CENTER FOR THE ADVANCEMENT OF PUBLIC INTEGRITY

A Practitioner's Guide to Wiretaps in Public Corruption Investigations

COLUMBIA LAW SCHOOL

CENTER FOR THE ADVANCEMENT OF PUBLIC INTEGRITY

About:

Author:
Wesley Cheng is a practitioner in New York City who has worked in numerous government offices, including as and Assistant District Attorney for the New York County District Attorney's Office, an Assistant Attorney General for the New York State Attorney General's Office, an Associate General Counsel at the Office of the Metropolitan Transit Authority Inspector General, and in the Office of the Special Narcotics Prosecutor for the City of New York.

What is CAPI?
The Center for the Advancement of Public Integrity is a nonprofit resource center dedicated to improving the capacity of public offices, practitioners, policymakers, and engaged citizens to deter and combat corruption. Established as partnership between the New York City Department of Investigation and Columbia Law School in 2013, CAPI is unique in its city-level focus and emphasis on *practical* lessons and tools.

Published: July, 2016 by the Center for the Advancement of Public Integrity at Columbia Law School.
Available at **www.law.columbia.edu/CAPI.**

Practitioner Toolkit Series

laura and john arnold foundation®

This publication is part of an ongoing series of contributions from practitioners, policymakers, and civil society leaders in the public integrity community. If you have expertise you would like to share, please contact us at **CAPI@law.columbia.edu**.

The series is made possible thanks to the generous support of the Laura and John Arnold Foundation. The views expressed here are solely those of the author and do not represent the views of the author's organization or affiliations, the Center for the Advancement of Public Integrity, Columbia Law School, or the Laura and John Arnold Foundation.

A Practitioner's Guide to Wiretaps in Public Corruption Investigations

The nonconsensual interception of wire, oral, or electronic communications of targets in criminal investigations[1] is a powerful law enforcement tool and can be used to great effect in many cases, including public corruption cases. Indeed, particularly in cases where wrongful behavior is covert – as is often the case when public officials are involved -- there is great value to evidence that allows prosecutors to use the defendant's own recorded words against him in the courtroom. But there are many factors to consider before using this labor-intensive, long-term tool in your corruption investigation, and once a decision has been made to seek a wiretap, there are several legal issues that may arise.

This paper sets forth some factors you should take into account when considering a wiretap, and precautions you should take to ensure you are in the best possible position for litigation following the wiretap, especially as it relates to a public corruption case. It also includes a sample federal wiretap application affidavit, and sample instructions for minimization.[2]

Appendices:

Appendix 1:
Sample wiretap application from United States v. Skelos.

Appendix 2:
Sample minimization instructions for oral and wire communications.

Appendix 3:
State-by-state wiretap requirements.

I. Is this the Right Case for a Wiretap?

Before discussing the legal issues relating to wiretaps, it is necessary to assess whether your investigation is the right case for a wiretap. In doing so, ask these questions:

1. Do we have the money?

On December 31, 2015, the United States Courts system released its annual wiretap report for the year.[3] The average cost of a wiretap was $42,216 and the most expensive wiretap cost $1,363,192, which involved a 390-day narcotics investigation in Rockland County, New York.[4] Overall, 4,148 wiretaps were authorized in federal and state courts, and, from these, 3,297 extensions were requested and authorized, more than a 79 percent renewal rate.[5] You must ensure that your agency has the financial resources to be able to support a wiretap, and that it can continue the investigation in the event of an extension of the initial tap.

2. Do we have the manpower?

An eavesdropping investigation involves a team of investigators that will need to monitor the wiretapped phone lines at all times. That means that someone will always need to be at the plant, where conversations are intercepted and recorded. Simultaneously, there will need to be an investigative team out in the field performing physical surveillance for at least some of the time the wiretap is live. Monitoring a phone 24 hours a day for 30 days at a time can be a huge drain on man power. You must ensure that your agency has enough investigators to carry on an investigation like this. These issues become even more important if a foreign language is involved and translators must be utilized.

3. Is this a wiretap worthy case?

Of the 4,148 wiretaps issued in 2015, approximately 3,292 of them (79 percent) were for narcotics cases.[6] The other 21 percent included homicide and assault (221 wiretaps), racketeering (141), conspiracy (220), larceny, theft and robbery (40), corruption (10), and gambling (33).[7] There were 191 other cases outside of these major categories. So, for the most part, wiretap cases are used to investigate major offenses.[8] In deciding whether to engage in a wiretap investigation, think of whether the amount of resources being used to investigate is worthy of the crime or target(s) you are seeking to eventually prosecute. In a public corruption case, this may be an easy call with an elected official, but it should be considered, particularly with lower-level public officials or employees.

In deciding whether to engage in a wiretap investigation, think of whether the amount of resources being used to investigate is worthy of the crime or target(s) you are seeking to eventually prosecute.

II. Legal Framework

If you have determined that a wiretap is practical in your public corruption investigation, then it's time to consider the legal foundation of an eavesdropping warrant. Eavesdropping warrants are a variant of general search warrants, and are thus governed by the limitations of a search warrant.[9] Title III, like a general search warrant, requires that an eavesdropping warrant only be issued upon a showing of probable cause.[10] It goes several steps further by requiring or authorizing the following:

- The application must include the name of the target (if known) and the type of communication that will be intercepted.[11]
- The statute enumerates the investigative, judicial and enforcement agencies that are allowed to seek, review and execute eavesdropping warrants.[12]
- The affiant on the application is required to state how "normal investigative procedures have been tried and have failed or reasonably appear unlikely to succeed if tried or to be too dangerous."[13]
- The authorizing judge has discretion to direct investigators to update the judge on the investigation at whatever intervals the judge requires.[14]
- The application must specifically state the time period for eavesdropping.[15]
- The statute states that eavesdropping can continue beyond the originally authorized time period, but only under certain circumstances.[16]

These requirements apply to all wiretap applications, not just those in public corruption investigations. As discussed in greater detail below, however, given the likely publicity that your public corruption case will generate, you will want to ensure that you scrupulously follow these requirements and are ready to defend you and your law enforcement partners' actions every step of the way. Litigation over adherence to these requirements is more likely to occur and to be more contentious in a corruption case than in an average wiretap case.

Once a judge has authorized an eavesdropping warrant, there are several other requirements to keep in mind:

- The statute specifies how intercepted conversations are to be preserved, safeguarded and stored.[17]
- The statute states what investigators must do in the case of intercepting a non-pertinent conversation, commonly referred to as minimization.[18]
- The statute states the circumstances under which intercepted conversations may be disclosed or used as evidence.[19]
- The statute lays out notice requirements for interceptees.[20]

Again, you will want to ensure strict adherence with all of these requirements in your corruption investigation.

III. Legal Considerations

Litigation arising from wiretaps comes from various areas of the statute. Here are some of the most important, generally speaking:

1. Exhaustion/Necessity

Every eavesdropping warrant is required to have a statement as to other investigative techniques used prior to the submission of the wiretap according to 18 USC § 2518(1)(c).[21] The statement must include why the procedures tried have failed, or why they reasonably appear to be unlikely to succeed if tried, or are too dangerous.[22] Investigative techniques to exhaust before an eavesdropping warrant becomes necessary include:[23]

• Physical surveillance	• Undercover agents
• Public record checks	• Search warrants
• Pen registers	• Controlled purchases
• Trap and Traces	• Confidential Informants
• GPS tracking	• Covert cameras
• Analysis of toll records	• Tracking devices
• Trash seizures	• Subscriber information
• Financial investigation	• Mail cover

It is important that statements of necessity not become "boilerplate assertions," "unsupported by specific facts relevant to the particular circumstances of this case."[24] This was the holding from the Ninth Circuit, which suppressed an eavesdropping warrant on these grounds in *United States v. Blackmon*.[25] In that case, investigators began eavesdropping on a target, and through this wiretap developed probable cause to begin eavesdropping on the defendant's phone.[26] However, the necessity section of the eavesdropping warrant from the initial target's phone was, with the exception of a few alterations, "a duplicate" of the defendant's necessity section.[27] The *Blackmon* court made specific note that "no further investigative efforts were attempted in between the application" for the initial wiretap and the defendant's wiretap.[28] Thus, the Court suppressed the wiretap because the necessity section of the eavesdropping warrant contained "generalized statements that would be true of any narcotics investigation."[29]

2. Official must authorize the application

18 U.S.C. § 2518(4)(d) and § 2516(1) require all Title III applications to name the identity of the authorizing individual in a wiretap, and also limits the pool of Department of Justice officials who are empowered to authorize the application. This was the subject of litigation in United States v. Giordano. In this case, investigators obtained an eavesdropping warrant on a narcotics trafficker, which was not authorized by the attorney general or one of his designated assistants. Instead, the attorney general's executive assistant authorized the eavesdropping warrant, and in suppressing evidence from the wiretap, the Supreme Court held that an executive assistant's authorization was inconsistent with the language and legislative history of Title III.

3. Minimizing Non-Pertinent and Privileged Calls

a. Pertinent vs. Non-Pertinent

In any eavesdropping investigation, there will be both pertinent and non-pertinent conversations intercepted. Title III only authorizes the interception of calls that are "pertinent" to the criminal investigation. 18 U.S.C. § 2518(5) accounts for this by requiring that an investigation be "conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." There isn't a specific bright-line rule on proper minimization, which has led to substantial litigation over this part of the statute.

In Scott v. United States, investigators intercepted conversations about a conspiracy to import and distribute narcotics. Approximately 40 percent of the intercepted calls were narcotics-related. However, investigators listened to all calls, which included non-pertinent conversations between the target and her mother. In ruling that suppression was not appropriate in this case, the Court declined to assess the subjective intent of the investigator, instead ruling that there would need to be an "objective assessment of the actions of the officer or agent conducting the surveillance in light of the facts and circumstances confronting him at the time, without regard to his underlying intent or motivation." Objectively, the Court ruled, each recorded call could contain evidence of criminality, and this analysis would need to be done on a case-by-case basis.

United States v. North was one such case where the Fifth Circuit used an objective analysis to suppress evidence on the grounds that investigators did not follow minimization requirements. In North, prior to eavesdropping on the defendant's phone, investigators were given minimization instructions to initially listen to the conversation to determine whether it was pertinent or non-pertinent. If it was deemed non-pertinent, the investigator would cease monitoring the call, and then spot check the call to determine whether or not the conversation had veered toward criminality. However, in one intercepted call, the defendant admitted more than an hour into the conversation that he had narcotics hidden in his car. The defendant did not have any narcotics-related conversations for approximately an hour, and investigators minimized only eight times for an average of less than one minute each time. Based on this information, investigators arrested the defendant and charged him with possession of cocaine. In ruling to suppress the evidence derived from the wiretap, the court held that it was not objectively reasonable for agents to listen in for nearly one hour to a conversation that did not turn to criminal matters until the last few minutes.

Perhaps the most important of these categories in public corruption investigations is the attorney-client privilege, because so many public officials are lawyers themselves, and consult lawyers in connection with their professional duties.

a. Privileged Communications

A subcategory of non-pertinent calls is privileged communications, such as those between attorney-client, parishioner-clergyman, doctor-patient, and husband-wife. Perhaps the most important of these categories in public corruption investigations is the attorney-

client privilege, because so many public officials are lawyers themselves, and consult lawyers in connection with their professional duties. The consequences of improper minimization of these kinds of communications were specifically addressed in United States v. Renzi. In that case, investigators were given the following instructions regarding attorney-client communications:

> Unless otherwise addressed in this memorandum, never knowingly listen to or record a confidential conversation between a person and his or her attorney when other parties are not present. Anytime that an attorney or law office employee is a party to a conversation, call the agent supervising the interception. . . If it is determined that a conversation involving an attorney constitutes confidential legal consultation of any kind, notify the agent supervising the interception, shut off the monitor and stop recording.

In Renzi, investigators failed to minimize 37 attorney-client conversations, which the District Court held went beyond the scope of what was authorized by the wiretap. The court also took issue with the government concealing from the court in its reports that they were recording these kinds of conversations, even if it was subject to taint team review. Investigators also failed to identify as privileged and seal attorney-client calls that it inadvertently intercepted during the wiretap in violation of the Department of Justice's Electronic Surveillance Manual. The court, viewing the conduct in totality, suppressed the entire wiretap as opposed to merely suppressing the privileged calls.

In another case, however, dealing with the spousal privilege, the court decided against suppressing the whole wiretap. In United States v. Goffer, investigators on a securities fraud wiretap investigation were given a minimization packet, which included the following instructions:

> There is also a privilege concerning communications between spouses. You are to discontinue monitoring if you discover that you are intercepting a personal communication solely between husband and wife. If it appears that a third person is present during this communication, however, the communication is not privileged. So, too, if the communication deals not with private matters between husband and wife, but instead with ongoing as opposed to past violations of law, it is not a privileged communication.

The District Court found that 18 conversations between the defendant and his wife were not properly minimized. Of these 18, three specifically stood out to the court as "particularly egregious," bordering on "voyeuristic" where investigators listened to deeply personal and intimate discussions about their marriage. The court characterized the lack of minimization in relation to these calls "disgraceful," yet declined to suppress the entire wiretap. The court found that, on the whole, the wiretap was professionally conducted and generally well-executed, and that later in the investigation, calls between the defendant and his spouse were minimized within the first ten seconds of the conversation.

Thus, if your investigators do not minimize properly, the use of all or part of your wiretap at trial may be in jeopardy. Instructing your monitoring agents in this area is key to avoiding problems in this area. Sample minimization instructions are included in the appendix to this paper.

4. Sealing Requirements

Immediately upon expiration of the authorized wiretapping period, 18 U.S.C. § 2518(8)(a) requires the recording be made available to the judge and sealed under his directions in order to preserve the integrity of the evidence. In a case where the recording has not been properly placed under seal, the government must provide a "satisfactory explanation" for its failure to comply with the sealing requirement. In United States v. Cline, the government had a one-week delay in sealing recordings in a narcotics trafficking case because of the judge's court schedule. In

upholding the defendant's conviction, the Tenth Circuit found that there was no evidence of bad faith or tampering, nor did it find any tactical advantage in favor of the government as part of the delay.

5. Notice Requirements

18 U.S.C. § 2518(8)(d) requires that named interceptees, as well as parties to intercepted communications in the judge's discretion, be given notice that their calls were intercepted within 90 days. A violation of this part of the statute does not necessarily result in suppression of the wiretap, however. In United States v. Principie, investigators arrested several targets as a result of an eavesdropping investigation into forged United States savings bonds. The government did not provide notice to the named target, Principie, or to an unnamed target, Slomka. In declining to suppress the wiretap, the Second Circuit held that, on top of showing notice was not properly served within 90 days, there must be a showing of actual prejudice to the defendant. Principie could make no such showing. As it related to Slomka, the court ruled that since Slomka was not a named target to any of the eavesdropping warrants, notice was not required under § 2518(8)(d). Instead, it was up to the Judge's discretion, and the court found that not supplying notice to Slomka, who played a minor role in the conspiracy, was not an abuse of discretion.

Nearly forty years after the Principie decision, the New York State Court of Appeals issued a similar decision. In People v. Rodriguez, the Court similarly held that suppression was not warranted after investigators failed to properly notify defendant of the warrant until more than 90 days after it expired in violation of CPL § 700.50(3), a similar statute to § 2518(8)(d). The court held that the defendant received notice of the warrant at arraignment, and there was no showing of prejudice as a result of not being notified prior to arraignment.

IV. Strategic Issues to Consider in Public Corruption Wiretaps

There are numerous strategic issues specifically related to wiretaps in public corruption cases that you should consider before moving forward with an application. First, you need to decide whose calls to intercept. In many wiretap investigations, the ultimate target may be the obvious choice to intercept, but that may not be true in a corruption case for a variety of reasons. For one, in many corruption cases the target will be a politician or other high-ranking government official and many such people are lawyers, raising the specter of privilege issues that require significant minimization. Second, a high-ranking official target may be more careful about talking on the phone in an inculpatory manner than someone else in the target's circle would be, making a wiretap on the underling's phone more fruitful. Third, it is not uncommon for the person at the top of a criminal conspiracy to let others do the dirty work for him – this is true of public officials as well as drug kingpins – meaning the official's phone may not be the best choice because he is not personally handling all of the negotiations and transactions involved in the crime.

It is not uncommon for the person at the top of a criminal conspiracy to let others do the dirty work for him – this is true of public officials as well as drug kingpins.

For example, in the investigation of New York State Senate Majority Leader Dean Skelos, prosecutors decided to intercept the phone of Skelos's son Adam as well as Skelos's own phone. As it turned out, the charged scheme centered around Dean Skelos's solicitation of bribes in the form of money and employment for Adam, so Adam's phone captured vital evidence about that scheme. In addition, Adam Skelos was much less careful about what he said on the phone than Dean Skelos was, and prosecutors did not have to worry as much about privileged calls in connection with that interception because Adam Skelos is not a lawyer.

When a lawyer's phone is targeted extra care is required. Agents and prosecutors must make certain to identify all individuals who call the phone or who are called by the phone, to ensure that minimization is done properly. In advance, agents will have to identify all numbers that the targeted lawyer is likely to call that might create privilege problems, e.g. phone numbers at the target's law firm if he works at a firm, or his own lawyer's numbers if he is represented. And as with all cases, prosecutors will have to repeatedly emphasize the importance of proper minimization to all agents and officers sitting the wire. It also may be challenging to tell the difference between legal and political advice when a politician is consulting with his or her counsel, or when a politician's chief of staff is also a lawyer. These complications make staying on top of what is happening on the wire even more important than in the average case.

Another issue that arises with targets who are public officials is the importance of ensuring that the investigation is not, and does not appear to be, politically motivated. As far as the wiretap goes, that means that monitoring agents will need to be particularly careful of conversations between the target and other elected or high-ranking officials, and consider aggressively minimizing political conversations that are not obviously criminal. Regardless of the prosecutor's office involved in the case, whether it is the U.S. Attorney's Office, the Attorney General's office, or a District Attorney case, no prosecutor will want to face allegations that a case is politically motivated, and listening in too freely to a public official's conversations about political matters may add fuel to that fire.

For all of these reasons, it is essential to be proactive in acknowledging any minimization mistakes in your 10-day reports and in any requests to extend the wire. To the extent there is litigation over the wiretap – which should be expected in a public corruption case – you will want to have established that you were diligent in fixing any problems with monitoring promptly and completely, and that you disclosed everything to the judge as soon as practicable and before asking for an extension.

V. Conclusion

Eavesdropping continues to be one of the most effective ways of investigating and prosecuting cases in the United States in the right circumstances, and can be highly valuable evidence in a public corruption case. But corruption cases have unique challenges, so remember to keep all of the above practical and legal considerations in mind before pursuing this kind of investigation.

Endnotes

[1] *See* Title III of The Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20 (1970).

[2] The requirements described in this paper are the federal requirements under Title III. For the most part, the requirements for a wiretap application at the state law level are very similar, if not identical, to the requirements enumerated in the federal wiretapping statute. However, some states narrow the scope of situations in which law enforcement officials can obtain a wiretap; in other words, the federal law operates as a ceiling and not a floor.

For example, in Alaska and several other states, law enforcement officials can receive permission for a wiretap only when probable cause for specific enumerated crimes has been shown. This is in contrast to the availability of a wiretap for any crime that the federal statute permits (although the requirement for probable cause remains). Even more of an outlier, the state of Montana does not have a state wiretap law at this time. Prosecutors seeking to obtain a wiretap in Montana must do so under the federal statute in federal court.

[3] *See* Wiretap Report 2015, available at http://www.uscourts.gov/statistics-reports/wiretap-report-2015.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *See* 18 USC §§ 2518(3)(a)(b) & (d).
(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that--
(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter [18 USCS § 2516];
(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
….
(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.
[10] *Id.*
[11] *See* 18 USC §§ 2518(4)(a)&(c).
[12] *See* 18 USC § 2518(4)(d).
[13] *See* 18 USC §§ 2518(3)(c).
[14] *See* 18 USC § 2518(6).
[15] *See* 18 USC § 2518(1)(d).
[16] *See* 18 USC § 2518(5).
[17] *See* 18 USC § 2518(8)(a).
[18] *See* 18 USC § 2518(5).
[19] *See* 18 USC § 2518(9).
[20] *See* 18 USC § 2518(8)(d).
[21] *See* 18 USC § 2518(1)(c).
[22] *Id.*
[23] *See Generally United States v. Penaloza-Romero* 2015 U.S. Dist. LEXIS 76913 (D. Minn. 2015).
[24] *See United States v. Blackmon*, 273 F.3d 1204, 1210 (9th Cir. 2001).
[25] *Id.*
[26] *Id.* at 1206.
[27] *Id.*
[28] *Id.*
[29] *Id.* at 1211.