State of New York
Court of Appeals

OPINION

No. 41
The People &c.,
Respondent,
v.
Joseph Schneider,
Appellant.

Stephen N. Preziosi, for appellant.
Morgan Dennehy, for respondent.
District Attorneys Association of the State of New York, amicus curiae.

DiFIORE, Chief Judge:

The issue raised on defendant's appeal is whether a Kings County Supreme Court Justice had jurisdiction to issue eavesdropping warrants for defendant's cell phones, which were not physically present in New York, for the purpose of gathering evidence in an

investigation of enterprise corruption and gambling offenses committed in Kings County. To resolve defendant's jurisdictional challenge, we must decide whether the eavesdropping warrants were "executed" in Kings County within the meaning of Criminal Procedure Law § 700.05 (4). We hold that eavesdropping warrants are executed in the geographical jurisdiction where the communications are intentionally intercepted by authorized law enforcement officers within the meaning of CPL article 700. Accordingly, the order of the Appellate Division should be affirmed.

I

Law enforcement officers in Kings County conducted a two-year investigation into an illegal gambling enterprise. In the early stages of the investigation, an undercover agent met with defendant's accomplice, PD, and placed bets at a location in Kings County. A variety of investigative tools were used to identify coconspirators and gather evidence, including physical surveillance and the installation of a bugging device and video surveillance at the Kings County location. Investigators obtained eavesdropping warrants on the cell phones of multiple targets, including targets physically present in New York. Defendant's participation in the illegal gambling enterprise was uncovered when his telephonic communications were intercepted pursuant to a warrant authorizing eavesdropping on the cell phone of PD, who regularly came to Kings County in furtherance of the gambling enterprise. In the intercepted calls, defendant and PD were overheard discussing password-protected internet accounts on sports gambling websites, through which defendant controlled the usernames, passwords, betting limits, gambling lines and spreads for all his gambling clients.

The Kings County District Attorney applied for eleven successive eavesdropping warrants to intercept communications on three cell phones linked to defendant, at least two of which did not have subscriber information but were connected to defendant by voice identification. A Kings County Supreme Court Justice issued the warrants after finding probable cause to believe that defendant was engaging in designated gambling offenses in Kings County, mainly through his website "thewagerspot.com," and that "normal investigative procedures . . . reasonably appear[ed] to be unlikely to succeed," justifying the use of eavesdropping. The warrants, as provided by statute, directed the particular communications service providers that controlled and operated the telephone wires and other digital and computer systems that transferred the telephonic and electronic communications to "provide all information, facilities, and technical assistance" to law enforcement to execute the warrants in Kings County.

Defendant was subsequently indicted in Kings County, along with seven others, for enterprise corruption, promoting gambling and related crimes. Among other acts attributed to defendant, the indictment alleged that on seventeen specific dates between September 13, 2015 and January 3, 2016, in Kings County, defendant and his accomplices received or accepted five or more illegal sports wagers on each date through defendant's gambling website, totaling more than five thousand dollars on each occasion. Defendant moved to suppress the evidence obtained pursuant to the warrants.[1] He did not assert that the government interception of his communications violated his constitutional privacy

[1] Defendant's suppression motion addressed only one of the three intercepted phone numbers attributed to him.

interests. Nor did he dispute that the charges were properly brought in Kings County based on the commission of designated crimes in that location. Instead, as relevant here, defendant claimed that the Kings County Supreme Court Justice lacked the authority to issue the eavesdropping warrants because defendant and his cell phones were not located in New York and his intercepted communications involved call participants who were not physically present in New York and therefore execution of the warrants did not occur in Kings County. He also claimed that the People violated his due process rights, the separate sovereign doctrine and other constitutional limitations because California law does not include gambling offenses as designated crimes for eavesdropping.

The suppression court denied the motion, concluding that there was probable cause to believe that defendant committed the designated gambling crimes (CPL 700.05 [8]) in Kings County, that the warrant was executed at a facility in Kings County where the communications were overheard and accessed by authorized law enforcement, and the warrants were properly issued by a Justice in Kings County. The court further rejected defendant's claim that, under this approach, a judicial warrant allows law enforcement to "re-route phone calls being made anywhere in the country to Kings County and thereby have nation-wide jurisdiction." The court concluded that since the crimes were allegedly committed in Kings County, there was jurisdiction to prosecute the crimes and a sufficient nexus for the issuance of the eavesdropping warrants in that county.

Defendant entered a guilty plea to all counts of the indictment against him. The Appellate Division affirmed the judgment, holding that the suppression court properly denied defendant's motion to suppress the eavesdropping evidence because CPL article

700 authorized the Supreme Court Justice in Kings County to issue warrants that would be "executed" in that court's judicial district, meaning where the communications would be "intentionally overheard and recorded" (176 AD3d 979, 980 [2d Dept 2019], quoting CPL 700.05 [3] [a]). The Court also rejected defendant's claim that the warrants represented an unconstitutional extraterritorial application of New York state law. A Judge of this Court granted defendant leave to appeal (34 NY3d 1132 [2019]).

II

There is no dispute here that law enforcement agents must obtain a judicial warrant to intercept real time cell phone communications. Historically, the Fourth Amendment guarantee against unreasonable searches and seizures (US Const Amend IV) focused on whether the government obtained information by physical intrusions on constitutionally protected areas (*see Carpenter v United States*, __ US __, 138 S Ct 2206, 2213 [2018]; *Olmstead v United States*, 277 US 438 [1928]). However, over fifty years ago, it was established that "'the Fourth Amendment protects people, not places,' [which] expanded [the] conception of the Amendment to protect certain expectations of privacy'" (*Carpenter*, 138 S Ct at 2213, quoting *Katz v United States*, 389 US 347, 351 [1967]). Given the more modern appreciation "that property rights are not the sole measure of Fourth Amendment violations," a person's right to privacy has become the paramount concern in assessing the reasonableness of government intrusions, especially as "innovations in surveillance tools . . . ha[ve] enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," and courts must continue to "secure the privacies of life against

arbitrary power" (*id.* at 2213-2214 [internal quotations omitted]; *see also Katz*, 389 US at 351-352; *Riley v California*, 573 US 373, 381-382 [2014]).

In New York, article I, § 12 of the New York State Constitution authorizes the issuance of eavesdropping warrants as a law enforcement investigative tool to overhear and intercept telephonic communications, provided that certain safeguards against unreasonable privacy invasions are met. "[I]n addition to tracking the language of the Fourth Amendment" (*People v Weaver*, 12 NY3d 433, 438-439 [2009]), article I, § 12, adopted in 1938, provides in relevant part that:

> "[t]he right of the people to be secure against unreasonable interception of telephone and telegraph communications shall not be violated, and ex parte orders or warrants shall issue only upon oath or affirmation that there is reasonable ground to believe that evidence of crime may be thus obtained, and identifying the particular means of communication, and particularly describing the person or persons whose communications are to be intercepted and the purpose thereof."

New York State's express constitutional privacy protections for telephonic communications predated the United States Supreme Court's recognition of the Fourth Amendment protection against eavesdropping (*see Katz*, 389 US at 351-353; *see also People v Capolongo*, 85 NY2d 151, 158 [1995]). Yet, our early statutory procedure for obtaining evidence by wiretap order was struck down as unconstitutional under the Fourth Amendment due to the absence of additional protections, given the gravity of the privacy

invasion in overhearing the content of the communications (*see Berger v New York*, 388 US 41 [1967]).[2]

In response to United States Supreme Court decisions in *Katz* and *Berger*, which invalidated government eavesdropping operations based on their failure to employ adequate privacy protections (*see Capolongo*, 85 NY2d at 159), Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC § 2510 *et seq.*) (Title III), "imposing upon the States minimum standards for electronic surveillance" (*Capolongo*, 85 NY2d at 159; *see also* L 1969, ch 1147). States were permitted to adopt procedures and standards that were more restrictive than those imposed by federal law or to prohibit wiretapping completely (*see id.; see also* 18 USC § 2516).

Soon after Title III was enacted, our state legislature enacted CPL article 700, which sets forth the procedural mechanism for securing a court-ordered eavesdropping warrant (*see Capolongo*, 85 NY2d at 159). In enacting article 700, the state legislature sought to "afford law enforcement 'greater flexibility in the employment of eavesdropping as an effective weapon against crime' and, in particular, organized crime, 'where the obtaining of evidence for successful prosecutions is often extremely difficult'" (*People v Rabb*, 16 NY3d 145, 151 [2011], quoting Governor's Approval Mem, Bill Jacket, L 1969, ch 1147, 1969 NY Legis Ann, at 586). Complying with federal law, New York also gave effect to

[2] The federal exclusionary rule recognized in *Weeks v United States* (232 US 383 [1914]), prohibiting the use in federal court of any evidence seized in violation of the Fourth Amendment was extended to illegally seized wiretap evidence (*see Nardone v United States*, 302 US 379 [1937]). New York followed suit in 1962, enacting CPLR 4506, which barred admission of any eavesdropping evidence that was unlawfully obtained (*see Capolongo*, 85 NY2d at 158, citing L 1962, ch 308).

our "strong public policy of protecting citizens against the insidiousness of electronic surveillance" by requiring strict compliance with CPL article 700 (*see Capolongo*, 85 NY2d at 159-160). Issuance of the eavesdropping warrants based on demonstrated probable cause, which is not challenged here, satisfied the overarching constitutional privacy protections.

Before discussing the relevant statutory language as to what constitutes the point of execution of the warrant for the purpose of jurisdiction under CPL 700.05, some context with regard to the geographical predicates to conduct eavesdropping investigations and issue eavesdropping warrants is instructive. As a first principle, the court's jurisdiction to issue eavesdropping warrants is not boundless, but is limited by the rules of geographical jurisdiction set forth in our state constitution and CPL article 20. Under our State Constitution, a defendant generally has a right to be tried in the county where the crime was committed (*see People v Greenberg*, 89 NY2d 553, 555 [1997]; NY Const, art I, § 2). A person may be prosecuted in a particular county where conduct occurred establishing an element of an offense or an attempt or a conspiracy to commit such offense (s*ee* CPL 20.40 [1]). Even where no conduct was committed within the county, a person may be prosecuted there under certain circumstances, such as where the result of an offense "occurred within such county" (CPL 20.40 [2]; *see also* CPL 20.60 [3] [causing the use of a computer service in one jurisdiction from another jurisdiction is deemed a use in both jurisdictions]).

Once the jurisdictional predicate to prosecute the crime in a particular county is established, as it was here, then, under CPL 700.10 (1), "a justice may issue an eavesdropping warrant . . . upon ex parte application of an applicant who is authorized by

law to investigate, prosecute or participate in the prosecution of the particular designated offense which is the subject of the application." Because this was a county-based prosecution (*see* CPL 20.40), the prosecutor authorized to prosecute the designated crimes in that jurisdiction—the Kings County District Attorney—was the proper warrant applicant (*see* CPL 700.05 [5]).

Turning next to the operative statutory language governing the "manner and time of execution," CPL 700.35 (1) provides that "[a]n eavesdropping . . . warrant . . . must be executed according to its terms by a law enforcement officer who is a member of the law enforcement agency authorized in the warrant to intercept the communications . . . ." The law enforcement officers here were competent to execute the warrants because they were authorized to investigate and arrest defendant in the jurisdiction where the interception occurred (*see* CPL 700.05 [6]). Notwithstanding the dissent's suggestion that defendant had no connection to New York (dissenting op at 8), the investigation and prosecution of defendant and his accomplices based on their participation in the gambling enterprise that operated in Kings County are not challenged and were jurisdictionally sound (*see People v DiPasquale*, 47 NY2d 764, 765 [1979]; CPL 20.40; *see also People v Carvajal*, 6 NY3d 305, 312 [2005]).

Despite the satisfaction of the jurisdictional and probable cause predicates in this case as mandated by our constitution and CPL articles 20 and 700, defendant challenges the jurisdiction of a Supreme Court Justice presiding in Kings County to issue the eavesdropping warrants on the theory that the court acted extraterritorially. Specifically, defendant claims that the warrants were not "executed" in Kings County as required by

CPL 700.05 (4) because his cell phones were not physically located in New York and his communications occurred outside of New York.[3] Resolution of this discrete challenge depends on the statutory interpretation of the word "executed" as used in CPL 700.05 (4), a term that is not defined in CPL article 700. CPL article 700, which sets forth the procedural mechanism of securing a court ordered eavesdropping warrant, and Penal Law § 250.00, which contains definitions used in article 700, provide the framework to determine where the warrants targeting defendant's communications were executed.

When resolving a question of statutory interpretation, the primary consideration is to ascertain and give effect to the legislature's intent (*see Matter of Marian T.*, 36 NY3d 44, 49 [2020]). The starting point in determining legislative intent is to give effect to the plain language of the statute itself—"'the clearest indicator of legislative intent'" (*id.*, quoting *Majewski v Broadalbin-Perth Cent. School Dist.*, 91 NY2d 577, 583 [1998]). Additionally, when the language at issue is a component part of a larger statutory scheme, the language must be analyzed in context and the related provisions must be harmonized and rendered compatible (*see id.* at 49). We are also "governed by the principle that we must interpret a statute so as to avoid an unreasonable or absurd application of the law" (*People v Garson*, 6 NY3d 604, 614 [2006] [internal quotation marks and citations omitted]).

[3] Although defendant claims that his calls were not made to parties in New York, the suppression court specifically found in denying defendant's suppression motion that "defendants were calling people in New York state from California and as such, a clear connection is established with New York state and Kings County."

To begin, under CPL 700.05 (4), "any justice of the supreme court of the judicial district *in which the eavesdropping warrant is to be executed*" is authorized to issue an eavesdropping warrant (emphasis added). When section 700.05 (4) is read as an integrated whole and in a commonsense manner along with other sections of the CPL and correlative Penal Law definitions, the statute makes plain that a warrant is "executed" at the time when and at the location where a law enforcement officer intentionally records or overhears telephonic communications and accesses electronic communications targeted by the warrant. Contrary to defendant's theory, a plain reading of CPL article 700 demonstrates that "execution" of a warrant depends on the action of authorized law enforcement officers vis-à-vis the communications and does not depend on the location of a target, the target's communication devices or the participants engaged in the call. Indeed, wiretapping occurs upon "the intentional overhearing or recording of telephonic . . . communication[s]" and that statutory definition expressly excludes the actions of telecommunications providers in their normal operations (Penal Law § 250.00 [1]).

"Eavesdropping" contemplates the performance of specific acts by government actors in three ways—wiretapping, mechanical overhearing of a conversation, or intercepting or accessing of an electronic communication (*see* CPL 700.05 [1]). The judicial warrants here authorized interception of both telephonic and electronic communications. Telephonic communications, when "intentionally overheard or recorded . . . by means of any instrument, device or equipment," are "[i]ntercepted communication[s]"—as are electronic communications that are "intentionally intercepted and accessed" (CPL 700.05 [3]; Penal Law § 250.00 [6]). Given the inclusion of

telephonic communications in the definition of "intercepted communication," the dissent's view that the legislature inexplicably failed to authorize interception and "wiretapping" of telephonic communications occurring on cellular phones is meritless (*see* dissenting op at 10-11). Notably, under the dissent's rather absurd hypothesis, the government apparently could not eavesdrop on cellular communications even where a cell phone or call participant is located within New York's borders.

Mirroring the federal definition of a wire communication, this state defines telephonic communication as "*any aural transfer* made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable *or other like connection between the point of origin and the point of reception* (*including the use of such connection in a switching station*) . . . ." (Penal Law § 250.00 [3] [emphasis added]; *see also* 18 USC § 2510 [1]). An "aural transfer" means "a transfer containing the human voice at any point between and including the point of origin and the point of reception" (Penal Law § 250.00 [4]; *see also* 18 USC § 2510 [18]). In contrast, "electronic communication" includes the transfer of various signals and data transmitted by wire (Penal Law § 250.00 [5]). Based on these definitions, execution of the warrants occurs at the point where authorized law enforcement intentionally overhears or records the human voice contained in telephonic communications and intentionally accesses the transferred signals or data in the electronic communications.

The legislative history accompanying substantive amendments made to CPL article 700 and Penal Law § 250.00 in 1988 demonstrates that the revisions were designed to keep pace with emerging technologies "as well as to bring New York law into conformity with

the then-existing federal law [18 USCA § 2510 *et seq.*]" (William C. Donnino, Practice Commentaries, McKinney's Cons Laws of NY, Book 11A, Penal Law § 250.05; *see also* Senate Introducer's Mem in Support, Bill Jacket, L 1988, ch 744 at 8-9). Through the 1988 amendments, the legislature clearly intended to continue the availability of wiretapping to be accomplished by the overhearing of "cellular and cordless telephonic communications" (William C. Donnino, Practice Commentaries, McKinney's Cons Laws of NY, Book 11A, Penal Law § 250.05), and to add the ability to capture communications involving "various new forms of electronic communications" (Governor's Approval Mem, Bill Jacket, L 1988, ch 744 at 6). The statutory definitions of "eavesdropping and wiretapping" were revised at that time "to distinguish . . . the tapping of telephone and telegraph communications, the mechanical overhearing of conversations or discussion, and the interception of data transmission" based on emerging electronic technologies (Mem in Support, Bill Jacket, L 1988, ch 744 at 8). These amendments were enacted well after the Federal Communications Commission approved the use of cellular telephone services in 1981 (*see* Rep of Senate Judiciary Commn at 9, S Rep 99-541, 99th Cong, 2d Sess, 1986). Acknowledging that law enforcement would require technical assistance in executing warrants involving modern modalities for both telephonic and electronic communication, the legislature's 1988 amendments "authorize[d] courts to direct that providers *of wire or electronic communication* services furnish the applicant with necessary assistance to accomplish unobtrusi[ve] interception," which was codified in CPL 700.30 (9) (Letter from

Div. of Criminal Justice Servs., Dec. 23, 1988, Bill Jacket, L 1988, ch 744 at 12 [emphasis added]). [4]

To be sure, the rerouting of cell phone communications by third-party service providers to the point of execution by authorized law enforcement officers enables "interception" as authorized by the warrant to occur, but is not itself the court-ordered interception. Federal and state statutes expressly recognize that telephonic communications are aural transfers, in part, and are controlled by service providers between two points (*see e.g.* Penal Law § 250.00 [3]). Anticipating the use of emerging technologies in the commission of crime, both federal and state statutes have recognized for decades the necessity of third-party communications carriers to facilitate court-ordered interception through switching technology that enables the rerouting of calls. To that end, in 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) to preserve the government's ability, pursuant to court order, to intercept

[4] As previously stated, the notion raised by the dissent that the statute, as written, does not authorize eavesdropping on cellular communications is meritless. Defendant never identified any distinctions in the types of technology used in wiretapping or in rerouting or redirecting communications as a basis for his jurisdictional challenges. Nor did defendant make any claim that he had a reasonable expectation of privacy in the telecommunications providers' use of their own technology in transferring the communications point to point. The dissent's extended discussion of these unpreserved issues comparing early landline phones and digital and wireless methods of transfers of telephonic communications and the resulting analysis based on those distinctions (*see* dissenting op at 10-13) is flawed. The definition of telephonic communications under both state and federal law has remained the same because the transfer of the human voice still remains the communication to be intercepted. While both federal and state statutes account for the evolving technology used by the providers to transfer the communications, that evolving technology does not alter the essence of an aural communication, which is clearly subject to interception by eavesdropping.

communications involving technologies such as digital and wireless transmission modes (*see U.S. Telecom Assn. v FCC*, 227 F3d 450, 454 [2000]). Most significantly, the Act "[did] not alter the existing legal framework for obtaining wiretap . . . authorization," as CALEA was intended to "preserve the status quo" (*id.* at 455 [citation omitted]). Similarly, in New York, pursuant to CPL 700.30 (9), an eavesdropping order may direct communications service providers to "furnish the applicant information, facilities, or technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference" to the service customer. Contrary to the dissent's conclusion, private communication carriers do not "execute" the warrant (dissenting op at 16). Indeed, our state statute mandates that the court "*shall not direct the service providers to perform the intercept* or use the premises of the service provider for such activity" (CPL 700.30 [9] [emphasis added]). Plainly, under CALEA and CPL 700.30 (9), an order directing the telecommunications carrier, which alone controls the transfer of communications, to provide technical assistance to investigators is not the equivalent of an interception; rather, these statutes anticipate the rerouting of digital communications by third parties employing their up-to-date technology as a preparatory step to effectuate the execution of eavesdropping warrants by government agents.

When read in the context of this legislative history, the statutory scheme supports our holding: the Kings County Supreme Court Justice presiding in the jurisdiction where defendant's communications were overheard and accessed and therefore intercepted by authorized law enforcement agents had the authority to issue the warrants. No language in

the statutory scheme equates the place of interception with the variable points where cell phones or call participants are located.

Defendant nonetheless claims that a Kings County Supreme Court Justice's authority to grant eavesdropping warrants is, at best, limited to "anywhere in the state," citing CPL 700.05 (4)'s definition of a "justice" who may issue a warrant "to authorize the interception of oral communications occurring in a vehicle or wire communications occurring over a telephone located in a vehicle." However, that part of CPL 700.05 (4) has no application to this case. CPL 700.05 (4) mandates that when interception of communications in a vehicle or over a telephone located in a vehicle is to be made through a listening device that is "installed or connected" in the vehicle, the eavesdropping "warrant may be executed and such . . . communications may be intercepted anywhere in the state." Under this section, it is only when communications occurring in a vehicle are intercepted by an eavesdropping "device" that physically moves out of New York along with the vehicle that the justice is without authority to order extraterritorial interception (*see* Peter Preiser, Practice Commentaries, McKinney's Cons Laws of NY, Book 11A, CPL 700.05). That portion of section 700.05 (4) does not relate to the place of execution of a warrant involving the rerouting of communications of a cell phone to a fixed wire room, nor does it conflict with our conclusion that jurisdiction in this case is tied to the place of authorized call interception. No devices were physically connected or implanted in a phone or vehicle in this case and no physical listening device employed by the law enforcement officers traveled outside Kings County. Thus, the vehicle-related language of CPL 700.05 (4) is inapposite to the resolution of this appeal.

III

Because "the New York eavesdropping statute was intended to conform 'State standards for court authorized eavesdropping warrants with federal standards'" (*People v McGrath*, 46 NY2d 12, 26 [1978], quoting Governor's Mem, L 1969, ch 1147, 1969 NY Legis Ann at 586), federal court decisions interpreting the federal eavesdropping statute are useful as an aide in interpreting provisions of the New York statute that are patterned after the federal counterpart. However, as we explained in *People v Gallina* (66 NY2d 52, 56 [1985]), when the language of our state statute differs from the federal statute, the distinction is considered "purposeful" and the plain language of CPL article 700 controls.

The jurisdiction of federal courts to issue eavesdropping warrants is defined in 18 USC § 2518. The federal statute—like our state statue—authorizes federal judges of "competent jurisdiction" to issue such an order "authorizing or approving *interception* of wire, oral, or electronic communications *within the territorial jurisdiction of the court in which the judge is sitting*. . . ." (18 USC § 2518 [1] [emphasis added]). Beginning with *United States v Rodriguez* (968 F2d 130 [2d Cir 1992]), every federal Circuit Court interpreting the language of section 2518 (1) has endorsed a "listening post" rule, which focuses on the point of "interception" in analyzing a court's jurisdiction to issue such warrants (*see United States v* Jackson, 849 F3d 540, 551-552 [3d Cir 2017] [collecting federal Circuit Court cases]). In *Rodriguez*, the Second Circuit concluded that "interception" occurred at both the site of the target phone in New Jersey *and* at the "place where the redirected contents [were] first heard" in the Southern District of New York (968 F2d at 136). The *Rodriguez* court thus employed "the listening post rule" in holding that

a warrant for such interception was properly issued by a judge of the Southern District of New York because the communications were overheard at a location "within the territorial jurisdiction" of that court. The Second Circuit concluded that the listening post rule served the key goal of the eavesdropping statute, which was to protect constitutional privacy interests from law enforcement abuse while providing technological tools to advance designated criminal investigations when normal investigative procedures are insufficient (*id.* at 136).[5] Other high courts have also followed the federal "listening post rule," concluding that, under their respective state statutes modeled upon Title III, the location of cell phones or call recipients does not drive the analysis, and execution of a warrant occurs at the place of interception—even where both parties to the calls or communications are not within the state (*see e.g. State v Ates*, 217 NJ 253, 273 [2014]; *see also Davis v State*,

[5] 18 USC § 2518 (3) permits a federal judge to issue an eavesdropping warrant for interception "outside" the territorial jurisdiction of the court "but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction." Defendant claims here that this section provides federal judges, not state judges, with "express authority to issue eavesdropping orders outside of their geographical jurisdiction," and concludes that this means that a state judge can administer eavesdropping orders only "within its borders." Determinatively, defendant failed to preserve any issue of law for our review as to whether the eavesdropping orders issued here involved installation of a "mobile interception device" as defined in section 2518 (3). Thus, while there is an apparent split in the federal Circuit Courts as to the meaning of a "mobile interception device" (compare *United States v Ramirez*, 112 F3d 849, 853 [7th Cir 1997] ["mobile interception device" means "a device for intercepting mobile communications"] with *United States v Dahda* (853 F3d 1101, 1112-1113 [10th Cir 2017] ["mobile interception device" means "a listening device that is mobile"], *affd* on other grounds __ US __, 138 S Ct 1491 [2018]), we do not consider whether the cellphone fits the definition of a mobile interception device.

426 Md 211, 226-227 [2012] [collecting cases]).[6] Because both the federal and state statutes link a court's jurisdiction to issue warrants to the point of interception, the decisions of federal and state courts interpreting their similar statutory provisions support our conclusion here.

Given the ubiquity of cell phones and widespread use of the Internet, this interpretation of our statutory scheme, one in line with the federal "listening post rule," reaffirms that eavesdropping warrants are a critical tool in investigating large-scale crime syndicates operating in our state. Defendant's "multiple plant" theory, pursuant to which a court's authority to issue a warrant is dependent upon the location of targeted cell phones or call participants, is not workable. Nor does defendant's proposal for inter-agency "cooperation" provide a solution. Linking jurisdiction to the undetectable locations of cell phones and creating dependence on outside law enforcement agencies to investigate and prosecute very serious crimes committed in this state is unreasonable. It would result in a logistical scheme that leaves jurisdiction in flux, creates multi-state wire rooms with diffuse oversight responsibility and in many cases would eliminate eavesdropping as an investigative tool. More importantly, centralized oversight by a single issuing court of

[6] In *Ates*, the New Jersey Supreme Court rejected the defendant's arguments that New Jersey law enforcement officers exceeded their jurisdiction in intercepting communications in cell phone calls among participants that were out of state, "creat[ing] an 'artificial connection' to New Jersey" and that only a judge from the defendant's state of residence could authorize a wiretap. The court explained that those arguments disregarded the fact that the New Jersey Wiretap Act requires an actual nexus to the state before an eavesdropping order can be issued, which is met by a predicate finding of probable cause to believe that a designated offense under New Jersey law is being committed and that communications about criminal offenses occurring in that state may be obtained through eavesdropping (*id.* at 268).

competent jurisdiction over the eavesdropping investigation of designated New York crimes is critical to protect against abuses in the invasion of an individual's privacy in the communications—the paramount constitutional concern—and to ensure that any interception is necessary, properly minimized, and promptly terminated in accordance with constitutional safeguards (*see People v Rodriguez y Paz*, 58 NY2d 327, 335-336 [1983]). That crucial oversight is impossible under defendant's proposed construct, which was certainly not the legislature's intent in carefully designing this State's eavesdropping statutes.

Defendant's remaining claims that the warrants at issue violated his constitutional rights as a California resident, the separate sovereignty doctrine and other constitutional rights of the state of California are without merit.

Accordingly, the order of the Appellate Division should be affirmed.

WILSON, J. (dissenting):

I agree with the majority that the issue is "discrete": does Criminal Procedure Law § 700.05 authorize a New York court to issue a warrant commanding the diversion into New York of a cellular telephone call between a California resident who has never been to

New York and persons not resident or present in New York, so that New York officers may listen to it in New York? I conclude that the statute does not.[1]

I

Joseph Schneider is a lifelong resident of California who—prior to his arrest and extradition in June 2016—had never set foot in New York. At one time, Mr. Schneider operated his own gambling website. But beginning in April 2015 he began using facilities provided by a competitor (and fellow Southern California resident) Gordon Mitchnick, for which Mr. Schneider paid Mr. Mitchnick $30,000 per month. Mr. Mitchnick managed a network of "Master Agents" and "Agents" across the country and supported the websites those agents used to place bets on professional and collegiate sporting events. A team in San Jose, Costa Rica provided technical support. The operation required that Mr. Mitchnick and his associates employ a range of strategies to conceal payments made by customers and launder their profits.

The principal evidence against Mr. Schneider consisted of conversations recorded over the course of a six-month wiretap investigation beginning in December 2015. But in the initial warrant application, the People did not allege that Mr. Schneider had any contact

[1] As the majority notes, Mr. Schneider advanced no claim under the Fourth Amendment of the U.S. Constitution or article I, § 12 of the New York Constitution. Further, I agree with the majority that Mr. Schneider failed to challenge the jurisdiction of the Kings County court to prosecute him, though we must be careful not to confuse the question of the court's jurisdiction to prosecute Mr. Schneider based on evidence turned up through the wiretaps with the court's statutory authority to issue the wiretapping warrants in the first place. Finally, I would also reject Mr. Schneider's claims framed under the Full Faith and Credit Clause and his explication of California's public policy, at least in the manner in which he has presented those arguments.

with the state of New York or that he had any customers located in New York. Instead, they summarized four conversations between Mr. Schneider and a New Jersey-based bookmaker, Patrick Deluise, as evidence that Mr. Schneider operated a gambling website used by Mr. Deluise. During one of the calls, Mr. Deluise informed Mr. Schneider that he was in Florida: he did not mention his location in the remaining three, and the warrant application did not assert that Mr. Deluise was in New York when any of those calls took place. The application went on to describe Mr. Schneider's business as "national in scope," noting that he had placed calls to numbers in California, Arkansas, Colorado, Florida, Michigan, Hawaii and Nevada and pointing to three incoming calls from Costa Rica, where online gambling is legal. New York was not among the states listed, and the warrant application contained no suggestion that Mr. Schneider had communicated by phone with anyone located in New York. Nevertheless, Supreme Court issued the warrant and the wiretap commenced.

Over the course of six-months, investigators extensively documented Mr. Schneider's conversations with agents and customers in California, Nevada, Michigan and Costa Rica. But they failed to turn up any evidence that Mr. Schneider made or received calls to or from anyone located in Kings County. Indeed, during that period Mr. Schneider made no calls to anyone in New York, and received just one, from a number registered to an address in Kingston.[2] The People do not assert that any other evidence uncovered during

[2] Although the majority highlights the suppression court's finding that *other* defendants made calls to New York from California (majority op at 10 n 3), the prosecution's warrant applications failed to demonstrate that Mr. Schneider was communicating with individuals in New York.

their lengthy investigation demonstrated that Mr. Schneider had contacts with persons located in New York.

II

Although Mr. Schneider advances no argument under article I, § 12 of the New York Constitution, its explicit protections against unreasonable interception of telephone communication—absent from the Fourth Amendment—are important in interpreting Article 700 of the Criminal Procedure Law. The majority apparently agrees, by acknowledging that New York's constitutional protections for the privacy of electronic communications exceed what the Fourth Amendment provides, but draws from that acknowledgement the odd conclusion that New York's constitution was amended in 1938 to "authorize" eavesdropping as an investigative tool (majority op at 6). That claim mischaracterizes the explicit language of article I, § 12 and misinterprets the intention of the delegates who authored it.

In 1928, the constitutionality of wiretapping was presented to the U.S. Supreme Court, which held that the Fourth Amendment did not prohibit or constrain wiretapping so long as the wiretapping was performed outside of the target's home (*Olmstead v US*, 277 US 438, 465 [1928]). Thus, with no reason to suspect anyone of a crime, the police could climb a telephone pole, install a wiretap, listen, and use the evidence in criminal prosecutions. Or, if allowed by the telephone company, they could sit in a chair at the company's offices and do the same. *Olmstead* was met with swift public condemnation (*see, e.g.*, Forrest Revere Black, *An Ill-Starred Prohibition Case*, 18 Geo LJ 120 [1930];

Osmond K. Fraenkel, *Recent Developments in the Law of Search and Seizure*, 13 Minn L Rev 1 [1928]; Editorial, *Government Lawbreaking*, NY Times, June 6, 1928 at 24 ["Prohibition, having bred crimes innumerable, has succeeded in making the Government the instigator, abettor and accomplice of crime. It has now made universal snooping possible"]).[3]

At the New York Constitutional Convention of 1938, the delegates added article I, § 12 to the Constitution. Its first paragraph copies the US Constitution's Fourth Amendment verbatim, but the amendment added a second paragraph not found in the Federal Constitution:

> "The right of the people to be secure against unreasonable interception of telephone and telegraph communications shall not be violated, and ex parte orders or warrants shall issue only upon oath or affirmation that there is reasonable ground to believe that evidence of crime may be thus obtained, and identifying the particular means of communication, and particularly describing the person or persons whose communications are to be intercepted and the purpose thereof."

[3] In an about-face, the U.S. Supreme Court thereafter held that the Communication Act of 1934, which provided that "no person" may divulge an intercepted telephone communication to "any person," prohibited the use of wiretapped information in both federal (*Nardone v United States*, 302 US 379 [1937]) and state (*Weiss v United States*, 308 US 321 [1939]) prosecutions. The managers of the bill that became the 1934 Communications Act "repeatedly declared that it was designed solely to transfer jurisdiction over radio, telegraph, and telephone to a new agency, the Federal Communications Commission, and that 'the bill as a whole does not change existing law'" (Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Proposal*, 52 Colum L Rev 165, 174 [1952]). Thus, "the *Nardone* decision was generally regarded as a bit of judicial legislation, a policy decision by the Court that the increased need to curb a dangerously prevalent practice justified a somewhat liberal remolding of a statutory section" (*id*. at 175).

This second paragraph was a direct response to *Olmstead*. In a message to the convention, Governor Lehman emphasized the need to protect scrupulously against wiretapping, citing to Justice Brandeis' dissent in *Olmstead* for the proposition that "writs of assistance and general warrants are but puny instruments of tyranny oppression when compared with wire tapping" (Message of Gov. Lehman, 1 Revised Record of the Constitutional Convention of the State of New York at 339, quoting 277 US at 476 [Brandeis J., dissenting]; *see also* Speech of Delegate Thomas B. Dyett, 1 Rev Rec at 505, quoting 277 US at 474-475; Speech of Delegate Philip Halpern, 1 Rev Rec at 550). Article I, § 12 of the New York Constitution does not "authorize" wiretapping: rather, it expresses our State's fundamental distrust of the use of wiretapping and intention strictly to limit its availability.

The scope of Article 700 must be understood with that background in mind. In 1967, the Supreme Court overruled *Olmstead* (*see Katz v United States*, 389 US 347, 353 [1967]), and held that New York's eavesdropping statute failed to require that warrants "particularly [describe] the place to be searched, and the persons or things to be seized" as required by the Fourth Amendment (*Berger v State of NY*, 388 US 41, 55 [1967]). In response, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("OCCSSA"), which established minimum federal statutory requirements for applications for eavesdropping warrants and the orders themselves (*see* 18 USC § 2518). Title III requires states to provide at least the protections it specifies but does permit states to adopt more restrictive measures. As Chief Judge Kaye explained: "Beyond the question of authority, however, stands our strong public policy of protecting citizens against the insidiousness of electronic surveillance by both governmental agents and private

individuals. New York State has, therefore, responded to the problems raised by electronic surveillance with greater protection than is conferred under Federal law, and continues to assert this strong public policy, through evolving legislation, as technology advances" (*People v Capolongo*, 85 NY2d 151, 160 [1995]).

Given the protections enshrined in the Constitution and enacted by statute, our "strong public policy" requires that we interpret our eavesdropping statutes narrowly especially where—as here—the statute is silent on the question before us (*id*. at 162-163 [applying notice provisions of Article 700 to introduction of foreign wiretap evidence where statutory scheme is silent on the rules governing the admission of such evidence]). Likewise, nothing in Article 700's legislative history suggests any contemplation of the narrow issue presented here: whether a New York court can issue a warrant requiring a telephone company to divert a signal into New York when neither party to the call is located in New York or resides in New York. Contrary to the majority's assertion (majority op at 14 n 4), I completely agree that CPL article 700 authorizes a New York court to issue an eavesdropping warrant when the warrant application shows that a cellular telephone line is being used to communicate to or from New York; I am puzzled by what portion of my "rather absurd hypothesis" would have caused the majority to think otherwise.

III

The easiest way to expose the majority's error is to remove the verbiage and line up the opinion's substantive points: (1) New York has longstanding constitutional protections specifically for telephone communications absent in the federal constitution (majority op

at 6); (2) because of "New York's strong public policy" in protecting privacy, "strict compliance with CPL article 700" is required (*id.* at 7-8); (3) resolution of Mr. Schneider's claim turns on the word "executed", "a term that is not defined" (*id.* at 10); and (4) "the court's jurisdiction to issue eavesdropping warrants is not boundless, but is limited by the rules of geographical jurisdiction set forth in our State Constitution and CPL article 20" (*id*. at 8). Stripped bare, the majority claims that because New York has a long history of protecting privacy rights in telephone communications and the legislature did not say what it meant by "executed," the legislature meant to grant New York courts the ability to issue warrants to listen in on any cell phone calls between anyone in the United States, or perhaps in the world, so long as a U.S. telephone carrier can divert the call to New York. To the contrary, the obvious conclusion from those points is that we should not interpret an undefined term to permit New York courts to authorize the issuance of warrants requiring the diversion into New York of telephone calls between people with no connection to New York and which calls neither originated nor terminated in New York.

The history of New York's protections of privacy, both constitutional and statutory, establishes the desire to afford electronic communication at least as much protection as is provided for searches and seizures of tangible objects. Instead, the majority grants law enforcement an unlimited geographic reach not available for searches and seizures of physical property. For example, police officers must execute warrants in "the county of issuance or an adjoining county" or in another county within the state "if (a) his geographical area of employment embraces the entire county of issuance or (b) he is a member of the police department or force of a city located in such county of issuance"

(CPL 690.25 [2]). Similarly, police officers may not make arrests outside their geographic jurisdiction unless assisted by officers in the jurisdiction where the arrest is made (CPL 120.60; *see also People v Johnson*, 303 AD2d 903, 905-906 [3d Dept 2003]). Nor does our law permit law enforcement agents from another state to conduct a search under either a federal or out-of-state warrant (*see People v La Fontaine*, 92 NY2d 470 [1998]). Those rules reflect the fundamental importance of territoriality in the authorization of searches and seizures. If New York officers have probable cause to believe that the home of a Californian contains evidence relevant to the prosecution of New York crimes, they must —and do—obtain a warrant from a California court. How can we infer such a dramatic change from a word the legislature did not define?

IV

Even were we to ignore New York's longstanding commitment to the privacy of electronic communications and look at the statute in a vacuum (which is not what the majority advocates [*see* majority op at 6]), I could not arrive at the majority's conclusion. I start, as does the majority, with the fact that the statute is silent on the meaning of "executed" (*id*. at 10). CPL 700.05 (4) authorizes the issuance of an "eavesdropping warrant" by Supreme Court Justices "of the judicial district in which the eavesdropping warrant is to be executed." An "'[e]avesdropping warrant' means an order of a justice authorizing or approving eavesdropping" (CPL 700.05 [2]), and "'[e]avesdropping' means 'wiretapping,' 'mechanical overhearing of conversation,' or the 'intercepting or accessing of an electronic communication', as those terms are defined in section 250.00 of the penal

law" (CPL 700.05 [1]). Thus, CPL 700.05 permits the issuance of an eavesdropping warrant for three different types of surveillance.

Penal Law § 250.00 carefully differentiates between "wiretapping" and "intercepting or accessing of an electronic communication" in a way that is crucial to understanding what "execution" of a warrant means.[4] Telephonic communications are "wiretapped," defined as the "intentional overhearing or recording of a telephonic or telegraphic communication by a person other than a sender or receiver thereof, without the consent of either the sender or receiver, by means of any instrument, device or equipment" (PL § 250 [1]). In contrast, electronic communications are "intercepted" or "accessed" through the "intentional acquiring, receiving, collecting, overhearing, or recording … by means of any instrument, device or equipment" (PL § 250 [6]). Thus, the legislature authorized eavesdropping warrants that "intercepted or accessed" electronic communications but did not use those words when authorizing eavesdropping warrants of

[4] "Wiretapping" is "the intentional overhearing or recording of a telephonic or telegraphic communication by a person other than a sender or receiver thereof . . . by means of any instrument, device or equipment." A "telephonic communication" means "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station)" (PL § 250 [3]). "Aural transfer" is in turn defined as "a transfer containing the human voice at any point between and including the point of origin and the point of reception" (PL § 250 [4]). "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system" (PL § 250 [5]).

telephonic communications.[5] Telephonic communications are explicitly excluded from the definition of electronic communication (PL § 250 [5] [a]), further evidencing the legislature's determination to treat those two forms of communication differently. The Bill Jacket for the 1988 amendments to CPL Article 700 confirms the legislature's explicit differentiation between wiretaps of telephonic communication and the surveillance of other types of communications (Senate Introducer's Mem in Support, Bill Jacket, L 1988, ch 744 at 8).

---

[5] The majority contends that this argument is "meritless," pointing to CPL 700.05 (3)'s definition of "intercepted communication," which includes a) telephonic or telegraphic communications, b) conversations or discussions intentionally overheard and recorded, and c) "an electronic communication which was intentionally intercepted or accessed." However, "intercepted communication" does not bear on the meaning of "executed" in CPL 700.05 [4]. Rather, it is an omnibus term used throughout Article 700 to refer to all three types of communications that may be the targets of eavesdropping warrants (*see* CPL 700.35 [3] ["In the event an *intercepted communication* is in code or foreign language, and the services of an expert in that foreign language or code cannot reasonably be obtained during the interception period, where the warrant so authorizes and in manner specified therein, the minimization required by subdivision seven of section 700.30 of this article may be accomplished as soon as practicable after such interception"] [emphasis added]; CPL 700.50 [3] ["Within a reasonable time … written notice of the fact and date of the issuance of the eavesdropping or video surveillance warrant … must be served upon the person named in the warrant and other such other parties to the *intercepted communications* or subjects of the video surveillance as the justice may determine in his discretion is in the interest of justice. … The justice … may in his discretion make available to such person or his counsel for inspection such portions of the *intercepted communications* or video surveillance"] [emphasis added]; CPL 700.65 [1] ["Any law enforcement officer who, by any means authorized by this article, has obtained knowledge of the contents of any *intercepted communication* or video surveillance, or evidence derived therefrom, may disclose such contents to another law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure"] [emphasis added]; CPL 700.70 ["The contents of any *intercepted communication*, or evidence derived therefrom, may not be received in evidence or otherwise disclosed upon a trial unless the people, within fifteen days after arraignment and before the commencement of the trial, furnish the defendant with a copy of the eavesdropping warrant"] [emphasis added]).

Those distinctions reflect the manner in which wiretaps were carried out prior to the advent of cell phones. Historically, telephonic communication — and hence wiretapping — traveled point-to-point through vast networks of wires or cables. Law enforcement could simply splice the wire servicing the phone to be monitored with a wire terminating at the law enforcement agency (Micah Sherr et al., *Signaling Vulnerabilities in Wiretapping Systems*, 3 IEEE Security & Privacy 13, 14 [2005]). The wires could be joined either between the telephone and the first junction box or at a local telephone exchange (James G. Carr et al, Law of Electronic Surveillance § 1.2 [Oct. 2020 Update]). Thus, wiretaps were carried out in close geographic proximity to the intended target. The definition of telephonic communication provided in Penal Law § 250 (3), which emphasizes the transmission of communication over wires, cables or other similar connections, indicates that the Legislature expected that overhearing or recording telephone calls would require accessing wires, regardless of the device used. It follows that the Legislature would have assumed that wiretaps—the physical accessing of the signal—would be carried out within the jurisdiction of the law enforcement agency executing the warrant, because a New York officer could not obtain a warrant from a New York court to travel to California and splice a wire there.

However, intercepting a call placed from a cell phone requires very different technology. Cell phones do not operate solely through the use of wires. Although wires and cables carry the cellular signal through some points of its travel, substantial portions of the transmission—including the initial transmission by the caller and the final receipt by the recipient—are wireless. A cell phone converts the voice of the caller into an encoded

electrical signal and transmits it to a local cell phone tower via the electromagnetic spectrum (Rich Mazzola, *How Do Cell Phones Work? A Story of Physics, Towers, and the Government*, Medium [Oct. 7, 2015], https://medium.com/swlh/richmazzola-how-do-cellphones-work-a-story-of-physics-towers-and-the-government-8369aa7226b1). The tower then directs the signal to its intended destination, where the receiving cell phone decodes the signal, allowing the receiver to hear the sender's voice (*id*). Wiretaps of cellular phone calls are now carried out by telephone companies rather than law enforcement: the company decodes the signaling information and separates out the call audio to a new channel, which is then transmitted to the law enforcement agency (Sherr et al. at 15). That process does not require a physical connection to the tapped line (*id*). Therefore, as a technological matter, a wiretap of a call made to or from a cell phone need not occur in territorial proximity to the intended target.

The majority claims that the Legislature's 1988 amendments to Article 700 anticipated the rise of new technology (majority op at 12-13). That is correct. The legislature made an explicit definitional choice, by which all "telephonic communications"—both conventional and cellular—were expressly excluded from the definition of "electronic communication." Because even calls placed to and from a cellular telephone contain aural transfers "made in whole or part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection" and "electronic communication" "does not include[] any telephonic or telegraphic communication" (PL § 250.05 [5] [a]), the majority's reliance on citations to the legislative history and commentators relating to the 1988 amendments is not illuminating.

Indisputably, the legislature added a definition of "electronic communication" distinct from telephonic communication—for example, to capture "various new forms of electronic communication" (e.g., emails, FTP transfers, SMS messages) that are not "aural"—but its intention to permit eavesdropping of those "electronic communications" does not bear on the territorial limitations for the execution of wiretapping warrants.[6]

The only new *telephone* technology expressly addressed by the 1988 amendments was car phones, not the handheld mobile phones ubiquitous today.[7] The legislature's treatment of car phones in the 1988 amendments cannot be reconciled with the majority's position. According to the majority, the 1988 amendments permit any court in New York

[6] The majority cites McKinney's Practice Commentaries for Penal Law § 250.05 to support its view that "the legislature clearly intended to continue the availability of wiretapping to be accomplished by the overhearing of 'cellular and cordless communications'" (majority op at 13). However, the quoted language refers to the fact that under New York law "people are entitled to privacy in their telephonic communications, even if a portion of the conversation is transmitted by radio" (William C. Donnino, Practice Commentaries, McKinney's Cons Laws of NY, Book 11A, Penal Law § 250.05). McKinney's, in turn, cites to *People v Fata*, a 1990 case in which the Second Department concluded that the warrantless surveillance of cordless telephone conversations was illegal (159 AD2d 180, 185 [2d Dept 1990]). *Fata* references the 1988 amendments to distinguish between federal law (which explicitly excludes cordless telephones from its definition of wire communications that may not be intentionally intercepted without a warrant) and state law (which does not) (*id*). From that fact—and the broader protections afforded New York state citizens under our constitution—*Fata* concluded that "the Legislature intended to provide greater protection for the privacy of telephone communications than that available under the Federal eavesdropping statute" (*id*).

[7] The legislature's focus on car phones is understandable. In the late 1980s, hand-held mobile phones were a high-end luxury good used by less than one percent of Americans (*see* Michael Decourcy Hinds, *Consumer's World; Mobile Phones, as Prices Drop, Aren't Just for Work Anymore*, NY Times [June 10, 1989], https://www.nytimes.com/1989/06/10/style/consumer-s-world-mobile-phones-as-prices-drop-aren-t-just-for-work-anymore.html). In contrast, car phones were an increasingly common consumer good (*id*).

state to authorize the wiretap of a telephone call, diverted from anywhere in the country, so long as the police listen to the call somewhere within the court's judicial district. If that were so, the legislature would have had no need to provide that, for "wire communications occurring over a telephone located in a vehicle . . . such warrant may be executed and such oral or wire communications may be intercepted anywhere in the state." The legislature's specific statewide expansion of the interception of telephone calls made over car phones only is nonsensical under the majority's interpretation, because under the majority's reading of the statute, calls from car phones could be diverted to anywhere in the state even without the car phone provision. Thus, the majority's interpretation of the statute should be rejected under our settled rules of construction (*see Majewski v Broadalbin-Perth Cent. School Dist.*, 91 NY2d 577, 587 [1998]; *Matter of OnBank & Trust Co.*, 90 NY2d 725, 731 [1997; *Roosevelt Raceway, Inc. v Monaghan*, 90 NY2d 293, 305-306 [1961]).[8]

Furthermore, simply as a matter of commonsense, when a signal is diverted to bring it into New York, it is done so by command of a warrant. If the warrant is never executed, the signal will not be diverted; if the signal is diverted, it is diverted solely by execution of the warrant. The fact that the telephone company, rather than the police, conduct the physical diversion is of no legal importance. Private actors working at the behest of law enforcement are treated as law enforcement (*see People v Esposito*, 37 NY2d 156, 160

[8] Although I place little or no weight on failed legislative attempts, I note that in the 2001-2002 legislative term, S.B. 5793 was introduced; it would have authorized "roving interceptions" of telephone communications by eliminating the "specification of the facilities from which, or the place where, the communication is to be intercepted" in cases where the People could show that those limitations were "not practical." Had that bill's sponsor shared the majority's view, the bill would never have been introduced.

[1975]). Where a telephone company acting pursuant to a warrant diverts an out-of-jurisdiction telephone call, it has executed the warrant at a point outside the judicial district in which the issuing court sits, which Article 700 does not allow. The fact that it is later listened to within the judicial district of the issuing court does not erase the warrant's initial out-of-jurisdiction execution (*cf. United States v Rodriguez*, 968 F2d 130, 144 [2d Cir 1992] [Meskill J., concurring] ["The contents of the Imperio Café communications were *acquired* by law enforcement officials when they were diverted in New Jersey. In Manhattan the *previously acquired* contents were transformed into sound, but, because they were already within the control of law enforcement agents, they were not newly 'acquired.' I do not believe the contents of a communication become acquired anew each time they are transformed into a different medium"]).

In sum, the meaning of the term "execute" in CPL 700.05 (4) must be understood in the relevant historical context. At the time of the statute's enactment, wiretaps on telephonic communications would have been carried out by law enforcement physically tapping lines in close geographical proximity to the targeted subject. The legislature could not have imagined that a warrant could be "executed" simply by instructing a nationwide cellular phone company to redirect into New York an out-of-state electronic signal that never would have entered New York, containing conversation between two people not located in New York. The majority can point to nothing in the legislative history that suggests the legislature intended to grant New York courts the ability to divert purely out-of-state voice calls into New York state by issuance of a warrant.

The scattershot of arguments offered by the majority for its expansive interpretation of "execute" do not bear on the proper interpretation of the term. The various citations to the legislative history of the 1988 amendments and commentators' views thereof stand for the unremarkable proposition that, by defining "electronic communication" and subjecting such communications to eavesdropping, the legislature took steps "designed to keep pace with emerging technologies" (majority op at 12-13). That is precisely the point: the legislature understood that new technologies, such as email or FTP transfers, could be subjected to warranted surveillance. It permitted those defined "electronic communications" to be "intercepted or accessed," but purposefully excluded "telephonic communications" from that provision. The statute does not authorize courts to issue warrants that "intercept" or "access" telephone calls. Instead, it used a word with a settled territorial component—"execution:" of a warrant—to limit a court's authority to seize telephone calls.

V

Neither the federal nor foreign state caselaw relied on by the majority supports its position. I discuss each in turn.

A

The majority's reliance on the federal "listening post" rule says nothing about how to interpret the CPL. There is no suggestion that the CPL's definition of wiretapping or rules relating to wiretapping are derived from federal law, or that the choice of the word "execute"—which the majority contends is the key to New York's statute—was derived in

any way from a federal statute or caselaw. Indeed, the federal statutory scheme is quite different. The federal statute, 18 USC § 2518 (3), does not use the word "execute" at all. Instead, it provides that a "judge may enter an ex parte order … authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting." Interception is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device" (18 USC § 2510 [4]). Thus, the federal statute lumps together, without distinction, voice and all other electronic communication regardless of the type of means used to transmit the signal, and authorizes the "interception" of all such information through the use of any type of device, whereas New York differentiates between voice communications that use wire or cable for any part of the transmission (which includes cellular phone calls) from the transmission of other types of electronic communication, with different rules applying to each, as explained *supra* at 10-11.

Moreover, when it comes to the ability of a court to issue a warrant to divert an out-of-jurisdiction call into a jurisdiction, federal and state courts are quite different. Because use of wires (or radio frequencies allocated by the federal government) necessarily implicates interstate commerce, federal courts have nationwide jurisdiction. It is perfectly understandable that federal statutes, and federal courts' interpretation of those statutes, may have fewer concerns about the ability of a federal court to issue an order diverting a call using facilities of interstate commerce to a listening post anywhere in the United States. Not so with state courts: query whether New Yorkers would be content if a Mississippi

court authorized the wiretapping of calls purely between New York residents who have never set foot in Mississippi.[9]

Furthermore, there is no view of the OCCSSA under which states courts may authorize more expansive eavesdropping than federal courts. Whether a federal district court could authorize the wiretapping of a cellular phone conversation that neither originated nor terminated within the judicial district in which the issuing federal court sits is unsettled, as I explain below. For that reason alone, we should be hesitant to grant New York courts the authority to grant wiretapping warrants for telephone conversations that neither originate nor terminate in New York.

The majority's reliance on *United States v Rodriguez* (968 F2d 130 [2d Cir 1992]), is misplaced, because it did not involve the wiretapping of purely extraterritorial phone calls nor the wiretapping of cellular phone calls. In *Rodriguez*, law enforcement in the Southern District of New York obtained the wiretap warrant in question in connection with an investigation of a crack organization based in the Hunts Point section of the Bronx (*id.* at 133). The organization's operations extended to a restaurant in New Jersey (*id*. at 133-134). In connection with the investigation, wiretaps were placed on four telephones at the New Jersey restaurant and the apartment of one of the conspirators in the Bronx (*id*. at 134). The calls were monitored at the Drug Enforcement Administration headquarters in

[9] The majority's reliance on the Communications Assistance for Law Enforcement Act (CALEA) and CPL 700.30 (9) is misplaced (majority op at 14-15). Both CALEA and CPL 700.30 (9) require telecommunications carriers to assist in the seizure of telephonic and electronic communications authorized by a proper warrant, but neither statute expands or contracts the territorial jurisdiction of courts, whether state or federal, to issue warrants.

the Southern District (*id*. at 135). The warrant application thus facially established that calls made from the New Jersey phone numbers were being made to a telephone in New York, and a telephone in New York was being used in furtherance of the crack operation. Those calls were between conventional land lines, carried by wire or cable, which necessarily physically traversed New York. Here, in contrast, the warrant application did not establish probable cause (or, indeed, any reason to believe) that Mr. Schneider's phone was making or receiving calls to or from New York, and the calls would not have entered New York but for their seizure pursuant to the warrant.[10] It is also important to note that in *Rodriguez*, Judge Meskill separately concurred. He emphasized his disagreement "with the majority's treatment of the wiretap issue, which effectively repeals 18 USC § 2518 (3)'s requirement that a judge may only enter an order authorizing the interception of communications 'within the territorial jurisdiction of the court in which the judge is sitting'" (*id.* at 143-44). As he explained:

> "I cannot join the majority in holding that the unilateral decision of law enforcement agents as to where to set up their listening post can grant authority to a judge in any jurisdiction to authorize a phone tap in any other jurisdiction. . . .The heart of the definition of 'intercept' in 18 U.S.C. § 2510(4) is the 'acquisition of the contents' of a communication. The contents of the Imperio Cafe communications were *acquired* by law

[10] The Second Circuit interpreted the federal definition of "interception" to mean both the location where "the contents of a wire communication are captured or redirected" and "where the redirected contents are first heard" (968 F2d at 135-136). Thus, it read the federal statute to authorize the diversion of the signal "through the use of any electronic, mechanical or other device" as explicit statutory authority to order the out-of-state wiretaps on the New Jersey phones. New York law contains no analogous provision for telephone wiretapping and, indeed, uses "interception" when authorizing eavesdropping of electronic communications only, not telephonic communications.

> enforcement officials when they were diverted in New Jersey" (*id.* at 144).

In *United States v Ramirez* (112 F3d 849 [7th Cir 1997]), the Seventh Circuit considered whether a federal district court could issue an eavesdropping warrant for a cellular phone call where the communication neither originated nor terminated within the judicial district of the issuing court. It concluded that the 1986 Electronics Communications Privacy Act, which authorized federal—but not state—courts to intercept "wire, oral, or electronic communications . . . outside [the district court's] jurisdiction but within the United States in the case of a mobile interception device" allowed a federal district court to intercept cellular telephone signals anywhere in the United States (*id.* at 853). It interpreted the phrase "mobile communication device" to mean "a device for intercepting mobile communications," not "the irrelevant mobility or stationarity of the device" (*id*). By relying on the "mobile communication device" provision, which applies only to federal courts, the Seventh Circuit implicitly decided that without that provision, a federal court could not issue eavesdropping warrants for communications occurring solely outside its judicial district. Indeed, the "mobile communication device" amendment expanding jurisdiction beyond the federal court's judicial district would be meaningless if courts could issue extra-jurisdictional warrants without it. Because that "mobile communication device" expansion was provided for federal courts only, both *Ramirez* and the ECPA suggest that state courts do not have the ability to issue eavesdropping warrants for wholly out-of-state communications.

More recently, the Fifth Circuit, in *United States v North* (728 F3d 429 [5th Cir 2013]) issued a decision holding that federal district courts may not divert cellular telephone calls into their jurisdictions and establish listening posts there, but then withdrew the decision and substituted it with a decision suppressing the wiretap on the ground of lack of minimization (735 F3d 212, 216 [5th Cir 2013]). However, the concurring opinion of Judge DeMoss sets out the rationale of the withdrawn opinion, which rejects the Seventh Circuit's construction of "mobile communication device," concluding that it refers to interception devices that themselves are mobile—not the interception of mobile phone communications (*id.* at 217-18).

Subsequently, in *United States v Glover* (736 F3d 509 [DC Cir 2013]), the court rejected the Seventh Circuit's interpretation of "mobile communication device," noting that "[a]ccording to a Senate Judiciary Committee report, the objective of the language was to ensure that warrants remain effective in the event a target vehicle is moved out of the issuing judge's jurisdiction *after* a warrant is issued, but before a surveillance device can be placed in the vehicle" (*id*. at 514). Most recently, in *United States v Dahda* (853 F3d 1101 [10th Cir 2017], *affd on other grounds*, 138 S Ct 1491 [2018]), the Tenth Circuit likewise concluded that "mobile communication device" meant a device that itself was mobile (*id*. at 1114 ["For example, some scholars point to small mobile devices such as 'IMSI catchers,' which are capable of intercepting the content from cell phone calls" (*id*. at 1113 n 4)]).

My point is not that the law is settled as to whether a federal court could issue an eavesdropping warrant to divert a purely out-of-state conversation into the judicial district

in which the court sits, where the warrant fails to establish that the warrant's target had ever made calls to that district or set foot in that district. To the contrary, my point is that the federal law is unsettled and, however great the federal jurisdiction might be, the jurisdiction of a state to authorize eavesdropping of purely out-of-state phone conversations can be no greater, and is likely lesser.

B

Additionally, the majority points to the adoption of the listening post rule by two other states' high courts. Those states, however, have markedly different statutory provisions from New York's and different state constitutional backdrops against which both legislative and judicial decisions should be framed. The majority cites to the New Jersey high court's decision in *State v Ates* (217 NJ 253, 271 [2014]) and that of Maryland in *Davis v State* (426 Md 211, 218 [2012]). The New Jersey wiretapping statute provides "[a]n order authorizing the interception of a wire, electronic or oral communication may be executed at any point of interception within the jurisdiction of an investigative or law enforcement officer executing the order," and defines the "point of interception" as "the site at which the investigative or law enforcement officer is located at the time the interception is made" (NJ Stat Ann 2A:156A-12; NJ Stat Ann 2A:156A-2v). New York uses "execution" of the warrant instead of "interception" of the signal and lacks New Jersey's statutory direction that the point of interception is where the listening officer is located.

Maryland's wiretapping law supports my position, not the majority's. Until Maryland's legislature amended its wiretapping law in 1991, eavesdropping warrants were

limited to calls occurring "within the jurisdiction of a particular circuit court"; the 1991 amendment "obviated the need for law enforcement agents to obtain multiple ex parte orders for each jurisdiction where a mobile phone might be located and allowed them to apply for one ex parte order in the jurisdiction where the 'base station' was located" (*Davis*, 426 Md at 222). Even so, in *Perry v State* (357 Md 37 [1999)]) and *Mustafa v State* (323 Md 65 [1991]), Maryland's Court of Appeals held that communications intercepted in another state are inadmissible at trial if they would violate the Maryland wiretap statute had they been intercepted in Maryland. In response, the legislature amended its law once again to authorize "certain out-of-state interceptions" (426 Md at 222, citing 2001 Md Laws 370). Then, in 2002, the legislature again amended Maryland's wiretapping statute to broaden its reach. Only in view of the repeated legislative efforts to expand the reach of its courts, and Maryland's use of the word "interception" which copied the federal statutory authorization, did the Maryland Supreme Court conclude that its statute should be read to reach extraterritorially. In contrast, New York's statutory scheme is different and evidences neither the words nor the legislative history that would render comparison to New Jersey or Maryland apposite.

VI

Last, in a pronouncement having nothing to do with the statutory language or legislative intent, the majority proposes a fusillade of policy justifications in support of its position. It is worth quoting them just to have them in mind:

- It is "not workable" if "a court's authority to issue a warrant is dependent upon the location of the targeted cell phones or call participants" (majority op at 19);

- "Linking jurisdiction to the undetectable locations of cell phones or callers and creating dependence on outside law enforcement agencies to investigate and prosecute very serious crimes is unreasonable" and "would result in a logistical scheme that leaves jurisdiction in flux; creates multi-state wire rooms with diffuse oversight responsibility and in many cases would eliminate eavesdropping as an investigative tool" (*id*);

- "More importantly, centralized oversight by a single issuing court of competent jurisdiction over the eavesdropping investigation of designated New York crimes is critical to protect against abuses in the invasion of an individual's privacy in the communications—the paramount constitutional concern—and to ensure that any interception is necessary, properly minimized and promptly terminated in accordance with constitutional safeguards" (*id*. at 19-20);

- "That crucial oversight is impossible under defendant's proposed construct, which was certainly not the legislature's intent in carefully designing this State's eavesdropping statutes" (*id*. at 20).

The astonishing feature of the majority's policy arguments is that they are pure conjecture. These policy arguments are based on nothing—not facts found below, not facts in the record, not even facts found by the majority from extra-record sources.

Here, instead, are some facts that render the majority's policy arguments untenable. First, both state and federal courts are required to report to the Administrative Office of the United States Courts all wiretaps sought, granted and denied (*see* 18 USC § 2519). For the eleven years from 2009-2019, state and federal courts together received 36,127 wiretap applications (*Table Wire 7 – Wiretap*, US Courts [Dec 31, 2019], available at https://www.uscourts.gov/statistics/table/wire-7/wiretap/2019/12/31). Thirty-six thousand, one-hundred eighteen applications were granted: only nine were denied (*id*). Not a single state or federal wiretap request was denied in 2017, 2018 or 2019 (*id*). So the idea

that crucial, strict oversight of wiretaps would be eroded if, for example, an officer from New York had to go to a California court to seek authorization for this very wiretap, is wholly fictional: there is no oversight to erode, because 99.975% of wiretap applications are granted.

Likewise, the idea law enforcement would be drastically impaired if officers from one jurisdiction had to cooperate with those in another—for example, if the officers here had to seek a warrant from the federal district court or a California state court instead of a New York state court—has no support in fact. Federal law enforcement agents frequently seek warrants in state courts. As an example, by 2014, the DEA was sending more than 60% of its wiretap applications to state courts, including a DEA operation with California state prosecutors that "built a wiretapping program that secretly intercepted millions of calls and text messages based on the approval of a single state-court judge" (Brad Heath, *DEA Changes Wiretap Procedure After Questionable Eavesdropping Cases*, USA Today [Jul. 7, 2016, 2:09 PM], https://www.usatoday.com/story/news/2016/07/07/dea-changes-wiretap-procedure-after-questionable-eavesdropping-cases/86802508/).

As Mr. Schneider points out, the People readily sought and obtained warrants in California state court for his arrest and a search of his home. Perhaps doing so was not quite as rapid as it would have been if a New York court could have issued the warrant for his arrest, but no facts support the majority's doomsday pronouncements, which should be viewed with great skepticism, as the U.S. Supreme Court has admonished:

> "[W]e have found no empirical statistics on the use of electronic devices (bugging) in the fight against organized crime. Indeed, there are even figures available in the wiretap

> category which indicate to the contrary. . . . Some may claim that without the use of such devices crime detection in certain areas may suffer some delays since eavesdropping is quicker, easier, and more certain. However, techniques and practices may well be developed that will operate just as speedily and certainly and—what is more important—without attending illegality" (*Berger,* 388 US at 60).

The proposition that the majority's holding will better ensure that "the invasion of an individual's privacy …—the paramount constitutional concern" is "properly minimized" runs headlong into a different set of facts (majority op at 20). New York accounts for a little less than 6% of the total United States population, yet in 2019, New York state courts accounted for 28% of all wiretap applications granted by all state courts (*Wiretap Report 2019*, US Courts [Dec. 31, 2019], https://www.uscourts.gov/statistics-reports/wiretap-report-2019). In contrast, the United States District Court for the Southern District of New York, which granted the greatest number of federal wiretap applications of any federal district court, accounted for just 4% of the federal total (*id*). Adding in the other New York federal district courts brings the New York federal court total to just 5.9% of all federally-issued warrants nationwide (*see Table Wire A1- Appendix Tables Wiretap*, US Courts [Dec. 31, 2019], available at https://www.uscourts.gov/statistics/table/wire-a1/wiretap/2019/12/31). Thus, compared either to the rest of the nation or the federal courts in New York, New York's prosecutors, aided by the New York state courts, are wiretap-happy—hardly fulfilling the Constitution's paramount concern to protect the privacy of New Yorkers touted by the majority. One should not expect the majority's grant of nationwide wiretapping authority to New York courts to provide enhanced protection of the right to privacy given the above data.

Yet one bit of truth in the majority's policy pronouncements is borne out by the facts: requiring New York law enforcement officials who desire to wiretap conversations not originating or terminating in New York, and not from or to a New York resident, to obtain authorization from either a federal court or the court of some other appropriate state may occasionally "eliminate eavesdropping as an investigative tool" (majority op at 19). In dissent in *Olmstead*, Justice Brandeis rejected the worth of that complaint in words of unequalled elegance:

> "Our Government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that, in the administration of the criminal law, the end justifies the means — to declare that the Government may commit crimes in order to secure the conviction of a private criminal — would bring terrible retribution. Against that pernicious doctrine this Court should resolutely set its face (277 US at 468)."

Wiretapping is a crime under our Penal Law. Neither the text nor the legislative history of CPL Article 700 suggests that the legislature authorized our courts to issue warrants commanding the diversion of purely out-of-state telephone calls between nonresidents so that they could be listened to by New York law enforcement agents. Firmly convinced thereof, I respectfully dissent.

Order affirmed. Opinion by Chief Judge DiFiore. Judges Stein, Fahey and Garcia concur. Judge Wilson dissents in an opinion, in which Judge Rivera concurs.

Decided June 3, 2021