State of New York
Court of Appeals

OPINION

No. 9
The People &c.,
Respondent,
v.
Emmanuel Diaz,
Appellant.

Dina Zloczower, for appellant.
Leonard Joblove, for respondent.
The Legal Aid Society; JustLeadershipUSA et al.; Brooklyn Defender Services et al.; Sanctuary for Families, Inc., amici curiae.

FEINMAN, J.:

The issue in this appeal is whether a correctional facility's release to prosecutors or law enforcement agencies of recordings of nonprivileged telephone calls made by pretrial detainees, who are notified that their calls will be monitored and recorded, violates the

Fourth Amendment. We hold that detainees, informed of the monitoring and recording of their calls, have no objectively reasonable constitutional expectation of privacy in the content of those calls (US Const, amend IV). Thus, a correctional facility may record and monitor detainees' calls, as well as share the recordings with law enforcement officials and prosecutors, without violating the Fourth Amendment.

I.

Defendant Emmanuel Diaz was arrested in July 2012 and charged with multiple counts of burglary and robbery. Upon his arraignment on the felony complaint, he was committed to the custody of the New York City Department of Correction (DOC). He was held in one of the Rikers Island Correctional Facilities until his family posted bail. During the eight months before defendant posted bail, he made approximately 1,100 phone calls from prison. At trial, the prosecution sought to introduce excerpts of four phone calls recorded by DOC containing incriminating statements. After colloquy with the parties concerning the notice that had been provided to inmates of the electronic surveillance, Supreme Court admitted the recordings into evidence, over defendant's objection. Defendant was subsequently convicted and sentenced.

The Appellate Division, with one Justice dissenting, affirmed the judgment (149 AD3d 974 [2d Dept 2017]). The majority found that defendant had impliedly consented to the monitoring and recording of his telephone conversations because DOC had given him sufficient notice that his calls would be monitored. The Court determined that the record reflected that DOC had provided several types of notice of the prison's policy to monitor and record inmate telephone calls, including the inmate handbook, signs posted

next to the telephones, and a recorded message preceding every phone call made by inmates. The majority held it was not reasonable for defendant to presume an expectation of privacy in the dissemination of the content of his recorded phone conversations. Although it remarked that the "better practice going forward" might be for DOC to expressly notify detainees that the recordings of their calls may be turned over to prosecutors, the majority concluded that the absence of such a warning did not render the calls inadmissible (id. at 976). Additionally, the majority found no merit to defendant's contention that the admission of the recorded phone calls into evidence deprived him of his right to counsel under the Federal and State Constitutions (id. at 975, citing People v Johnson, 27 NY3d 199, 205-206 [2016]).

The dissenting Justice would have held that the calls were inadmissible because defendant was never informed that the recordings of his calls would be made available to the prosecutor for potential use at trial (Diaz, 149 AD3d at 977 [Hall, J.P.]). The dissent contended that DOC should be required to provide proof that detainees were given express notice that their recorded telephone calls could be turned over to the prosecution for use at trial (id. at 978). Although the dissent recognized that defendant had no reason to expect privacy in his calls, it posited that this did not mean he consented to the prosecution having access to them. The dissenting Justice granted defendant leave to appeal.

II.

In 2008, DOC began monitoring prisoner phone calls pursuant to an amendment to the Rules of the City of New York and the subsequent development of new DOC policies

and procedures.[1] Under the Rules of the City of New York, inmates may make telephone calls during their incarceration, but, "[u]pon implementation of appropriate procedures," their calls may be listened to or monitored where they have been given "legally sufficient notice" (40 RCNY 1-10 [a], [h]). As set forth in its Operations Order,[2] DOC "shall record all inmate telephone calls and retain these recordings," except calls to inmates' attorneys and others included in the Department's "Do Not Record List."[3] The Operations Order requires that inmates be notified that their telephone calls will be monitored and/or recorded by three different methods: (1) signs posted near the telephones used by inmates, stating in both English and Spanish that calls are monitored and recorded and that using the phone constitutes consent to the recording or monitoring; (2) a notice in the inmate handbook that calls can be monitored and recorded; and (3) a recording in Spanish or English that plays when an inmate picks up the phone receiver, stating that the call may be recorded and monitored (see Operations Order pp. 8-9, § III [E] [1], [2]).

[1] The changes were part of a revamping of the Minimum Standards for New York City Correctional Facilities first adopted in 1978 (see City of New York Board of Correction, Notice of Adoption of Amendments to the Minimum Standards for New York City Correctional Facilities [2007], available at https://www1.nyc.gov/assets/boc/downloads/pdf/minimum standards amendments.pdf [last accessed 1/17/19]).

[2] New York City Department of Correction, Operations Order No. 01/09 [eff Mar. 9, 2009]).

[3] Inmates' calls to their attorneys, doctors, and clergy are privileged and not recorded, nor are calls to certain specified agencies (see Operations Order p. 1, § II [A]; see also 40 RCNY 1-10 [h]).

Defendant asserts that DOC's release of his recorded telephone calls to the prosecution without a warrant violates his Fourth Amendment right to privacy.[4] Specifically, defendant maintains that a person's consent to governmental intrusion can be no broader than the notice provided. This issue was previously raised in People v Johnson (27 NY3d 199 [2016]) but was unpreserved. The parties agree that the issue is now properly before us.

III.

"The Fourth Amendment protects '[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures'" (Carpenter v United States, ___ US ___, ___, 138 S Ct 2206, 2213 [2018]) and safeguards two interests—retaining possession of property, and maintaining personal privacy (see Texas v Brown, 460 US 730, 747 [1983] [Stevens, J., concurring with Brennan and Marshall, JJ.]; United States v Jacobson, 466 US 109, 113-114 [1984]). A seizure pertains to the first interest, and a search pertains to the second (Texas v Brown, 460 at 747). The application of the Fourth Amendment depends on whether the person invoking its protection can claim a reasonable expectation of privacy in the face of government action (see Smith v Maryland, 442 US 735, 740 [1979]). A legitimate expectation of privacy exists where a person has demonstrated an actual (subjective) expectation of privacy and

[4] Defendant had cursorily asserted before the trial court that the recordings violated both his federal and his state constitutional rights, but made no argument below that the State Constitution afforded him greater protection than the Fourth Amendment (see People v Garvin, 30 NY3d 174, 185 n 8 [2017], cert denied 139 S Ct 57 [2018]), and he advances no such argument here.

that expectation is one that society is prepared to recognize as reasonable (see Katz v United States, 389 US 347, 361 [1967] [Harlan, J., concurring]). If such expectations of privacy are lacking, no Fourth Amendment violation occurs (see New York v Class, 475 US 106, 112 [1986]).

Even if defendant subjectively believed that his calls were private – a notion that is largely belied by the record – that expectation was not objectively reasonable. Given the government's weighty interest in ensuring institutional security and order, surveillance is ubiquitous in the prison context (see Hudson v Palmer, 468 US 517, 527-528, 529-530 [1984] [an incarcerated individual's "expectation of privacy must always yield to what must be considered the paramount interest in institutional security"]; Bell v Wolfish, 441 US 520, 559 [1979]).

For instance, correctional officers routinely conduct warrantless searches of inmates and their cells to keep other inmates and themselves safe (see Bell, 441 US at 547). The logic underlying the routine monitoring and recording of phone calls is no different (see United States v Hearst, 563 F2d 1331, 1345 [9th Cir 1977] [detainees' expectations of privacy in their phone calls are superseded by "the government's weighty, countervailing interests in prison security and order"]; see also Lanza v State of New York, 370 US 139, 143 [1962] ["it is obvious that a jail shares none of the attributes of privacy of a home, an automobile, an office, or a hotel room. In prison, official surveillance has traditionally been the order of the day"]; see e.g. United States v Willoughby, 860 F2d 15, 21 [2d Cir 1988] [detention facility's practice of randomly monitoring and recording pretrial detainees' phone calls "in the interest of institutional security is not an unreasonable

invasion of the privacy rights of pretrial detainees"]). In addition, defendant, like all Rikers Island inmates, received a number of prominent, unavoidable warnings that his calls were subject to electronic monitoring and recording by DOC. Because any expectation of privacy in defendant's calls was not objectively reasonable, "the Fourth Amendment is therefore not triggered by the routine taping of such calls" (United States v Van Poyck, 77 F3d 285, 291 [9th Cir 1996]).

On this basis, federal and state courts across the country have long held that detainees provided with prior notice of the government's monitoring and recording of their phone calls have no reasonable expectation of privacy in the content of the communications (see United States v Gangi, 57 Fed Appx 809, 814 [10th Cir 2003]; United States v Friedman, 300 F3d 111, 123 [2d Cir 2002]; United States v Eggleston, 165 F3d 624, 626 [8th Cir 1999]; Van Poyck, 77 F3d at 290-291; United States v Horr, 963 F2d 1124, 1126 n 3 [8th Cir 1992]; United States v Sababu, 891 F2d 1308, 1329 [7th Cir 1989]; United States v Amen, 831 F2d at 379-380; State v Gilliland, 294 Kan 519, 534, 276 P3d 165, 177 [2012]; State v Hill, 333 SW3d 106, 126 [Tenn Crim App 2010]; In re Grand Jury Subpoena, 454 Mass 685, 688-689, 912 NE2d 970, 973 [2009]; Decay v State, 2009 Ark 566, 6, 352 SW3d 319, 325-26 [2009]; Preston v State, 282 Ga 210, 214, 647 SE2d 260, 263 [2007]; State v Smith, 117 Ohio App 3d 656, 661, 691 NE2d 324, 327 [Ohio Ct App 1997]). In light of this precedent, defendant understandably does not dispute that DOC's monitoring and recording of his phone calls did not constitute a violation of his Fourth Amendment rights.

Defendant, and the dissent, argue that, although DOC's interception of the content of the call may have been lawful, its release of the recordings to the prosecutor's office without notice was an additional search that violated the Fourth Amendment. We disagree.

As a number of courts have explained, where detainees are aware that their phone calls are being monitored and recorded, all reasonable expectation of privacy in the content of those phone calls is lost, "and there is no legitimate reason to think that the recordings, like any other evidence lawfully discovered, would not be admissible" (United States v Eggleston, 165 F3d at 626; see also United States v Novak, 531 F3d 99, 103 [1st Cir 2008] [holding that because the defendant had consented to the monitoring of his calls, they could be introduced into evidence "consistently with the requirements of the Fourth Amendment"]; United States v Green, 184 Fed Appx 617, 618 [9th Cir 2006] [observing that disclosure of recordings to prosecution "does not … provide a basis for establishing a violation of … the Fourth Amendment"]; see also People v Natal, 75 NY2d 379, 382-383 [1990]).[5] Moreover, the signs posted near the telephones used by the inmates state that calls are monitored in "accordance with DOC policy" which, according to the DOC Operations Order, provides that while recordings are confidential and not available to the public, the District Attorney's Office may request a copy of an inmate's recorded calls which will be provided upon approval by DOC.[6] Although the inmate handbook provided

[5] This is particularly true where, as here, DOC provided multiple notices both that inmates' conversations could be monitored and recorded and that use of the phones constituted consent to that monitoring and recording (see United States v Workman, 80 F3d 688, 693-694 [2d Cir 1996]; Amen, 831 F2d at 379).

[6] See Operations Order pp. 6, § III (5) (b); 7, § III (C) (1).

at Rikers Island gives notice that inmate telephone calls may be monitored "for purposes of security," that statement simply explains one of the reasons for DOC's monitoring practice; it says nothing about the potential uses or dissemination of the recordings. In addition, the recorded notice heard when first making a telephone call does not restrict the use of the recording.

We therefore reject defendant's argument that he retained a reasonable expectation of privacy once the calls were lawfully intercepted by DOC and hold that there were no additional Fourth Amendment protections that would prevent DOC from releasing the recording to the District Attorney's Office absent a warrant.

Defendant's remaining arguments, challenging the "voluntariness" of any findings of consent to the monitoring and recording of his phone calls, and claiming that his due process and equal protection rights were violated, are unpreserved for our review.[7]

Finally, we agree with the Appellate Division that the existing record does not support a finding that defendant's trial counsel was ineffective as a matter of law.

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

[7] Defendant has abandoned his argument made to the Appellate Division that admission of the recordings deprived him of his right to counsel under the Federal and State Constitutions.

People v Emmanuel Diaz

No. 9

WILSON, J. (dissenting):

The New York City Department of Correction (DOC) routinely records the telephone calls of Rikers Island inmates "for security purposes," yet delivers the recordings to the District Attorney's office for use in prosecution. The Fourth Amendment cannot permit that practice.

I

Mr. Diaz was advised of the consequence of using the phone in Rikers Island; the majority says he proceeded at his peril and therefore forfeited any privacy right he may have had in his calls. That conclusion is superficially understandable but, in reality, ignores crucial facts: (1) Mr. Diaz was not free to leave Rikers Island but was incarcerated for eight months awaiting trial, with no other viable means of everyday communication with the outside world;[1] (2) others accused of crimes but out on bail cannot be subjected to governmental recording and monitoring without a warrant; (3) Mr. Diaz was charged with crimes and needed to assemble a defense and gather evidence that might mitigate his sentence if convicted; (4) Mr. Diaz was specifically told that the recording of his calls was for the purpose of jail security; and (5) Mr. Diaz was not told that his calls would be funneled en masse to the District Attorney prosecuting his case, to be combed for statements to use against him.

Those differences matter. By discounting them, the majority's analytical framework is internally inconsistent. The majority relies approvingly on Justice Harlan's well-accepted statement that the expectation of privacy "is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'" (Katz v United States, 389 US 347, 361 [1967] [Harlan, J., concurring]). The majority begins by

[1] Yes, he could write letters, but those too could be opened and examined. He could see in-person visitors, but only as frequently as they could make the onerous journey to Rikers Island, which is hardly a substitute for everyday phone communication.

announcing that "*detainees, informed of the monitoring and recording of their calls*, have no objectively reasonable constitutional expectation of privacy in the content of those calls" (majority op at 2, emphasis added). The majority's rationale must rest on the proposition that pretrial detainees have a diminished expectation of privacy resulting from the fact of detention; otherwise, the government could notify the general public that it was monitoring their phone calls and thereby eliminate the reasonable expectation of privacy. The majority's analysis must also depend on the notion of implied consent, because if pretrial detention alone were sufficient to remove all expectation of privacy in inmate phone calls, the majority would have no need to mention consent at all. Thus, under the majority's framework, neither Mr. Diaz's status as a pretrial detainee nor his implied consent would—without the other—eliminate his privacy rights in the calls.

Later, however, the majority states: "[c]orrectional officers routinely conduct warrantless searches of inmates and their cells to keep other inmates and themselves safe. The logic underlying the routine monitoring and recording of phone calls is no different" (majority op at 6, internal citation omitted). That conclusion rests on the proposition that pretrial detainees have no expectation of privacy. But unlike the majority's rationale here, the cases upholding the constitutionality of such searches do not depend on any theory of notice or implied consent (see Bell v Wolfish, 441 US 520, 557 [1979] [upholding a policy that detainees must exit their rooms while correctional officials conduct "shake-down" searches because that "appropriate security measure" does not infringe on whatever expectation of privacy detainees may have]). However, as I explain later, all four Appellate

Division Justices below, and the parties in this case, agree that pretrial detainees like Mr. Diaz have some expectation of privacy in their phone calls—conclusions that accord with existing case law on the subject (cf Florence v Board of Chosen Freeholders of County of Burlington, 566 US 318, 322, 338-39 [2012] [upholding a policy to conduct visual strip and body cavity searches of all pretrial detainees upon intake but suggesting those searches could violate a detainee's privacy rights in other scenarios]; Bell, 441 US at 557-58 [assuming without deciding that pretrial detainees retain at least "a diminished expectation of privacy"]). Indeed, the People concede that if DOC gave no notice to inmates that their calls would be recorded or monitored, that recording or monitoring would violate the Fourth Amendment. I discuss this in part I, infra.

The broader problem, with which the majority fails to come to grips, is that determining what expectation of privacy society would recognize as reasonable depends on the government's need for—and intended use of—the information obtained in derogation of a privacy right. The fact that information is known to someone other than its owner does not divest the owner of all privacy interests in that information. In the old world, it was relatively simple to draw a line between private information exchanges to which no third party was present and nonprivate information exchanges to which a third party was present. But the new world does not—and cannot—abide by that taxonomy. Eventually, as I explain in part IV, we come back to Justice Harlan's question: what would society consider reasonable? As Judge Pigott, a retired member of this Court, wrote of the DOC policy at issue today: "The current arrangement between the Department of

Correction and the District Attorney's office creates a serious potential for abuse and may undermine the constitutional rights of defendants who are unable to make bail" (People v Johnson, 27 NY3d 199, 208 [2016] [Pigott, J., concurring]). Society should not consider that arrangement reasonable.

II

The Fourth Amendment guarantees that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" (US Const, amend IV). That promise requires the government to obtain a search warrant supported by probable cause, or else the consent of the person being searched, before searching something in which that person has a legitimate expectation of privacy. Those requirements manifest the "basic purpose of this Amendment": a commitment to "safeguard the privacy and security of individuals against arbitrary invasions by governmental officials" (Carpenter v United States, 138 S Ct 2206, 2213 [2018]), quoting Camara v Municipal Court of City and County of San Francisco, 387 US 523, 528 [1967]).

The Founders designed the Fourth Amendment as a "response to the reviled general warrants and writs of assistance of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity" (id. at 2206, quoting Riley v California, 134 S Ct 2473, 2494 [2014], internal quotation marks omitted). That opposition to unwarranted government searches was "in fact one of the driving forces behind the Revolution itself" (Riley, 134 S Ct at 2494, citing Boyd v United States, 116 US 616 [1886]), reflecting the consensus that such unrestrained government

power had no place in the new United States. By requiring a warrant or consent to search or seize an individual's person or property, the Fourth Amendment serves "to put the courts of the United States and Federal officials"—and, since its incorporation against the states, state courts and officials[2]—"in the exercise of their power and authority, under limitations and restraints as to the exercise of such power and authority" (Weeks v United States, 232 US 383, 391-92 [1914]).

The Supreme Court initially interpreted the Fourth Amendment to protect against searches of material things only, explicitly rejecting in Olmstead v United States a claim that it protects against the interception of electronic communications (277 US 438 [1928], overruled in part by Katz v United States, 389 US 347 [1967]). But the Court later abandoned that limitation, confirming that the right of privacy rests with "people, not places"—and includes communications in which a person has a reasonable expectation of privacy (Katz, 389 US at 351). Mr. Diaz has such an expectation here.

Importantly, all agree to the proposition that Mr. Diaz has some protectable expectation of privacy in his calls. The lower courts so held,[3] and, by concluding that Mr.

[2] Mapp v Ohio (367 US 643 [1961]) incorporates the Fourth Amendment against the states.

[3] The Appellate Division noted that "'convicted prisoners do not forfeit all constitutional protections by reason of their conviction and confinement in prison,' and certainly 'pretrial detainees, who have not been convicted of any crimes, retain at least those constitutional rights that . . . are enjoyed by convicted prisoners'" (People v Diaz, 149 AD3d 974, 976 (3d Dep't 2017), quoting Bell, 441 US at 545). From the Appellate Division's conclusion that the notice given to Diaz—in the inmate handbook, in the signs posted by the telephones, and in the audio recording that plays before each outgoing call—sufficiently constituted his implied consent to be recorded by DOC, it necessarily follows that the court concluded Mr. Diaz has an expectation of privacy that would require consent to search. With the addition of the dissenting Justice Hall, all four Justices agreed that, absent consent,

Diaz forfeited that expectation through implied consent, the majority agrees as well. The People reaffirmed at oral argument that Mr. Diaz "certainly" has an expectation of privacy in his phone calls and that absent his consent, monitoring or recording his calls would have violated his Fourth Amendment rights.[4]

Those concessions and lower court holdings square with Fourth Amendment jurisprudence by which we are bound. As the Appellate Division reiterated, "convicted prisoners do not forfeit all constitutional protections by reason of their conviction and confinement in prison" (Bell, 441 US at 545). Indeed, "[t]here is no iron curtain drawn between the Constitution and the prisons of this country" (Wolff v McDonnell, 418 US 539, 555-56 [1974]). Convicted prisoners retain, for instance, at least some of the constitutional protections guaranteeing freedoms of speech and religion (see Pell v Procunier, 417 US 817 [1974]; Cruz v Beto, 405 US 319 [1972]; Cooper v Pate, 378 US 546 [1964]); freedom from invidious racial discrimination (Lee v Washington, 390 US 333 [1968]); access to the courts (Johnson v Avery, 393 US 483 [1969]); and due process of law in any deprivation of life, liberty or property (Meachum v Fano, 427 US 215 [1976]). Accepting that convicted inmates retain some constitutional protections, "*[a] fortiori*, pretrial detainees, who have not been convicted of any crimes, retain at least those

---

the monitoring or recording of the calls would violate Mr. Diaz's right to privacy under the Fourth Amendment.

[4] A word on wiretapping: Mr. Diaz makes no claim under any wiretapping statute, so there is no need to interpret those statutes in his case. In People v Cisse, argued the same day as this case, Mr. Cisse made no Fourth Amendment claim, only a wiretapping claim. For purposes of the wiretapping statute, consent, however limited, renders the interception not a violation of the wiretapping statute; the same is not true as regards a limited waiver of one's Fourth Amendment rights.

constitutional rights that we have held are enjoyed by convicted prisoners" (Bell, 441 US at 545).

However, for pretrial detainees and convicted inmates alike, "[t]he fact of confinement as well as the legitimate goals and policies of the penal institution limits these retained constitutional rights" (Bell, 441 US at 546; see also Jones v North Carolina Prisoners' Labor Union, 433 US 119, 125 [1977]; Pell, 417 US at 822). To that end, there must be a "mutual accommodation between institutional needs and objectives and the provisions of the Constitution that are of general application" (*Wolff*, 418 US at 556). That principle "applies equally to pretrial detainees and convicted prisoners," who implicate the same security concerns regardless whether they have been convicted of any crime (Bell, 441 US at 546). Accordingly, the "restrictions and limitations" that our society places on an incarcerated individual must be consistent with "the considerations underlying our penal system"—of which "institutional security and preserving internal order and discipline are essential" (id. at 545, 546). Our system gives wide latitude to correctional officials to take "appropriate action to ensure the safety of inmates and corrections personnel and to prevent escape or unauthorized entry" (id. at 547), on the theory that those officials are best situated to determine what security measures are required to maintain security and order in a correctional facility. That latitude has been used to uphold a range of intrusions—some quite severe—into an inmate's expectation of privacy.

For a criminal defendant who is not detained but is instead out on bail, the Fourth Amendment undoubtedly requires law enforcement to obtain a warrant to monitor that

person's calls. As a pretrial detainee not convicted of any crime at the time the phone recordings at issue in this case were made, Mr. Diaz is, as a starting point, entitled to that same level of constitutional protection. Nevertheless, the People argue that DOC's monitoring is lawful because, by using the phones after receiving notice of DOC's recording policy—which explicitly states that use of the phones shall constitute implied consent—Mr. Diaz impliedly consented to a search by DOC. I disagree with that view—now advocated by the majority—because it disregards the limits of DOC's institutional authority, which if left unchecked undermines the foundation of the Fourth Amendment's protection against unwarranted government intrusions.

A

There is a serious question as to whether, in the sort of circumstances present here, consent can be implied from an inmate's use of the phones following notice.[5] In numerous areas of the law, consent is deemed involuntary—and hence ineffective—when made under duress (see, e.g., Centro Empresarial Cempresa S.A. v Am. Movil, S.A.B. de C.V., 17 NY3d 269, 276 [2011] [releases from liability]; Hammelburger v Foursome Inn Corp., 54 NY2d 580, 592-94 [1981] [mortgage foreclosure]; Austin Instrument, Inc. v Loral Corp.,

[5] The idea that notice plus action equals consent is highly suspect in this context. Were notice plus action sufficient to constitute consent to a search, "law enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications" (Smith v Maryland, 442 US 735, 750 [1979] [Marshall, J., dissenting]). In the particular context of incarceration, where Mr. Diaz has no realistic option but to use the phones to communicate with loved ones and participate in his defense, and no bargaining power to negotiate the terms of DOC's policy, Justice Marshall's concern resonates even more strongly.

29 NY2d 124, 130 [1971] [economic duress in contracts generally]; cf McFarland v McFarland, 70 NY2d 916, 917 [1987] [marital separation agreements]; Matter of Sarah K., 66 NY2d 223, 232 [1985] [adoption]). Although the Fourth Amendment permits some intrusions into an inmate's privacy rights without consent (see, e.g., Bell, 441 US at 558-60 [upholding policy to conduct visual strip and body cavity searches of all inmates after in-person visits]; id. at 555-57 [upholding policy to search inmates' living areas and possessions while they are not present]), there is a further serious question as to whether DOC may establish lawful grounds to monitor inmate phone calls without consent for purposes related to prison safety and security. I do not opine on either of those questions here: as to the first, because it is a largely factual question requiring development of a record; as to the second, because DOC is not represented in this litigation and because the People have conceded that absent an inmate's consent, the monitoring and recording would violate the Fourth Amendment.

Thus, for the purposes of this case, I assume that Mr. Diaz waived his expectation of privacy—as against DOC, for security purposes—by providing his implied consent to be monitored and recorded in accordance with DOC policy. According to the record, inmates and pretrial detainees at Rikers Island received three forms of notice of that policy. First, all inmates must sign the inmate handbook, which states:

> "All calls, except for calls with your attorney or other privileged calls, may be monitored and/or recorded by the Department *for security purposes*. In order for your attorney and other privileged calls not to be monitored you must provide the Department with the phone numbers to which calls should not be monitored, and the Department will check that those

> numbers belong to attorneys or other persons with privileged contact with you. Your use of the telephone in a Department facility constitutes your implied consent to such monitoring" (emphasis added).

Second, signs posted in English and Spanish next to the telephones read:

> "INMATE TELEPHONE CONVERSATIONS ARE SUBJECT TO ELECTRONIC MONITORING AND/OR RECORDING *IN ACCORDANCE WITH DOC POLICY*. AN INMATE'S USE OF INSTITUTIONAL TELEPHONES CONSTITUTES CONSENT TO THIS MONITORING AND/OR RECORDING" (emphasis added).

Third, a brief recorded message at the start of each call warns that calls "may be recorded and monitored" (A236).[6] The first notice plainly limits the purpose of the monitoring and recording to that conducted "by the Department for security purposes"; the second, by referencing "DOC POLICY" incorporates the first; and the third, in its brevity, does nothing to dispel the prior restrictions on the purpose and use of the monitored calls. The implied consent provision of the inmate handbook, for its part, states that "[y]our use of the telephone in a Department facility constitutes your implied consent to *such recording*"—that is, to the limited recording described. Likewise, the signs posted by the phones state that use of the phones "CONSTITUTES CONSENT TO *THIS* MONITORING AND/OR RECORDING"—as in, to the monitoring and recording for security purposes that the signs reference in the first place. DOC thereby sought Mr. Diaz's

[6] The record does not contain a recording or transcription of the actual message, only a testimonial description of it.

implied consent for its own security purposes—the only purpose for which it could seek consent; that is the only consent Mr. Diaz even arguably gave.

Working again from the agreed-upon proposition that Mr. Diaz and other pretrial detainees have some reasonable expectation in the privacy of their calls, the mere fact that Mr. Diaz has communicated some information to some other person does not entitle the prosecution to obtain that information without his consent or without a warrant—neither of which it had in this case.[7] In other words, Mr. Diaz's consent to a search by DOC, a non-law enforcement governmental entity, for its own security purposes cannot reasonably be construed to include consent for the District Attorney—a law enforcement entity—to search that information for prosecutorial purposes.

B

The bases on which an incarcerated person's—or anyone's—constitutional rights may be overcome is limited by the nature of the governmental need. The majority implicitly recognizes as much, noting that prison surveillance is justified by the "government's weighty interest in ensuring institutional security and order" (majority op at 6, citing Hudson v Palmer, 468 US 517, 527-28, 529-30 [1984]). As but one example, although the Fourth Amendment by its language prevents all unreasonable warrantless

[7] Even when only a single governmental entity is involved—and not two, as was the case here, "[t]he standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of 'objective' reasonableness—what would the typical reasonable person have understood by the exchange between the officer and the suspect?" (Florida v Jimeno, 500 US 248, 251 [1991] [holding that a criminal suspect's consent for police to search his vehicle did not constitute consent for police to search a bag within the vehicle that could not reasonably have contained the object police were searching for]).

searches and seizures, the governmental need for a warrantless search in exigent circumstances (see Mincey v Arizona, 437 US 385, 394 [1978]) or incident to a lawful arrest (see Chimel v California, 395 US 752, 763 [1969]) can overcome the privacy right that the constitution guarantees. As relevant to Mr. Diaz, the Supreme Court has long "insisted that prisoners be accorded those rights not fundamentally inconsistent with imprisonment itself or incompatible with the objectives of incarceration"; that is, they retain those rights not inconsistent with the legitimate penological needs and safety and security concerns that incarceration entails (Hudson, 468 US at 523).

Nothing in this case justifies the governmental intrusion of Mr. Diaz's privacy inherent in the District Attorney's unfettered access to his phone calls for the duration of his pretrial detention. The security purposes that expressly underlie DOC's policy to record and monitor detainees' calls are not offered to justify the wholesale disclosure of those recordings to the District Attorney to prosecute Mr. Diaz for the crime for which he was detained—nor could they.

To determine whether the government may lawfully infringe upon an inmate's privacy, the Supreme Court has explained that:

> "The test of reasonableness under the Fourth Amendment is not capable of precise definition or mechanical application. In each case it requires a balancing of the need for the particular search against the invasion of personal rights that the search entails. Courts must consider the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted" (Bell, 441 US at 559).

The Court further explained: "when an institutional restriction infringes a specific constitutional guarantee . . . the practice must be evaluated in the light of the central objective of prison administration, safeguarding institutional security" (id. at 547, citing Jones, 433 US at 129; Pell, 417 US at 823). Indisputably, DOC has a substantial interest in ensuring that pretrial detainees (and convicted inmates alike) are not planning to smuggle contraband into the facility, attempting to tamper with potential witnesses, planning an escape, or participating in the planning of some further crime.[8]

That interest, however, does not justify the intrusion of privacy inherent in turning those recordings over to the prosecution. It is simply implausible that the wholesale disclosure of phone call recordings to the District Attorney advances jail security—and the parties do not contend so. Such disclosure does not strengthen DOC's ability to maintain order, to discover an inmate's efforts to smuggle contraband or hatch an escape, or to monitor for involvement in illegal activity on the outside. DOC, not the District Attorney, is responsible for facility security. Although disclosing the recordings to the District Attorney may often facilitate prosecution for past criminal activity, "[p]rivacy comes at a cost" (Riley, 134 S Ct at 2493); whatever benefit that access might entail is not nearly

[8] The record contains no evidence that DOC's monitoring of inmate phone calls is necessary to maintain security at Rikers Island, nor is there evidence that the District Attorney's office has any weighty need for the recordings. Until 2008, DOC did not record inmate phone calls (and, therefore, did not turn any such recordings over to the District Attorney). There is no evidence that, before the District Attorney's office had unfettered access to recordings of inmate phone calls, its functions were hampered, much less hampered so significantly as to justify the intrusion at issue here. The People make no argument at all as to their *need* for the phone calls—they simply assert a right to have them because DOC has them. If the People did have such a need, the time-honored path to establish it would be through application for a search warrant.

sufficient to overcome the protections the Fourth Amendment provides. Instead, that type of suspicionless search by the government is just what Fourth Amendment prohibits.

III

The People argue that, under what is termed the "third-party" doctrine, a person forfeits all expectation of privacy in information voluntarily disclosed to a third party. Thus, they argue, Mr. Diaz forfeited his expectation of privacy in the call recordings by consenting to DOC's recording and monitoring. That argument fails, and its acceptance bodes ill for the privacy interests of law-abiding individuals.

Application of the third-party doctrine would contravene the test set out in Bell and therefore cannot be available here. DOC is a governmental actor that has obtained limited consent from Mr. Diaz for "security purposes" only. According to the People and the majority, that access constitutes the "third-party disclosure" that eliminates all privacy interests Mr. Diaz (or the recipients of the calls) may have in those phone calls. The majority maintains that when the inmate handbook "gives notice that inmate telephone calls may be monitored 'for purposes of security,' that statement simply explains *one* of the reasons for DOC's monitoring practice; it says nothing about the potential uses or dissemination of the recordings" (majority op at 8, emphasis added). Under the majority's construction, if I ask to borrow your car to drive to the corner store, I may enter it into a demolition derby, because I did not say the *only* thing I was going to use it for was to go to the store. You would be shocked if I said you had impliedly consented, and no court would conclude you had impliedly consented to a use fundamentally different from the one I specifically expressed.

Beyond its detachment from the way consent operates in the real world, the majority's rule contravenes the Bell test by disposing of any inquiry into the DOC's need to collect the information it seeks through a particular search. By allowing DOC to collect information "for security purposes" and routinely deliver it to law enforcement on the theory that the subject has forfeited all expectation of privacy, the majority enables the government to circumvent the Fourth Amendment by collecting private information without a warrant for one ostensible purpose and then deeming it non-private for a purpose as to which a warrant would have been required.

Consider the following. Suppose DOC determined that it could maintain jail security without monitoring and recording inmates' calls after all. But, because the District Attorney wanted the recordings, DOC continued to record all nonprivileged conversations and to turn them over to the District Attorney. Unless we are willing to say that irrespective of DOC's need to record inmate conversations—which Bell requires us to weigh against an inmate's expectation of privacy—the District Attorney's desire to do so is sufficient to overcome the privacy rights of inmates in such calls, we cannot permit such a simple evasion of the Fourth Amendment as is offered here.

For that reason, the People's argument that Mr. Diaz's calls are nonprivileged and therefore subject to the third-party doctrine is a red herring. My phone call to a friend is nonprivileged, but that does not mean the state may intercept it without a warrant and use

its contents to prosecute me.[9] Surely, the state may ask my friend what I said, and my friend may volunteer the contents of our conversation or may be compelled to do so by legal process. Neither of those methods would violate the Fourth Amendment. Likewise here, the District Attorney could have contacted the recipients of Mr. Diaz's phone calls to inquire about the contents of his conversations, and could have subpoenaed them. But merely because the state could use lawful means to obtain the substance of the information from third parties does not mean that it may use *any* means to obtain the information simply because it has been divulged to some third party.

This case is also distinguishable from those in which the police request to search a location for a particular type of contraband or evidence, obtain consent, and discover something else in plain view. For instance, if the police obtain permission from a homeowner to search a home for drugs, and instead find unregistered handguns on the table, the police may seize those handguns, and the prosecution may use them as evidence to support a weapons possession charge. In that case, the homeowner consented to a search *by law enforcement*, and it is the plain-view doctrine, not the third-party doctrine, that allows police to seize those guns. Mr. Diaz consented to no such law enforcement search. He presumably understood that his phone communications would be searched by DOC—

[9] In evaluating the societal reasonableness of the wholesale transfer of Mr. Diaz's phone calls to the District Attorney, it is vital to remember that both DOC and the District Attorney are governmental actors. As a society, we understand that my friend—a private actor—is free to recount to others—even to the District Attorney—our conversation, but that the District Attorney is not permitted to bug our call to obtain that same information.

the government actor responsible for security on Rikers Island, not the District Attorney—the government actor responsible for his criminal prosecution.

We come back around, then, to whether we, as a society, want to prosecute crime by jailing suspects for lengthy periods of time in relatively inaccessible locations and monitoring their calls for statements that might be used against them. We might obtain a higher conviction rate with rubber hoses or waterboards, but that is not the civilization we want. Our society is committed to safeguarding the right against self-incrimination and the right to counsel. I find myself again with Judge Pigott in describing the society we do want and with it, what measure of privacy pre-trial detainees should reasonably expect:

> "Faced with the possibility that anything a defendant says over the telephone can (and will) be used against him a trial, the defendant's only real choice is not to use the phones at all. I cannot sanction that result. Trial courts must be vigilant to protect the detainees' constitutional rights, and consideration should be given to placing limitations on the prosecutor's ability to obtain these recordings" (Johnson, 27 NY3d at 211 [Pigott, J., concurring]).

Such limitations are at the core of the Fourth Amendment's promise.

IV

The broader deficiency in the majority's analysis is that the third-party doctrine is eroding under the flow of technological change, just as traditional conceptions of privacy based in property, places, and physical objects have been abandoned over the last century. Nearly a century ago, in Olmstead v United States, the Supreme Court held that wiretapping did not violate the Fourth Amendment:

> "The [Fourth] Amendment itself shows that the search is to be of material things -- the person, the house, his papers, or his effects. . . . The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing, and that only. There was no entry of the houses or offices of the defendants. . . . The language of the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched" (277 US 438, 464 [1928]).

Four decades later, the Court diverged from that property-based conception of privacy rights, acknowledging in Katz v United States that over time, "the underpinnings of Olmstead . . . have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling" (389 US 347, 353 [1967]). Representing a broad expansion of privacy protections to "people, not places" (id. at 516), Katz holds specifically that the government cannot constitutionally intercept calls placed from a phone booth. Although the booth itself was located on a public street, the "critical fact in this case" was that "one who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world" (id. at 511, 517). With the advent of cell phones, it would be absurd to maintain that place-based conception of privacy—to say that the "critical fact" underpinning our expectation that the government will not intercept our calls is the act of shutting a door behind us before dialing.

The chief concern of the Fourth Amendment is to protect against arbitrary government power that unjustifiably intrudes on the sphere of privacy attendant to

personhood. That guarantee is foundational to our national promise, and we must be vigilant in our efforts to ensure it is not eroded. The way in which we articulate its contours is not static, because the conditions in which information about each of us is discoverable by the state is not static.

For the first two centuries of our nationhood, Fourth Amendment doctrine has been based in large part on a fairly simple rubric about what is private and what is not; something is not private if it is observable to the public, or if it is voluntarily disclosed to another, or if it is outside your home. But in many ways, as the differences between Katz's world and today's exemplifies, those assumptions no longer hold. As technology has developed, old assumptions and guideposts are ever challenged, providing doctrinal puzzles that we must solve with coherence and with respect for the principles that undergird the Fourth Amendment. The old rules of thumb are deteriorating as useful metrics of the reasonableness of an expectation of privacy.

The Supreme Court's most recent articulations of Fourth Amendment doctrine have recognized that, just as privacy rules for an agrarian society did not translate well into an industrial one, privacy rules from the Industrial Age do not translate well into the Information Age. For instance in Kyllo v United States, the Court held that a thermal imaging scan of a suspect's home was a search; "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search—at least where (as here) the technology in question is not in general public use" (533 US 27, 34 [2001], quoting Silverman v United States, 365 US 505, 512 [1961],

internal citation omitted). That holding challenged the old doctrinal assumption that a person had no expectation of privacy in something "observable" to law enforcement.

Increasingly, Fourth Amendment jurisprudence is retreating from the traditional third-party doctrine, in recognition that a *sine qua non* of modern society is the deposit of mountains of personal data with third parties who preserve it indefinitely. Most recently, in Carpenter v United States, the Supreme Court held "that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI," or cell-site location information, the vast data that places a cell phone—and, by implication, its user—in a particular place at a particular time (138 S Ct 2206, 2217 [2018]). Accordingly, the Court concluded, the government could not obtain CSLI from wireless carriers, which it had used at trial to place Mr. Carpenter near the locations of several robberies for which he was charged, without a warrant. Carpenter grew from the Court's earlier decision in Riley v California, which held that the police may not, without a warrant, search the digital contents of a cell phone lawfully seized from a person who has been arrested (134 S Ct 2473 [2014]). In both cases, the government seized the data at issue from a third-party wireless carrier with which the user had indisputably and knowingly shared it.

The mere fact of disclosure to a third party, however, did not eliminate the user's expectation of privacy in that information. Indeed, in Carpenter, the defendant's movements were on the public streets, and he would have been visible to anyone in his vicinity. Under a traditional view, he could not have had a reasonable expectation of

privacy in his location, but the Court held that he could have a reasonable expectation of privacy in the location data sent by his cell phone to his wireless carrier. Mr. Carpenter's wireless carrier needed to have that information for its own business purposes, not to aid the government in prosecuting Mr. Carpenter; likewise here, DOC needs to record Mr. Diaz's phone calls for its own security purposes, not to aid the government in prosecuting Mr. Diaz.

In its shift away from the blind application of the third-party doctrine, the Court recognized that that doctrine "partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another" (Carpenter, 138 S Ct at 2219); by sharing information with a third party, such as a bank (see United States v Miller, 425 US 435 [1976]) or a telephone company (see Smith v Maryland, 442 US 735 [1979]), an individual is traditionally said to have "assumed the risk that the company would reveal to police" the information at issue (Smith, 442 US at 744).

But, that "diminished privacy interest does not mean that the Fourth Amendment falls out of the picture entirely" (Riley, 134 S Ct at 2488). Importantly, Smith and Miller "did not rely solely on the act of sharing" to hold that the information at issue was not private (Carpenter, 138 S Ct at 2219). Instead, the Court considered "the nature of the particular documents sought to determine whether there is a legitimate expectation of privacy concerning their contents" (id. at 2220, quoting Miller, 425 US at 442, internal quotation marks omitted). In Carpenter and Riley, the nature of the cell phone information sought—a robust record of the user's life and whereabouts—made it sufficiently

distinguishable from the bank records sought in Miller and the outgoing numbers dialed from a landline sought in Smith.[10] Given the ubiquity of modern cell phones and their technological capacity to trace our every location and communication, "in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements" (Carpenter, 138 S Ct at 2220, quoting Smith, 442 US at 745).

That comparison emphasizes the new nature of smartphone technology and the massive quantity of data stored on those devices to distinguish Carpenter and Riley from prior third-party doctrine decisions. Although in Mr. Diaz's case the intrusion stems from good, old-fashioned landline surveillance, it too involves modern technology that made it possible for DOC to record and store massive amounts of data and deliver more than a thousand voice recordings to the District Attorney with the click of a mouse. The intrusion is also distinguishable in a more odious way: the third party obtaining and sharing the information is not a private party but is instead an arm of government. It is exactly such governmental intrusions from which the Fourth Amendment shields us.

The attempt to reconcile old doctrine with an evolving new doctrine is difficult. In his concurring opinion in Riley, Justice Alito expressed concern that the majority opinion

[10] Although the Court has distinguished, not overruled, cases such as Smith and Miller along these lines, I agree with Justice Marshall that "[t]hose who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes" (Smith, 442 US at 749 [Marshall, J., dissenting]); "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance" (id. at 750). For that reason, such third-party disclosures constitute consent for the information at issue to be shared with the third party company only, not with law enforcement.

extended more protections to the outgoing phone calls of arrestees using a cell phone to comparable calls made using a landline. But, recognizing that that there was no workable alternative, he agreed with the decision that the Fourth Amendment does not allow warrantless search of a cell phone lawfully seized from an arrestee.

Justice Alito's point is well-taken and exposes a tick in the development of Fourth Amendment doctrine. Distinguishing modern smartphones from older, more "traditional" forms of technology reflects the perspective of a particular point in time—a basis that makes little sense when the founding principles that underlie the Fourth Amendment do not contemplate differences between the technological developments of a subsequent era. "Traditional surveillance techniques" are only traditional from our vantagepoint; the new technology of a smartphone will seem traditional, perhaps passé, to the next generation.

Soon, it might not be unusual to see people walking down the street wearing X-ray goggles—will others have forfeited their expectation of privacy in whatever those goggles can see? After all, they are in public, where their expectation of privacy is diminished, and the search image is "observable" thanks to technology in "general public use" (Kyllo, 533 US at 34 [limiting its holding that observations conducted with sense-enhancing technology may only violate the Fourth Amendment if that "technology . . . [is] not in general public use"]). When advances in biotechnology enable tracking of our movements using biometrics that can be constantly read by satellites, will we have forfeited what expectation of privacy remains in our whereabouts?

I offer those questions not to sound a dystopian alarm, but to underscore that when we apply old Fourth Amendment doctrine to new technologies and develop new rules based on those changes, we must extract the principle—and not the prior articulation—from the old doctrine. The map of a flat world worked for a time, but no longer. The rules that define our right of privacy vis à vis law enforcement must ensure that law enforcement cannot collect evidence in ways that undermine the privacy rights we want to allow as a society. Returning again to Justice Harlan's normative question, the Fourth Amendment asks not only whether the individual asserting the interest has demonstrated a subjective expectation of privacy, but also whether that expectation would be accepted as reasonable by society. Although there may be no principled basis for permitting the police to observe you in your home through a high-power telescope but not through a heat-sensing infrared device, or to place cameras on streets everywhere but not use cell site data to track you, those decisions define the Fourth Amendment's sweep.

The majority's holding here is, in essence, the flat map of the world imposed on a spherical one. DOC claims to have obtained Mr. Diaz's telephone calls out of necessity, just as did the phone company in Carpenter. Mr. Diaz has used those phones out of necessity to communicate with the outside world, just as the plaintiff in Riley used his smartphone to participate in everyday modern life. Mr. Diaz's ability to avoid use of the prison phone for the eight months of his incarceration is far less realistic than Mr. Carpenter's ability to avoid carrying his cellphone during his hours-long crime spree; he could have used burner phones, as many people do when engaging in criminal activity. Yet, the government must obtain a warrant to seize the wireless carrier's records of Mr.

Carpenter's movements—movements that, unlike Mr. Diaz's, were nontestimonial and observable to the naked eye. Application of the third-party doctrine to internet service providers, social media sites, wireless phone carriers, credit card companies, medical insurers and so on would mean that the government may, without a warrant, obtain all that information and more simply because we have "voluntarily" disclosed it to a third party. Instead, Fourth Amendment law, and privacy law more generally, must adapt to times in which we, like Mr. Diaz, have no realistic choice but to divulge information to third parties for a specific purpose, yet retain our rights against the warrantless seizure of that information by the government. Sadly, today's decision is another Olmstead.

For that reason and for those discussed above, I dissent.

* * * * * * * * * * * * * * * * *

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

Decided February 21, 2019