22-P-870 Appeals Court

COMMONWEALTH vs. THANH DU.

No. 22-P-870.

Suffolk. June 7, 2023. - October 6, 2023.

Present: Wolohojian, Singh, & Hand, JJ.

Controlled Substances. Electronic Surveillance. Cellular Telephone. Search and Seizure, Electronic surveillance. Evidence, Wiretap. Statute, Construction. Practice, Criminal, Motion to suppress. Words, "Oral communication," "Wire communication," "Interception," "Secretly," "Contents."

Indictments found and returned in the Superior Court Department on January 8, 2020.

A pretrial motion to suppress evidence was heard by Catherine H. Ham, J.

Applications for leave to prosecute an interlocutory appeal were allowed by Dalila Argaez Wendlandt, J., in the Supreme Judicial Court for the county of Suffolk, and the appeals were reported by her to the Appeals Court.

Paul B. Linn, Assistant District Attorney, for the Commonwealth.

Nancy Dolberg, Committee for Public Counsel Services, for the defendant.

WOLOHOJIAN, J. An undercover Boston police officer, using a cell phone, made surreptitious audio-visual recordings of three purchases of drugs from the defendant. Each recording was made without the defendant's knowledge or consent, and without obtaining a warrant. The question presented in these interlocutory cross appeals is whether the Massachusetts communications interception statute (statute or wiretap statute),[1] G. L. c. 272, § 99, requires that the recordings be suppressed. We conclude that it does.

The facts are undisputed.[2] Each of the three drug transactions at issue followed the same pattern. Before meeting with the defendant, an undercover officer used a software

---

[1] In Commonwealth v. Thorpe, 384 Mass. 271, 272 (1981), cert. denied, 454 U.S. 1147 (1982), the Supreme Judicial Court referred to the statute as the "Massachusetts communications interception statute," which more accurately describes the statute than the more commonly used colloquial shorthand "wiretap statute," because the statute's scope extends to the secret interception of communications by a variety of electronic means, not simply wiretaps. See, e.g., Commonwealth v. Yusuf, 488 Mass. 379 (2021) (stored body camera video footage); Commonwealth v. Moody, 466 Mass. 196 (2013) (text messages transmitted over cellular network); Commonwealth v. Tavares, 459 Mass. 289 (2011) (concealed recording device). Accordingly, although we sometimes refer in this opinion to the statute as the "wiretap statute," we do so without intending to suggest any narrowing of its reach.

[2] We recite the facts as found by the judge, supplemented by undisputed testimony of the officer who testified at the suppression hearing and by our own observations of the three recordings, which were admitted at the evidentiary hearing and are part of the appellate record.

application[3] on his cell phone to begin an audio-visual communication (call)[4] with officers who were located nearby conducting surveillance (remote officers). This software application was designed to enable (and did, in fact, cause) the undercover officer's cell phone to transmit to the remote officers all audio and video captured by the undercover officer's cell phone during the call. The remote officers could (and did) observe and listen "live" to the calls as they were being transmitted. At the same time, the undercover officer's cell phone also transmitted the audio-visual recordings to the

[3] The application is called Callyo, which was described at oral argument as an electronic tool designed to aid law enforcement in a variety of investigatory ways. Examples of the uses to which Callyo has been put in police investigations can be found in United States vs. Powell, U.S. Dist. Ct., No. 18-CR-30042 (S.D. Ill. Mar. 17, 2020) (recording, storage, and download of call involving confidential informant); People v. Lewis, 2020 IL App (2d) 170900, aff'd, 2022 IL 126705 (interception and recording of text messages); State v. Bilgi, 19 Wash. App. 2d 845 (2021) (interception and recording of text messages).

[4] On the first and second occasions, the call began over ten minutes before the undercover officer met the defendant; on the third, it began two minutes before. During these periods, the undercover officer would report information such as where the defendant told him to meet, that the defendant was approaching, or what the defendant was wearing. The video captured the officer's location and surroundings as he either stood waiting or while walking to meet the defendant.

"cloud,"[5] where they were stored. The participating officers knowingly consented to this arrangement.

The drug purchases were made in public places chosen by the defendant, who arrived on foot. Two of the transactions took place on sidewalks, and the other took place in a store parking lot. On each occasion, the officer purchased one hundred dollars' worth of narcotics from the defendant,[6] a suspected street dealer.[7] When the defendant arrived within range of the undercover officer's cell phone, his voice and image were recorded and transmitted without his knowledge or consent. Although the defendant knew that he was orally communicating with a drug purchaser, he did not know that (1) the purchaser was also an undercover police officer, (2) the undercover officer was audio-visually recording the interaction, (3) the

---

[5] "Cloud computing" is "the practice of storing regularly used computer data on multiple servers that can be accessed through the Internet." Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/cloud%20computing [https://perma.cc/D6VT-G8GG]. See Commonwealth v. Gelfgatt, 468 Mass. 512, 536 (2014) (Lenk, J., dissenting) (definition of cloud computing); G. Jacobs & K. Laurence, Professional Malpractice § 17.1 n.8 (Supp. 2022).

[6] On the first occasion, the undercover officer bought three bags of drugs (one cocaine, one fentanyl, one inconclusive); on the second and third occasions, the officer purchased two bags of fentanyl.

[7] Based on text messages stored on the cell phone of a person who had died of an overdose, the police "cold called" the defendant to see if he would sell them drugs.

audio-visual recording was being transmitted to the remote officers, who were observing and listening live, or (4) the recording was also being transmitted to the cloud, where it was being intercepted, recorded, and stored. As would naturally be expected in the context of an undercover investigation, the police kept all of these matters secret from the defendant.

Once the drug purchases were finished and the defendant had walked away, the undercover officer used a verbal code to report to the remote officers that the transaction had been completed. Each recording was then terminated. Later, one of the remote officers downloaded copies of the recordings from the cloud onto a disc. Although it is not stated explicitly in the record, it is self-evident that the further recording onto a disc also happened without the defendant's knowledge or consent.

The defendant was charged with multiple counts of distributing class A and B substances as a subsequent offender, in violation of G. L. c. 94C, §§ 32 (a), (b), and 32A (a), (b). He moved to suppress the recordings on the ground that they violated the wiretap statute, G. L. c. 272, § 99; he did not raise any constitutional ground for suppressing the recordings. The Commonwealth made two arguments in opposition. First, it argued that the recordings fell within the exception to the wiretap statute where police have a reasonable suspicion that the defendant is engaged in a designated offense in connection

with organized crime. See G. L. c. 272, § 99 B 4, 7. Second, it argued that the defendant had no reasonable expectation of privacy in public places.

After an evidentiary hearing at which the only witness was the remote officer who downloaded the recordings, whose testimony the judge credited, the judge suppressed the audio portion of the recordings but did not suppress the video portion. The judge concluded that the video portion need not be suppressed because the defendant did not move to suppress it; this was incorrect -- the defendant's motion was not so limited. As to the audio portion of the recordings, the judge found that the defendant had a reasonable expectation of privacy, under art. 14 of the Massachusetts Declaration of Rights, in his "low-volume" one-on-one conversations with the undercover officer, even though they occurred in public settings. The judge then analyzed the evidence to determine whether the Commonwealth had proven a reasonable suspicion that the defendant was selling drugs as part of organized crime, and concluded that it had not:

> "Here, except for [the defendant], the police did not know the identity of any other members of [a] narcotics distribution organization. There is an assumption by the police that [the defendant] is working with others to distribute narcotics. There is no evidence that [the defendant] is working with anyone. Therefore, there is no organized conspiracy to distribute narcotics, as only one person cannot conspire with himself. Where the Commonwealth has not met its burden that the crime [was] engaged in by multiple players, although drug dealing can

> be [a] nexus to organized crime, the statute['s] exception has not been met."

Accordingly, the judge suppressed the audio portion of the recordings, expressly noting that the undercover officer would be permitted to testify to his own recollections of the transactions at trial. Both the Commonwealth and the defendant sought leave to pursue interlocutory appeals from the judge's decision. These were allowed by a single justice of the Supreme Judicial Court, who referred the appeal to this court.[8] It is in this posture that the case is now before us.

Discussion. It is important to note at the outset that the defendant did not below -- nor does he here -- argue that the surreptitious recordings should be suppressed under the Fourth Amendment to the United States Constitution or art. 14. Instead, the defendant argues that the recordings must be suppressed under G. L. c. 272, § 99 P, which has its own exclusionary provision. The statute provides for the exclusion from evidence of "the contents of any intercepted wire or oral communication or evidence derived therefrom," if the communication was intercepted in violation of the statute. G. L. c. 272, § 99 P. Thus, the core question presented in this

[8] The single justice denied the defendant's petition to the extent it sought interlocutory review of the judge's decision not to suppress the fruits of a warrantless search and seizure.

appeal is whether the audio-visual recordings violate the statute. If they do, then their "contents" -- as that term is defined by the statute -- are to be suppressed under § 99 P. See Commonwealth v. Gonzalez, 426 Mass. 313, 315 (1997) (recordings made in violation of wiretap statute "are not admissible in criminal trials for the Commonwealth"). The term "contents" is broadly defined to mean "any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication." G. L. c. 272, § 99 B (5).

The history, purpose, and evolution of the wiretap statute have been extensively explained by the Supreme Judicial Court, see, e.g., Commonwealth v. Rainey, 491 Mass. 632, 645-647 (2023); Commonwealth v. Tavares, 459 Mass. 289, 294-296 (2011), and we need not repeat them here. For purposes of this case, we need only note that in 1968,[9] concerned about the "uncontrolled

[9] Vast changes in technology have occurred since 1968, but they have not prompted the Legislature to amend the statute. By contrast, other jurisdictions have updated their wiretap statutes with more regularity to account for technological advances. See, e.g., Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, Title 1, § 101(c), 100 Stat. 1848, 1851 (adding prohibition on interceptions of "electronic communications" to existing prohibitions on interceptions of "wire" and "oral" communications); 1999 Ill. Laws 657 (defining "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system"); 2021 Or. Laws 357 (defining "[v]ideo conferencing program" as

development and unrestricted use of modern electronic surveillance devices," the Legislature decided that Massachusetts should be among the minority of States[10] requiring that all parties consent to the interception of wire and oral communications.[11] G. L. c. 272, § 99 A, third par. "[T]he Legislature was concerned principally with the investigative use of surveillance devices by law enforcement officials to eavesdrop surreptitiously on conversations." Rainey, supra at 645. See Commonwealth v. Morris, 492 Mass. 498, 505 (2023) (legislative focus of wiretap statute is on deterrence of invasion of privacy rights by "law enforcement officers' surreptitious eavesdropping as an investigative tool" [citation

---

"software or an application for a computer or cellular telephone that allows two or more persons to communicate via simultaneous video transmission").

[10] The other jurisdictions are California, Delaware, Florida, Illinois, Maryland, Montana, New Hampshire, Oregon, Pennsylvania, and Washington. See Cal. Penal Code § 632(a); Del. Code Ann. tit. 11, § 1335(a)(4); Fla. Stat. § 934.03(2)(d); 720 Ill. Comp. Stat. 5/14-2(a)(1); Md. Code Ann., Cts. & Jud. Proc. § 10-402(c)(3); Mont. Code Ann. § 45-8-213(1)(c); N.H. Rev. Stat. Ann. § 570-A:2(I); Or. Rev. Stat. § 165.540(1)(c); 18 Pa. Cons. Stat. § 5704(4); Wash. Rev. Code § 9.73.030(1).

[11] Massachusetts is often colloquially referred to as a "two-party consent" jurisdiction, but it is more accurate to describe it as an all-party consent jurisdiction. See Ferch, Secretly Recording Public Officials: Challenges to the Massachusetts Wiretap Act, 65 Bos. B.J. 43, 43 (Summer 2021).

omitted]); Commonwealth v. Gordon, 422 Mass. 816, 833 (1996) (same).

With a few exceptions contained in G. L. c. 272, § 99 D,[12] none of which are invoked in this case, the statute prohibits

---

[12] That subsection provides as follows:

"D. Exemptions.

"1. Permitted interception of wire or oral communications.

It shall not be a violation of this section --

"a. for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of such communication, or which is necessary to prevent the use of such facilities in violation of section fourteen A of chapter two hundred and sixty-nine of the general laws; provided, that said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

"b. for persons to possess an office intercommunication system which is used in the ordinary course of their business or to use such office intercommunication system in the ordinary course of their business.

"c. for investigative and law enforcement officers of the United States of America to violate the provisions of this section if acting pursuant to authority of the laws of the United States and within the scope of their authority.

"d. for any person duly authorized to make specified interceptions by a warrant issued pursuant to this section.

the "interception" of "any wire or oral communication." G. L. c. 272, § 99 C 1. Because each of these terms bears on the analysis of this case, we pause to examine them in detail before proceeding further.

An "oral communication" is defined as "speech, except such speech as is transmitted over the public air waves by radio or other similar device." G. L. c. 272, § 99 B 2. A "'wire communication' means any communication 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." G. L. c. 272, § 99 B 1. The term "wire communication" includes transmissions made over cellular networks, and "is broad enough to cover non-oral electronic

---

"e. for investigative or law enforcement officers to violate the provisions of this section for the purposes of ensuring the safety of any law enforcement officer or agent thereof who is acting in an undercover capacity, or as a witness for the commonwealth; provided, however, that any such interception which is not otherwise permitted by this section shall be deemed unlawful for purposes of paragraph P.

"f. for a financial institution to record telephone communications with its corporate or institutional trading partners in the ordinary course of its business; provided, however, that such financial institution shall establish and maintain a procedure to provide semi-annual written notice to its corporate and institutional trading partners that telephone communications over designated lines will be recorded."

transmissions." Commonwealth v. Moody, 466 Mass. 196, 208 (2013).

"The term 'interception' means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication," G. L. c. 272, § 99 B 4, except where the interception is made by a law enforcement officer in the course of investigating a "designated offense,"[13] see G. L. c. 272, § 99 B 7, committed in connection with organized crime "if the officer is a party to such communication or has been given prior authorization to record or transmit the communication by such a party" (one-party consent exception). G. L. c. 272, § 99 B 4. "Organized crime . . . consists of a continuing conspiracy among highly organized and disciplined groups to engage in supplying illegal goods and services." G. L. c. 272, § 99 A, first par.

---

[13] Designated offenses are "arson, assault and battery with a dangerous weapon, extortion, bribery, burglary, embezzlement, forgery, gaming in violation of [G. L. c. 271], intimidation of a witness or juror, kidnapping, larceny, lending of money or things of value in violation of the general laws, mayhem, murder, any offense involving the possession or sale of a narcotic or harmful drug, perjury, prostitution, robbery, subornation of perjury, any violation of this section, being an accessory to any of the foregoing offenses and conspiracy or attempt or solicitation to commit any of the foregoing offenses." G. L. c. 272, § 99 B 7.

> "To show a nexus to organized crime, there must be some evidence of an ongoing illegal business operation. The Commonwealth also must demonstrate a high degree of discipline and organization among the suspected members of the criminal enterprise. However, facts suggesting coordination of efforts among cohorts standing alone is insufficient. . . . For a conspiracy to commit an offense enumerated in G. L. c. 272, § 99 B 7, to rise to the level of organized crime, there must, at the very least, be an organized plan from which one reasonably may infer the existence of an ongoing criminal operation. Finally, the Commonwealth must show that the designated offense was committed to promote the supply of illegal goods and services or the furtherance of an ongoing criminal business operation." (Quotations and citations omitted.)

Commonwealth v. Burgos, 470 Mass. 133, 140 (2014). See Tavares, 459 Mass. at 299-300.

Our cases have found this standard to be met where there was evidence of an ongoing coordinated effort among multiple people to engage in one of the statute's designated offenses, see note 13, supra, for the group's financial gain or goals. Thus, for example, in Commonwealth v. Lykus, 406 Mass. 135, 142 (1989), a group of people made a coordinated effort to extort ransom money from the family of a person who had disappeared. By way of further example, in Commonwealth v. Thorpe, 384 Mass. 271, 278 (1981), cert. denied, 454 U.S. 1147 (1982), there was a continuing conspiracy among multiple people to supply illegally the civil service examination. Similarly, in Commonwealth v. Fernandes, 492 Mass. 469 (2023), Commonwealth v. Mitchell, 468 Mass. 417 (2014), Commonwealth v. Hearns, 467 Mass. 707 (2014), and Commonwealth v. Davis, 83 Mass. App. Ct. 484 (2013), there

was an organized network of individuals engaged in selling contraband, often involving large quantities (more than a kilogram) of drugs. By contrast, where the evidence did not establish a nexus between a disciplined network's "organized efforts to supply illicit goods or services" and a designated offense under the statute, the requirements of the statute have been held to have not been satisfied. Tavares, 459 Mass. at 302. See Burgos, 470 Mass. at 142; Commonwealth v. Long, 454 Mass. 542, 557-558 (2009).

Finally, we examine the word "secretly" as it is used in the definition of "interception." G. L. c. 272, § 99 B 4. "Secretly" does not "encompass[] only those situations where an individual has a reasonable expectation of privacy." Commonwealth v. Jackson, 370 Mass. 502, 506 (1976). The wiretap statute's protections are not "coextensive with the Fourth Amendment and art. 14," nor are they limited "only [to] communications as to which the speaker maintains a reasonable expectation of privacy." Rainey, 491 Mass. at 644 n.21. See Morris, 492 Mass. at 506. For this reason, the Commonwealth's argument that the statute cannot be violated absent a reasonable expectation of privacy misses the mark, as did the judge's approach of engrafting art. 14 concepts onto the statute. Although a surreptitious recording may in certain circumstances be suppressed under art. 14, see, e.g., Commonwealth v. Yusuf,

488 Mass. 379, 393-394 (2021); Commonwealth v. Blood, 400 Mass. 61, 77 (1987), as well as under the wiretap statute, the two avenues of analysis do not rise and fall together.[14] The Supreme Judicial Court has explained that if we "were to interpret 'secretly' as encompassing only those situations where an individual has a reasonable expectation of privacy," it "would render meaningless the Legislature's careful choice of words" in § 99. Jackson, supra. See Morris, 492 Mass. at 506 n.10 ("wiretap statute evinces the Legislature's intent to provide broader protections than those provided by the State and Federal Constitutions").

For purposes of the statute, a recording is made "secretly" when it is made without the actual knowledge of the person being recorded. Jackson, 370 Mass. at 507. See Commonwealth v. Hyde, 434 Mass. 594, 595-601 (2001); Project Veritas Action Fund v. Rollins, 982 F.3d 813, 819 (1st Cir. 2020) (construing wiretap

[14] A good example of this principle in action can be found by comparing Moody, 466 Mass. 196, and Commonwealth v. Delgado-Rivera, 487 Mass. 551 (2021), cert. denied, 142 S. Ct. 908 (2022). In Moody, the defendant argued that the secret interception of text messages violated the statute and accordingly should be suppressed under the statute's exclusionary provision. The court agreed. By contrast, in Delgado-Rivera, the defendant argued that the search of another person's cell phone violated the defendant's expectation of privacy in his own text messages, such that suppression was required under the Fourth Amendment and art. 14. The court disagreed.

statute); Glik v. Cunniffe, 655 F.3d 78, 86-87 (1st Cir. 2011). The Commonwealth may prove actual knowledge "where there are clear and unequivocal objective manifestations of knowledge [on the part of the person being recorded], for such indicia are sufficiently probative of a person's state of mind as to allow an inference of knowledge and to make unnecessary any further requirement that the person recording the conversation confirm the caller's apparent awareness by acknowledging the fact of the intercepting device." Jackson, supra.

With these concepts in hand, we turn now to the audio-visual recordings at issue in this case. As an initial matter, we consider whether there was an "interception" within the meaning of the statute. As we have already noted, "[t]he term 'interception' means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication." G. L. c. 272, § 99 B 4. "Record," for purposes of the wiretap statute, means "to cause (sound, visual images) to be transferred to and registered on something [by] electronic means in such a way that the thing so transferred and registered can . . . be subsequently reproduced"[15] (citation omitted). Moody, 466 Mass. at 209.

[15] It is clear that the reference in Moody to sound and visual images includes electronic signals created from sound or visual images.

Rainey, 491 Mass. at 644 n.22. A single communication can be intercepted at more than one point in time or place. Cf. Yusuf, 488 Mass. at 390-392 (body camera recording assessed, for art. 14, both at moment of recording and as of moment two weeks later when footage was reviewed for a different investigatory purpose). Here, there were four interceptions of each encounter between the undercover officer and the defendant: (1) the undercover officer's audio-visual recording of his encounter with the defendant; (2) the remote officers' hearing of the audio-visual transmission of the encounter; (3) the storing of the audio-visual recording in the cloud; and (4) the downloading of the audio-visual recording from the cloud to a disc. The first of these audio-visually intercepted the contents of an oral communication between the undercover officer and the defendant; the remaining three intercepted wire communications. See Moody, 466 Mass. at 208 (text communication over cellular network constitutes wire communication).

All four of the interceptions were made "secretly" within the meaning of the statute because the Commonwealth produced no evidence either of the defendant's actual knowledge or of "clear and unequivocal objective manifestations of knowledge" on his part. Jackson, 370 Mass. at 507. The testifying officer frankly acknowledged that the recordings were made secretly and that, as a matter of common sense, one would expect that to be

the case in the context of an undercover investigation. We have reviewed the recordings ourselves and see nothing to indicate the defendant knew he was being recorded.[16] It is undisputed that the defendant did not consent. This is not a situation where an audio-visual recording was made openly, or for a noninvestigative purpose untargeted to a particular suspect, or while knowing one is voluntarily speaking with police who are taking the statement down. Contrast Morris, 492 Mass. at 506 (station-house recording of police interrogation where defendant knew his voluntary statement was being preserved by police); Rainey, 491 Mass. at 643-644 (voluntary victim statement to police officer wearing body camera); Commonwealth v. Rivera, 445 Mass. 119, 123-125 (2005) (in-store surveillance camera); Gordon, 422 Mass. at 833 (administrative booking video).

As to the one-party consent exception, although the Commonwealth established one of the statute's "designated offenses" -- namely, an "offense involving the possession or sale of a narcotic or harmful drug," G. L. c. 272, § 99 B 7 --

[16] The Commonwealth argues that the defendant should have been on notice that a cell phone could be used for such purposes and that the videos show that the cell phone was in plain view. Setting aside that the Commonwealth did not preserve the issue for appeal by raising it below, see Commonwealth v. Bettencourt, 447 Mass. 631, 633 (2006), there was no evidence below as to how the cell phone was displayed by the undercover officer, and our independent review of the videos does not lead us to conclude that it was displayed in plain view in a manner that would lead the defendant to be on notice that he was being recorded.

it failed to prove a nexus to organized crime. As the judge correctly found, there was no evidence that the defendant, an apparent street dealer, was acting in concert with others as part of an organized criminal enterprise. Nor did the particulars of the three transactions, which involved small amounts, give rise to such an inference. Contrast Mitchell, 468 Mass. at 426; Hearns, 467 Mass. at 715-716; Davis, 83 Mass. App. Ct. at 490-491.

For these reasons, we conclude that the interceptions in this case violated the statute. We accordingly turn to the statute's exclusionary provision to consider the appropriate remedy. Where, as here, an oral or wire communication has been unlawfully intercepted, the statute permits a criminal defendant to "move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom." G. L. c. 272, § 99 P. "Contents" is broadly defined as "any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication." G. L. c. 272, § 99 B 5. The definition extends beyond the words of the communication itself or an aural recording of it.[17] It may "mean simply that not only

[17] This is one of several points of distinction between the wiretap statute and Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211 (1968) (Title III). Unlike our Legislature, Congress has

must the recording of an unlawfully intercepted conversation be suppressed, but also any evidence that the conversation was recorded: for example, any transcripts or summaries of, or references to, the recording; or the testimony of a third person (not a party to the conversation) who either monitored the conversation at the time it took place or listened to a recording of it later." Commonwealth v. Jarabek, 384 Mass. 293, 298 (1981). The same definition of "contents" applies to both oral and wire communications.

Where, as here, the audio and visual components were captured during a unitary audio-visual recording, nothing in the statute suggests that they should be considered separately to determine whether they constitute "contents" as defined by the statute.[18] But even considering them separately, both fall within the statutory definition. The audio portion of the recordings does so because it is information concerning the existence, contents, and substance of the defendant's oral

---

"purposefully narrowed the definition of 'wire communication' under Title III to include only 'aural transfer'" (citation omitted). Moody, 466 Mass. at 207. See United States v. Larios, 593 F.3d 82, 90 (1st Cir.), cert. denied, 560 U.S. 935 (2010) (Title III applies only to aural wire communications).

[18] This case does not involve a video-only recording of a communication or a video recording of communication that was audio recorded separately. Nor do we consider or decide whether the contents of such video recordings may fall within the statute.

communications with the undercover officer. The video portion of the recordings does so because it is evidence that the conversations were recorded, and because it shows the defendant while he was having those oral communications with the undercover officer and, accordingly, is "information concerning the identity of the parties to such communication."[19] G. L. c. 272, § 99 B 5. Given the Legislature's broad definition of "contents," both the audio and video aspects of the audio-visual recordings should have been suppressed. Because the definition of "contents" is the same for both wire and oral communications, the outcome is the same whether we look only to the undercover officer's initial audio-visual recording of the oral communications with the defendant, or to the subsequent interceptions of the wire communications from the undercover officer.

The Commonwealth counters that, despite the definition of "contents," the video portion of the recordings should not be suppressed because the defendant had no reasonable expectation of privacy in public places. But this argument impermissibly imports art. 14 considerations into the wiretap statute. As we have already explained, the Legislature deliberately did not

---

[19] Neither party briefed the question whether the portions of the recordings when the defendant was not in audio-visual range of the undercover officer's cell phone violated the statute, and we therefore do not consider the issue here.

incorporate art. 14 analysis into the statute, but instead carefully crafted a scheme that rests instead on whether a recording is made "secretly."

At oral argument, both sides expressed concerns regarding the possible consequence of any decision we might reach. On the one hand, counsel for the defendant represented that Callyo (the software application used by the officers here) is being adopted by police departments across the country to conduct surreptitious surveillance on ordinary citizens. Even accepting this representation and accounting for the sophisticated investigatory uses to which Callyo is being put elsewhere as described in reported cases from other jurisdictions, see note 3, supra, the Legislature has created a strong bulwark against secret surveillance by law enforcement in this Commonwealth. General Laws c. 272, § 99, is among the most protective of electronic surveillance statutes in the country, see note 10, supra, and more protective than Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211 (1968). As demonstrated in the outcome we reach here, the statute is adequately designed to deal even with a sophisticated and novel surveillance tool such as Callyo.

On the other hand, the Commonwealth raises the fear that police officers will be exposed to criminal and civil liability should they be found to have violated the statute. The statute

does indeed provide for criminal penalties and civil remedies. See G. L. c. 272, § 99 C 1 (criminal penalty), Q (civil remedy). But the statute allows the Commonwealth to insulate itself prophylactically from liability by obtaining a warrant. See G. L. c. 272, § 99 D 1 d; note 12, supra. In addition, the statute protects investigative and law enforcement officers from criminal and civil liability if they violate the statute "for the purposes of ensuring [officer] safety" while operating undercover. G. L. c. 272, § 99 D 1 e. In such circumstances, although the officers will be insulated from liability, the contents of the unlawful interceptions are nonetheless excluded from evidence. See G. L. c. 272, § 99 D 1 e. In sum, the statute reflects the Legislature's careful balancing of competing concerns.[20]

The portion of the order allowing the motion to suppress the audio portion of the recordings is affirmed. So much of that order as denied the defendant's motion to suppress the video portion of the recordings is reversed. Nothing in this opinion is to be read to limit the undercover officer's testimony at trial as to what was said during the three

---

[20] When police wish to use a novel surveillance tool such as Callyo, we encourage them to seek a search warrant beforehand. Because our statutes and Declaration of Rights may be more protective of individual privacy rights than similar laws in some other States, the police should not simply rely on the fact that the tool has been used in other jurisdictions.

transactions or what he observed during them. See Jarabek, 384 Mass. at 293, 299.

So ordered.