.J. 129 (2016), the Supreme Court sought to harmonize these options for law enforcement. The Court noted that the privacy concerns differ among the noted records based upon how much information they may reveal about the individual. For example, telephone billing records yield much more potential information about a person than do public utility usage records. The varying degrees of information that records may reveal is related to the level of proof law enforcement must demonstrate in order to obtain the records. The more information that a search will reveal, the greater the burden on law enforcement will be to act reasonably through judicial intervention.

3) Options available to law enforcement.

Law enforcement can resort to four options to obtain and review records which are in possession of a third party.

Do Nothing;
Apply for a Search warrant;
Seek a Criminal Action Order; or
Seek a Grand Jury Subpoena.

The Option of doing nothing usually applies where the police are conducting a review of records that are already in their possession and the defendant has no legitimate expectation of privacy (e.g., NCIC).

The search warrant provides the greatest level of protection by strictly requiring a neutral and detached judge to make a probable cause finding. At the other extreme, a grand jury subpoena can be issued without judicial intervention on slight evidence linked only to relevance to the investigation under review. A criminal action order requires an intermediate level of review, including judicial scrutiny and involvement to make sure the order calls for relevant and material information related to a criminal investigation.

In synthesizing law enforcement needs with the varying degrees of privacy interests in electronic records, the Court in Lunsford ruled that cell phone tracking information may only be obtained by the police

through either a search warrant or by demonstrating exigent circumstances that excuse the police from obtaining a warrant as was discussed in the seminal cell phone tracking case of State vs. Earls, 214 N.J. 564(2013).

For telephone billing records, the Court adopted a mid-level protection scheme. In order to obtain billing records, a search warrant is no longer necessary. Rather, the police must apply for a court order under N.J.S.A. 2A:156A-29(e) to obtain telephone billing or toll records. In accordance with that statute, law enforcement must demonstrate specific and articulable facts showing that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation. N.J.S.A. 2A:156A-29(e). The requested records must cover a finite period of time which does not extend beyond the date of the order. Judicial review of *ex-parte* applications of this type will help guard against abuses in general and root out bulk requests for information that are unconnected to a criminal investigation. In addition, a judge may quash or modify an order if the information or records requested are unusually voluminous, among other reasons.

Finally, for other types of records, such as utility usage or internet subscriber information, it appears that the relatively low-level grand jury subpoena *duces tecum* is sufficient to protect the privacy interests involved.

II. Telephone-Based Communications and Records

1) Cell phones – In general

In modern-day life, a cell phone provides far more services than simply communicating with another party. The advancing technology provides the cell phone user with access to the internet, stored photos and movies, the ability to photograph and record audio and video data and an enormous volume of other helpful services. This reality was not lost on the United States Supreme Court when it examined the privacy implications when a cell phone is seized by the police.

Riley vs. California, 573 U.S. 373(2014)

Following a routine motor vehicle stop, the petitioner was arrested for driving on the revoked list. An inventory search of his vehicle incident to its impoundment revealed hidden, loaded handguns. The defendant was arrested for the weapons offenses and searched incident to the arrest. As a result of that search, the police recovered a cell phone from the petitioner. A forensic search of the phone by a trained officer who specialized in gang activities yielded significant evidence of criminal activity by the petitioner, including an attempted murder. The petitioner's attempt to suppress the evidence obtained from his cell phone prior to trial was rejected by the motion judge. Thereafter, based largely upon the evidence recovered from his cell phone, the petitioner was tried and convicted of weapons offenses, assault and attempted murder.

The Supreme Court ruled that the unique capabilities and storage capacity of modern cell phones render them distinctly different from other physical objects that are seized as a matter of routine from people who are arrested. According to the Court, people have and maintain a reasonable expectation of privacy in the digitally-stored contents of their cell phones. In the absence of exigency, consent or some other exception to the warrant requirement, police agencies that seek to search the contents of a cell phone seized incident to an arrest must obtain a search warrant.

2) Cell Phone Numbers

> a) While there might be an expectation of privacy inherent in a cell phone number under certain circumstances, there can be no expectation of privacy in a cell phone number that has voluntarily been revealed to a third party. As explained in State vs. DeFranco, 426 N.J.Super 240(App.Div.2012), this rule of law can apply even when the number that was revealed to a third party has been changed.

b) Pass codes - For encrypted cell phone pass codes, see Sate vs. Andrews, 243 N.J. 447(2020) (Although pass code is minimally testimonial, this may be overcome when the code's existence, possession and authentication are a foregone conclusions).

3) Text messaging

a) Authentication - Text messages and Twitter (X) posting meet the definition of a writing under the NJRE and are subject to the low-level criteria necessary for authentication as a condition of being considered as evidence. State vs. Hannah, 448 N.J. Super 78(App.Div.2016).

b) Standing - In State vs. Armstrong, 463 N.J.Super 576(App.Div.2020), the police used the content of certain text messages that the defendant sent to a third party (former girlfriend) as evidence against him in a murder trial. The content of the text messages had been turned over by the third party to the police from her cell phone on a voluntarily, consensual basis. The defendant's attempt to suppress the text messages was rejected at trial without a hearing. The Appellate Division ruled that the defendant had neither an expectation of privacy in the text messages he sent once they were received and stored on the recipient's cell phone. Moreover, given the relationship between the defendant and the recipient, the defendant had no participatory interest in the crime with the recipient such that he would have automatic standing to bring a motion to suppress.

c) Text devices provided for work-related purposes – Although employees who have been provided text-messaging devices for work may have an expectation of privacy in their text messages, including those that are strictly personal in nature, the workplace special needs exception to the warrant requirement permits review of the related records without a

search warrant. City of Ontario vs. Quon, 130 S.Ct. 2619(2010).

d) Access to cell phone records – CDW

A communications data warrant (CDW) is different from a wiretap order in both the nature of the communication to which it is addressed and the standard for its issuance. A wiretap order permits the interception by law enforcement of a communication contemporaneous with the transmission while a CDW is directed to acquisition of communications or data in post-transmission electronic storage kept by an electronic communications service or remote computing service for reasons of backup protection for the communication.

Because of this difference, a CDW is not subject to the more restrictive procedures and enhanced protections of the Wiretap Act, which include a showing of necessity because normal investigative procedures have failed. Instead, under N.J.S.A. 2A:156A-29e, the standard for the issuance of a CDW by a judge of the Superior Court requires only a showing of "reasonable grounds to believe that the record or other information pertaining to a subscriber or customer of an electronic communications server is relevant and material to an ongoing criminal investigation."

There are no specific time limitations under the statute that limit how far back in time the state may forage for electronically stored data. As a practical matter, the answer to this question should be "as long as it takes to obtain the relevant and material evidence." See State vs. Finesmith, 408 N.J.Super 206(App.Div.2009).

e) Use of cell phone data for vehicle tracking – In State vs. Earles, 214 N.J. 564 (2013), the Supreme Court recognized that while cell phone tower pings provide law enforcement an

important investigative tool, expectations of privacy require that the police secure a search warrant or rely upon exigent circumstances when accessing these cell phone data.

f) Tracking devices installed on a vehicle – The installation of a tracking device on motor vehicles constituters a search within the meaning of the 4th Amendment and generally would require a search warrant. See United States vs. Jones, 565 U.S. 400(2012).

4) Telephone communications by Defendants in custody –

a) There is no legitimate expectation of privacy related to inmate access to telephones in jails or prisons. Hudson vs. Palmer, 468 U.S. 517(1984); State vs. Jackson, 460 N.J.Super 258(App.Div.2019). However, defendants in police custody (and the people they call) have a legitimate expectation of privacy in calls they make for help following an arrest. State vs. McQueen, 248 N.J. 26(2021).