CENTER FOR APPELLATE LITIGATION

120 WALL STREET – 28TH FLOOR, NEW YORK, NY 10005 TEL. (212) 577-2523 FAX 577-2535
http://appellate-litigation.org/

ISSUES TO DEVELOP AT TRIAL

March 2020 - Vol. 5, Issue 2

This issue flags two recent Appellate Division cases that together support robust probable cause and particularity challenges to search warrants of cell phones and social media/computer files. The cases demonstrate a special judicial concern for privacy interests where computer and digital searches are involved. To the extent your motion to controvert might have been denied before these cases were decided, consider a motion to reargue.

Some background: Under the state and federal constitutions, no warrants "shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." This clause, known as the Warrants Clause, was designed as a bulwark against "the 'general warrant' abhorred by the colonists" and to prevent "a general exploratory rummaging in a person's belongings." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

Particularity requires that a warrant "clearly state what is sought[,] while "[b]readth deals with the requirement that the scope of the warrant be limited to the probable cause on which the warrant is based." United States v. Cioffi, 668 F. Supp.2d 385, 390 (E.D.N.Y. 2009)(quoting United States v. Hill, 459 F.3d 966, 973 (9th Cir. 2006)). In other words a warrant may violate the clause in two, often interrelated, senses: "either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries." Id. "[A] search warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." Groh v. Ramirez, 540 U.S. 551, 559 (2004).

Two recent cases:

People v. Thompson, 178 A.D.3d 457 (1st Dep't Dec. 5, 2019) - The First Department held that the search of the defendant's cell phone was overbroad under both the federal and state constitutions.

The Court was particularly concerned with the absence of probable cause with respect to crimes that occurred before the date (September 1, 2016) specified in the warrant application. Therefore, the warrant was overbroad insofar as it authorized examination of the defendant's internet usage from January 1 to September 13, 2016, and also authorized, without a time limitation, examination of essentially all the other data on the defendant's phone. "The evidence available to the warrant-issuing court did not support a reasonable belief that evidence of the

crimes specified in the warrant would be found in all of the 'locations' within the defendant's cell phone to which the warrant authorized access – for example, in defendant's browsing history six or seven months before September 1, 2016, or in his emails, the examination of which was authorized without any time restriction"

People v. Melamed, 178 A.D.3d 1079 (2d Dep't Dec. 24, 2019) - Here, the Office of the Attorney General had obtained a warrant to search the defendant's business premises, alleging that the defendant had caused illegal construction and demolition to be performed at a rent-stabilized building owned by the defendant's company. The application alleged that the defendant committed the crimes of offering a false instrument for filing, endangering the welfare of a child, and violating Real Property Law § 443

The warrant the OAG obtained on the basis of the investigator's affidavit permitted the OAG to search and seize broad categories of items, including those relating to other businesses the defendant controlled. The warrant did not name or specify any particular crime or offense to which the search was related and did not incorporate the affidavit by reference. The OAG seized nine computers and dozens of boxes of papers and files. The indictment charged the defendant with numerous crimes, beyond what was specified in the affidavit.

The Second Department found the warrant to be "precisely the kind of general warrant the Federal Constitution prohibits." It failed to conform to the particularity requirement required by the Fourth Amendment. Specifically, other than a date restriction covering a period of approximately five years, the warrant permitted the OAG to search and seize all computers, hard drives, and computer files stored on other devices, without any guidelines, parameters or constraints on the type of items to be viewed and seized. As to paper documents, it merely identified generic classes, permitting the search and seizure of "virtually all conceivable documents that would be created in the course of operating a business." The "all documents" search was not restricted by any reference to the crimes to which the items searched and seized should relate, and the affidavit couldn't save the warrant from its facial invalidity because it was not incorporated by reference into the warrant.

One judge dissented, so the case may be headed to the Court of Appeals.

Takeaways:

- If law enforcement executes a cell phone/computer/digital device search warrant, scrutinize the warrant with attention to the particularity requirement. Based on the two cases above, consider whether

    - the warrant identifies a specific crime, and whether the indictment alleges the same or different crimes
    - the warrant authorized a search beyond the date of the alleged offense, and how broad that period is
    - how broad/general are the areas to be searched (e.g. "internet usage;" "browsing history")

- whether there was probable cause alleged that evidence of the crimes specified would be found in the areas specified
- for paper documents, are the classes of documents generic or restricted to the crimes to which the items seized should relate

- If the affidavit could arguably provide the necessary limitations, check whether the warrant incorporated the affidavit by reference

  - Under Groh v. Ramirez, 540 U.S. 551, 560 (2004), a warrant relying on supporting materials to guide an executing officer must "at least incorporate [those materials] by reference[.]"

  - Argue lack of incorporation regardless of whether the prosecution alleges that the material was before the Magistrate or the warrant states that the Magistrate was satisfied that the affidavit established probable cause. If the warrant does not incorporate the affidavit by reference, its lack of particularity /overbreadth violates the Fourth Amendment under Groh.

- Cite the federal and state constitutions (U.S. amends. IV, XIV; N.Y. const., art. 1, § 12) and emphasize that the particularity requirement "'assumes even greater importance" where digital and computer searches are involved, because "the potential for privacy violations occasioned by unbridled exploratory search" of such files is "'enormous.'" Melamed, at 2-3, quoting United States v. Galpin, 720 F.3d 436, 446-47 (2d Cir. 2013) See generally Carpenter v. United States, 138 S.Ct. 2206, 2217 (2018)(in finding an expectation of privacy in historical cell site location information, Court notes that a cell phone is "almost a 'feature of human anatomy,'" which tracks nearly exactly the movements of its owner and "faithfully follows its owner" into private and personal spaces).

- If you lost a prior motion to controvert, consider moving to reargue based on this new authority.

  - A motion to reargue "shall be based upon matters of fact or law allegedly overlooked or misapprehended by the court in determining the prior motion, but shall not include any matters of fact not offered on the prior motion." Note that a motion to reargue a point decided by the trial court must be made within thirty (30) days of service of a copy of the order and written notice of its entry. CPLR 2221(d).

  - A motion for leave to renew may be made after 30 days, and must show either new facts not offered on the prior motion, or "that there has been a change in the law that would change the prior determination." If new facts are offered, you have to explain the failure to present such facts originally. CPLR 2221(e).

  - You can also do a combined motion. CPLR 2221(f).

ISSUES UPDATE

In our September 2019 newsletter, we suggested a constitutional challenge to Correct. Law § 168-f(4), which requires sex offenders to register "no later than ten calendar days after any change of address." We proposed that the statute was unconstitutionally vague because it does not define "address," and violated the Equal Protection Clause because it discriminates against indigent SORA registrants, subjecting them to felony prosecution and confinement.

We provided you with template papers that relied upon a few favorable out-of-state cases. Since then, however, the Second Department has held that "the word 'address' does not suffer from vagueness" and provides officials with "clear standards" for enforcement. See People v. Lanham, 177 A.D.3d 637, 638 (2d Dep't 2019).

Please continue litigating this issue if it arises in a case. A split among Departments would position the case for Court of Appeals review, nor did the Second Department address the Equal Protection claim.