

A Primer on Searches and Investigations by Law Enforcement Agencies

By Samuel M. Braverman

December 5, 2024

Local prosecution offices, such as county district attorney's offices, and national law enforcement bureaus, including the FBI, have recently conducted several high-profile investigations of municipal, national and corporate wrongdoing. Although these investigations can be routine for those involved, the media often portray them in dramatic and theatrical terms. To de-dramatize the subject and make the process more accessible, I offer a primer on how law enforcement conducts these investigations based on my front-row seat to these events from the last 30 years of practice.

Law enforcement agencies, such as local police, the FBI, the Securities and Enforcement Commission (SEC), are authorized to investigate individual and organizational violations of law. Officers are tasked with enforcing the codes and statutes that prohibit or require certain actions. Therefore, they are allowed to make an arrest when the officer has probable cause to believe that a statute has been violated and the person to be arrested was responsible for that violation—whether as a principal, or as

an accomplice, a conspirator, a facilitator, or one who solicits another to commit the offense. The information the arresting officer relies upon can be supplied by a fellow officer, by a known source of informa-

tion, or by the officer's own senses of observation. Sometimes an arrest is based upon an arrest warrant, signed by a judge in the jurisdiction where the person to be arrested is located.

Officers can conduct searches of people, areas, and things, either because they have a search warrant, issued by a magistrate upon probable cause, or because the search is connected to an arrest, such as "in the arm's reach area of the person to be arrested" or "in plain view of the officer when making an arrest." If the officer has a search warrant, it is because the magistrate reviewed an affidavit of probable



Courtesy photo.

Samuel M. Braverman of Anderson Kill.

cause—information which shows that it is more likely than not that an identified person committed a crime -- and then signed a warrant, specifying the time, place and manner for the search.

Search warrants can specify the person to be searched and the type of search (e.g., “obtain a DNA sample from the target’s oral cheek cells,” or “a hair/fingerprint/handwriting/voice exemplar”), the area to be searched (e.g., the “office,” the “car” or “the second bedroom on the left on the third floor of the home at 123 Main Street”), or the type of item to be seized (e.g., “all electronic equipment, including computers, cellular telephones, mini-computers, digital recording devices, external and internal storage devices, as well as all paper files containing tax returns, supporting documents for corporate and individual returns, and correspondence regarding tax returns”). The specifics of the description of the search are very important because “general warrants” (“take anything there,” “arrest everyone present”) are almost universally overbroad and the results gained from such warrants can be suppressed—that is, ordered unusable at trial.

Search warrants can allow law enforcement to place a listening device or camera device in an area that the owner keeps private from others, but officers do not need a warrant to place the listening or camera device in a public place where no one has an expectation of privacy, such as in a streetlight or train station. Search warrants can authorize the police to enter an area to look for evidence of crimes, and if they find anything, to return to the magistrate for an additional warrant (unaffectionately known as “sneak and peek” warrants). Warrants can also be issued to allow for a pen register, which creates a list of all calls to and from a certain

telephone number, or for a wiretap, to record all incoming and outgoing calls on a telephone number. Warrants for the placement of wiretaps usually carry numerous limitations, such a minimization of non-material calls, and no listening or recording of privileged calls (such as those between attorney and client, husband and wife, and religious leader and adherent).

Most importantly, items seized pursuant to search warrants give prosecutors information that can be used to generate more probable cause to seize other items, either from the same target or from other sources. So if a prosecutor has probable cause to seize a target’s phone (based upon a witness’s information), she gets a warrant for the phone and has law enforcement seize it. Even if the phone is password-protected, there are several law enforcement programs that enable the breaking into of nearly every kind of smartphone. The contents of the seized phone can then create probable cause for the next target’s cellphone, and the next search warrant, and so on, without end or limitation.

Prosecutors also have two very powerful tools to obtain documents and testimony from individuals without warrants or probable cause. The first is the grand jury and its subpoena power. The grand jury is empaneled to investigate crimes and to issue indictments alleging criminal activity. As the legal adviser to the grand jury, the prosecutor presents cases to the grand jury and issues subpoenas (orders commanding compliance) in its name. These subpoenas can be issued for testimony before the grand jury (subpoenas ad testificandum) or for documents (subpoenas duces tecum), or both. Although the prosecutor must use the grand jury power only for a legitimate investigation of criminal activity,

the process is subject to little or no oversight. The recipient of a grand jury subpoena can move to quash (have a court throw out) the subpoena, but that rarely works because the prosecutor tells the court that they are working on “some important violation of law”. The recipient of the subpoena cannot meaningfully respond because they do not have any information about what the “important” task is, and so the court routinely defers to the prosecution on the scope and materiality of the subpoenaed materials and denies the motion. Sometimes a court will limit the scope of the production if it is exceptionally burdensome, or expensive, or overbroad. Subpoenas can be issued to third parties for enormous amounts of information (e.g., “all the social media posts for the following 15 individuals,” “all the bank statements,” or “all the emails for the listed corporation”). There is no requirement that the recipient of the subpoena must notify the individual or entity that created the data.

The second subpoena is the trial subpoena for testimony. This tool can shine the very bright spotlight of public trial and cross examination, which can be extremely detrimental to a public image of a person or entity. Worse, the trial subpoena puts the person or entity in the dangerous position of deciding whether to testify (with the risks of perjury and self-incrimination) or risk contempt. In some circumstances, this risk can be abated with a non-prosecution agreement (where a prosecutor agrees not to prosecute a person or entity for cooperation, including producing documents or giving truthful testimony at a future trial). Alternatively, the risk of self-incrimination and the protections of the Fifth Amendment can be brushed aside with grants by prosecutors (in a state court) or orders of a

court (in a federal court) of immunity and a material witness order compelling testimony under penalty of arrest. This allows the prosecutor to immunize a person constitutionally from prosecution in the forum where it is granted (i.e., state court by a state prosecutor and federal court by a federal prosecutor), and then to compel the testimony under penalty of contempt.

Federally, prosecutors also have 18 United States Code Section 1001 at their disposal, which makes any material false statement to a federal law enforcement agent in a federal matter, or any attempt to hide a fact, or any use of a false writing, a federal crime punishable by up to five years in prison. This can be as innocuous as telling an FBI agent, “I didn’t speak with that person last week” when you actually did speak with that person. Further, 18 U.S.C. Sections 1501-1521 (Obstruction of Justice) offers a host of additional bludgeons for anyone who stands in the way of law enforcement’s investigations.

Another off-the-grid type of investigatory tool for prosecutors is the “proffer” meeting, which occurs in many forms, but essentially is the exchange of information for the hope of a benefit. In the traditional proffer, a person with information goes with their lawyer to the prosecutor’s office and meets with law enforcement to “proffer” what he knows in exchange for the hope that down the road, the prosecutor will either not charge that person, charge the person with lesser offenses, or make a sentencing recommendation that provides for some leniency. There is also an “innocence proffer,” where a person offers evidence to the prosecutor that shows the person is not guilty of any crime, or a “reverse proffer”, where the prosecution puts on a show-and-tell of some of the evidence that would be

presented at a trial in an effort to overcome a reluctant target or defendant and demonstrate to the target why a guilty plea or a cooperation plea agreement would be beneficial to the target.

Proffers can lead to several different types of contracts between prosecution and defendant. The contracts can take the form of written cooperation agreements as used in state courts (agree to plead guilty to certain charges in exchange for testimony and a promised sentence) or in federal courts (agree to plead guilty to criminal charges in exchange for a government motion at sentencing pursuant to U.S. Sentencing Guideline Section 5K1.1 that recommends lenience but without a specific sentence). The term “Queen for a Day” protection, as described about proffer sessions, is its own article about the use and derivative use of proffered information.

One of the most productive and hidden-from-view tactics is for a federal law enforcement agent to approach a target in an informal setting, such as a hotel lobby when the target is on vacation, and with a cup of coffee in hand, sit down next to the target on the bank of chairs and say “Good morning, Bob. How’s your trip with the wife and kids going? Nice to get time away from the CFO job at the office?” The target is now panicked that a stranger knows his name when he is on vacation, away from

his home, office, and attorney, and is being questioned by a guy in a polo shirt with a military-style haircut. There is no legal requirement that the agent has to tell the target that any material false statement could subject the target to prison, but as soon as the target falsely disclaims knowledge about a co-conspirator or a transaction or a business event, he has committed a crime and the agent has all the leverage he needs. Now the agent lets the target know that he is already guilty of making a false statement and if the target wants to help himself, he should cooperate with the agents or face prosecution.

The takeaways from this toolkit are simple: first, of course, is stop any involvement in criminal activity, and in lieu of that, stop writing it down. Everything is discoverable in today’s digital world, including attempts to destroy prior memorialization of criminal activity. Second, stop talking to law enforcement without an attorney present. No matter the circumstances, having an experienced criminal defense attorney with you for questioning and negotiating is essential. Always ask for an attorney before you say anything else. And third, repeat step one.

Samuel M. Braverman is a shareholder in Anderson Kill’s New York office and national co-chair of the firm’s white collar defense group.