Commonwealth v. Augustine and the Future of the Third-Party Doctrine

Lawrence Friedman*

In Commonwealth v. Augustine,1 the Massachusetts Supreme Judicial Court recognized that the state constitution protects an individual’s reasonable expectation of privacy in cellular telephone call location data, even when that information qualifies as a third-party’s business record. This means that the Commonwealth, in order to gain access to such data, must first obtain a search warrant based upon probable cause, as required by Part I, Article 14, of the Massachusetts corollary to the Fourth Amendment. The Augustine decision has been praised for explicitly addressing the tension between new digital communications technology and basic privacy concerns, and some commentators have even suggested that Augustine may herald the demise of the third-party doctrine.2

On close inspection, however, Augustine, by its terms, does not spell the end of the third-party doctrine. To the contrary, the Supreme Judicial Court’s scrupulous opinion tacitly reaffirms the core of the doctrine: individuals have no reasonable expectation of privacy in information voluntarily revealed to third-parties. Though Augustine points in the right direction as far as privacy is concerned, by itself the decision does not provide a sufficient foundation for a court to seriously question the continued utility of the third-party doctrine. Such a reconsideration is, arguably, long overdue. Regardless whether the third-party doctrine ever represented a sound rule

* Professor of Law, New England Law | Boston. I presented a preliminary version of this essay at the New England Journal on Criminal and Civil Confinement Symposium, “Crime, Privacy, and Technology: The 21st Century Wild West,” on October 16, 2014. Thanks go to my friends and colleagues Tigran Eldred, Victor Hansen, and Shaun Spencer, for their excellent comments and suggestions; and to my research assistant, Suzanne Donnelly, for her superlative research and editing.

of constitutional law, its application today serves to diminish the scope of one’s information privacy well beyond what the U.S. Supreme Court might have contemplated when it first articulated the doctrine nearly four decades ago. Indeed, as we increasingly transact the business of our lives on-line, we are approaching the point at which individuals will no longer be able to legitimately claim that the government must satisfy the requirements of the Fourth Amendment or its state constitutional equivalents prior to obtaining our most personal and intimate information.

I

Before explaining why Augustine reaches the correct result but does not seriously undermine the third-party doctrine, let us take a step back. The doctrine is of modern vintage, deriving primarily from two United States Supreme Court cases, United States v. Miller and Smith v. Maryland, decided in 1976 and 1979, respectively. Miller concerned bank records and Smith the use by police of a pen register device. The court’s conclusion was the same in both: individuals have no reasonable expectation of privacy under the Fourth Amendment when it comes to information they voluntarily convey to third parties, whether it be financial information to a bank or the digits of a phone number to the telephone service provider.

Following these decisions, Congress responded with legislation designed to protect individual financial records and to provide some oversight governing the use of pen registers by law enforcement. But for constitutional purposes, the precedent set by Miller and Smith remains the judicial touchstone: absent some reasonable expectation of privacy, an individual lacks the protections afforded by the Fourth Amendment. Though the Massachusetts Supreme Judicial Court historically has shown a great willingness in recent years to entertain arguments that Article 14 may, in certain circumstances, provide broader protection than would otherwise be available under federal law, the court has not been so inclined in respect to the third-party doctrine or the implications of the doctrine.

5. Miller, 425 U.S. at 436.
7. Miller, 425 U.S. at 437; Smith, 442 U.S. at 745–46.
In a 1980 decision, *District Attorney for the Plymouth District v. New England Telephone & Telegraph Company*, the Supreme Judicial Court addressed the third-party doctrine in the context of a request by the Commonwealth to compel a telephone company to provide it technical assistance in installing a cross frame unit trap device on a suspect’s phone line. At the time, the district attorney’s office was conducting an extensive criminal investigation into illegal gaming operations. The lower court had issued a warrant and order pursuant to statute; that order authorized the interception of wire communications to and from the telephone number subject to the warrant. Though the telephone company did not object to aiding the interception of wire communications, it took issue with the requirement that it provide the government with technical assistance. The Supreme Judicial Court concluded that the judge acted within his discretion in granting the motion to compel: the company would be required to assist in the installation, though it preferred not to act as a government agent, because “it alone ha[d] the equipment and skills necessary to carry out an operation.”

Discussing the “constitutional considerations” raised by the Commonwealth’s request, the court notably observed that “[t]he company did not, and arguably c[ould not], present constitutional objections which might be advanced by others, most particularly the argument that the recording of the source of an incoming call is an unreasonable search” in violation of the rights of one who dials the subject’s telephone number. The court relied upon the U.S. Supreme Court’s then-recent holding in *Smith* that the use of a pen register in a telephone company office was “not a search within the meaning of the Fourth Amendment.”

The court acknowledged that it had suggested, in a prior case, and “in a contrary tone,” that the use of a pen register required compliance with “probable cause requirements of the Fourth Amendment.” In this case, however, “[p]resumably, the Supreme Court would not regard the installation of a cross frame unit trap at a telephone company office as a search in

---

11. A cross frame unit trap or similar device “records the telephone numbers of incoming calls, or attempted incoming calls, to a telephone line under surveillance.” *Id.* at 866.
14. *Id.* at 867.
15. *Id.* at 868.
the constitutional sense.” With this statement, the Supreme Judicial Court tacitly embraced the U.S. Supreme Court’s reasoning in *Smith* and made the third-party doctrine a part of Massachusetts search-and-seizure jurisprudence.

To be sure, the court acknowledged that the protections afforded individuals under Article 14 might be broader than those available under the Fourth Amendment. But here the court did not find an “adequate basis for reaching any conclusion about the constitutional rights of persons who dial the number of the surveyed telephone line.” The lower court had ruled that a wiretap was justified and all statutory requirements had been satisfied; the court accordingly declined to “pass on the possible rights of third persons to object on State constitutional grounds.”

In his dissenting opinion, Justice Paul Liacos noted that the Commonwealth’s actions in the case ought to “sound Fourth Amendment alarms.” He argued that the majority opinion would encourage “dragnet surveillance of telephone subscribers, innocent as well as lawbreakers, without probable cause.” Though he did not entirely disagree with the majority’s constitutional analysis, Justice Liacos “would . . . have gone further to indicate [his] disagreement with the Federal approach” and to explore protections afforded by Article 14. He also observed that nothing in the record demonstrated probable cause to invade the privacy of those individuals placing calls to the suspect’s tapped line; the record accordingly lacked any indication that anyone had called the suspect’s phone number for criminal purposes.

In a subsequent case decided in 1982, *District Attorney for the Plymouth District v. Coffey*, the Commonwealth appealed from an order granting the defendant’s motion to suppress evidence derived from the use of a cross frame unit trap. The Supreme Judicial Court reversed, holding that the evidence should not have been suppressed under either the Fourth Amendment or Article 14, because the Commonwealth had not installed the cross frame

---

18. Id.
19. Id.
20. Id.
21. Id. at 871.
22. Id. at 872 (Liacos, J., dissenting).
23. Id. at 872 n.1 (Liacos, J., dissenting). In a footnote, Justice Liacos observed that the U.S. Supreme Court had endorsed the notion that states may impose greater restrictions on police activity than those required under federal constitutional standards, and that the Supreme Judicial Court had taken this view in other cases and ought to hold that Article 14 “forbids warrantless use of a pen register or of a cross frame unit trap.” Id. He argued that Article 14 should “protect[] the control one has over information about himself.” Id.
24. Id. at 873.
trap, and the telephone company had not violated the Massachusetts wiretap statute or the Federal Communications Act by installing the cross frame unit trap without a warrant.\(^\text{26}\) In *Coffey*, a private citizen had called her telephone company to request that it install a cross frame unit trap because she had been receiving harassing phone calls and wanted to determine their origin.\(^\text{27}\) Because the Commonwealth had not made the request, it had not sought a warrant.\(^\text{28}\) The defendant argued that his Fourth Amendment and Article 14 rights had been violated, and that the use of the device absent a warrant violated the Federal Communications Act of 1934 (FCA).\(^\text{29}\) Relying upon *Smith*, the lower court concluded that no search had occurred within the meaning of the Fourth Amendment and there had been no violation of the FCA because that statute did not prohibit the use of pen registers or similar devices.\(^\text{30}\) Nonetheless, the court ruled the Commonwealth had conducted an improper search under Article 14\(^\text{31}\) and allowed the defendant’s motion to suppress.

On appeal, the Supreme Judicial Court concluded that neither the Fourth Amendment nor Article 14 was implicated on these facts because the Commonwealth had not been involved in the search, notwithstanding that the fruits of the search had been turned over to law enforcement.\(^\text{32}\) The court reasoned that a constitutional analysis was “triggered only when either the Federal or State government is significantly involved in the search, either participating in it or directing it in some way.”\(^\text{33}\) The record before the court contained no evidence that suggested significant state involvement in the search here.\(^\text{34}\) Absent state action, the evidence derived from the trap should not have been suppressed under either the Fourth Amendment or Article 14.

Justice Liacos concurred. He noted that the majority opinion implied that a search had, in fact, occurred when it concluded that the private action did not warrant suppression of the evidence discovered. This implicit finding was at odds with *Smith*, in which the U.S. Supreme Court had held that, despite state involvement, the use of the pen register device had not amounted to a search.

\(^{26}\) *Id.* at 1278.
\(^{27}\) *Id.*
\(^{28}\) *Id.*
\(^{29}\) *Id.* at 1278–79.
\(^{30}\) *Id.* at 1279.
\(^{31}\) *Id.*
\(^{32}\) *Id.*
\(^{33}\) *Id.*
\(^{34}\) *Id.*
The court again addressed the third-party doctrine in the 1990 case, Commonwealth v. Cote. In that case, the district attorney had issued a grand jury subpoena to Allied Answering Service (Allied), seeking its records pertaining to messages and calls received and delivered in connection with the defendant’s account. Allied complied with the subpoena and produced the business records, which consisted of a number of paper message slips. The district attorney then sought an indictment but did not present the grand jury with the message slips Allied had produced and, indeed, did not mention them at all. The grand jury subsequently issued an indictment and the defendant was later convicted.

The defendant argued that the district attorney had misused the grand jury’s subpoena powers—by requesting these records with no prompting by the grand jury—and thereby violated the defendant’s rights under the Fourth Amendment and Article 14. The Supreme Judicial Court agreed that the district attorney had acted improperly by using a grand jury subpoena in a manner that would not further the grand jury’s function. At the same time, the district attorney’s action did not significantly impair the integrity of the grand jury or prejudice the defendant in the proceedings.

The court rejected the defendant’s contention that his constitutional privacy rights had been violated. Relying upon Miller, the court concluded that no expectation of privacy existed in the defendant’s bank records, because he had voluntarily conveyed that information to the banks in the ordinary course of business, thereby assuming the risk that a third-party might disclose this information to the government—a risk that existed notwithstanding the “assumption that [the information would] be used only for a limited purpose and the confidence placed in the third party [would] not be betrayed.” The court noted that Article 14 provided no greater protection than the Fourth Amendment in these circumstances: the defendant had no reasonable expectation of privacy in messages transmitted to an Allied employee.

Commonwealth v. Buccella, a 2001 case, concerned a high school student charged with violating the civil rights of one of his teachers and destroying property. The trial court had granted a motion to suppress certain written work the student had submitted. Unlike in Miller, the defendant

36. Id. at 47.
37. Id.
38. Id.
39. Id.
40. Id. at 48–49.
41. Id. at 50 (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).
here had turned over information to a governmental entity—a public high school—and not to a private third party. Given that school attendance is compulsory, the court reasoned that such submission of written work is not “entirely voluntary.” The Supreme Judicial Court expressed doubt as to whether the principles underlying *Miller* would even apply in this context, observing that “[i]t would appear reasonable to expect that a government agency, to which a citizen is required to submit certain materials, will use those materials solely for the purposes intended and not disclose them to others in ways that are unconnected to those intended purposes.” In the circumstances of this case, then, the student had a reasonable expectation of privacy that papers given to public school teachers would be used solely for educational purposes.

II

And now we come to the Supreme Judicial Court’s 2014 decision in *Commonwealth v. Augustine*. In the course of investigating the death of the defendant’s girlfriend, prosecutors obtained “cell site location information” (CSLI) regarding the defendant’s location around the time of the girlfriend’s disappearance. This was the information in dispute. As the trial court explained, under the Stored Communications Act (SCA), the government may require a provider of an electronic communication service to disclose records pertaining to subscribers through judicial order based upon “specific and articulable facts showing that there are reasonable grounds to believe that the contents of wire or electronic communication . . . is relevant and material to an ongoing criminal investigation.” The Commonwealth applied for and obtained such an order in *Augustine*.

The defendant nonetheless argued that government access to CSLI would “infringe[] on one’s reasonable expectation of privacy under [A]rticle 14,” as well as under the Fourth Amendment. In response, the Commonwealth maintained that cell phone users have no reasonable expectation of privacy in CSLI, a business record, because they voluntarily

43. *Id.* at 383.
44. *Id.*
45. *Id.*
48. *Id.* Cell phones, as opposed to land lines, use radio waves that are transmitted to base stations any time a cell user places a call or sends a text message; additionally, through the process of registration, cell phones will periodically identify itself to a cell tower when a phone is turned on. One can determine a cell phone’s location by correlating the precise time and angle at which a phone’s signal arrives at different cell towers. *Id.*
49. *Id.* (quoting 18 U.S.C. § 2703(d)).
50. See *id.*
transmitted the information to the cell phone provider. Absent a reasonable expectation of privacy, Article 14 did not require the Commonwealth to secure a warrant in order to obtain the information.

The lower court found that Miller and Smith did not apply to CSLI, reasoning that the ordinary cell phone user may well understand that these devices use radio waves to connect calls, but it “requires a jump in logic” to conclude that “the user is also aware that his provider is making a record of the location from which he made the call and is storing it for some indefinite period.” Further, “there is no overt or affirmative act by the user whereby she voluntarily exposes her location to a third party.” Rather, CSLI is automatically generated without the cell subscriber’s participation. Finally, CSLI is generated “even without a call being made” through the registration process. It follows, the court concluded, that one cannot “assume[] the risk” that the government will be able to track one’s movements simply by carrying a cell phone on one’s person.

The Commonwealth sought interlocutory review with the Supreme Judicial Court. It argued, first, that there was no state action because the Commonwealth played no role in collecting the CSLI at issue; rather, Sprint collected the data on its own, and it existed prior to the Commonwealth’s involvement in this case. The court rejected this argument, explaining that, when the government compels a private party to provide to it an individual’s personal information, there is state action. Next, the Commonwealth argued that, pursuant to the third-party doctrine, it did not need to obtain a warrant in this instance and it was entitled to obtain the CSLI from Sprint so long as it complied with statutory requirements. The court acknowledged the precedent set by Miller and Smith but declined “to wade into these Fourth Amendment waters,” instead focusing on the third-party doctrine under Article 14—specifically, “whether, notwithstanding that the CSLI is a business record of the defendant’s cellular service provider, the defendant ha[d] a reasonable expectation of privacy” recognized and protected by Article 14.

51. Id. at *5.
52. Id.
53. Id. at *6.
54. Id.
55. Id.
56. Id.
57. Id.
59. Id. at 856.
60. Id. at 855.
61. Id. at 858.
The court agreed with the defendant that the nature of cellular use and technology in current society “render[ed] the third-party doctrine of Miller and Smith inapposite; the digital age has altered dramatically the societal landscape from the 1970s, when Miller and Smith were written.” The court observed that cell phones have become an indispensable part of modern life, with many individuals and households electing to forgo landline telephones. More importantly, cell phones physically accompany their users and are “almost permanent attachments to their bodies.” Consequently, the court reasoned, CSLI implicates the same privacy concerns as a GPS tracking device—and may reveal even more personal information because this information tracks a user’s location well beyond the places that a car could travel.

The court noted that CSLI is produced and maintained purely as a function of cellular telephone technology—unlike financial information or numbers dialed on a landline, as in Miller and Smith, CSLI is not provided voluntarily. Indeed, the transmission of this information is not connected to the reasons people use cell phones—for example, to place calls or to access the Internet. In other words, individuals do not buy cell phones to share detailed information as to their whereabouts. And so the court concluded that, despite the fact that CSLI is a private cell service provider’s business information, “it is substantively different from the types of information and records contemplated by Smith and Miller.” Accordingly, it would be “inappropriate” to apply the third-party doctrine to CSLI.

The court went on to consider whether CSLI implicates the defendant’s privacy interests so as to trigger Article 14’s search warrant requirement. In this case, the defendant had manifested a subjective privacy interest in his CSLI records, one that the court concluded society would recognize as reasonable. Consequently, government-compelled production of the de-
fendant’s CSLI records held by Sprint constituted a search in the constitutional sense; henceforth, the Commonwealth “generally must obtain a warrant before acquiring a person’s historical CSLI records.”

In dissent, Justice Ralph Gants distinguished between two types of CSLI: “telephone call CSLI” (here, sought by the Commonwealth and ordered by the court) and “registration CSLI” (providing location points of a cell phone only when a call is made or received). While registration CSLI is automatic every seven seconds, telephone call CSLI is episodic. The dissent argued that the material differences between the two types of CSLI have constitutional consequences: the “distinctive characteristics” of CSLI upon which the majority relied characterize registration CSLI, not telephone CSLI, and there is a world of difference between these two types of CSLI in respect to the location points they reveal and the degree to which disclosure of this information might intrude upon personal privacy. The dissent maintained that the telephone call CSLI is much closer to the traditional telephone records that are still governed by Smith and the third-party doctrine. Moreover, the dissent observed that cell phone users must recognize, at least implicitly, that in order to complete a call the cell company must identify both the location of the cell phone and the number called. The dissent accordingly would have applied the third-party doctrine to the telephone call CSLI at issue in this case and in similar future cases.

III

The result in Augustine flows from precedent. Voluntariness lies at the core of the Supreme Judicial Court’s conception of the third-party doctrine, though it (no less than any other court) has not endeavored to explain in so many words what voluntariness means in the constitutional sense. Still, the precedent cases track the general view of voluntariness articulated by the philosopher, John Hyman: “a certain thing is done voluntarily if, and only

70. Id. at 866-67.
71. Id. at 868 (Gants, J., dissenting).
72. Id.
73. Id. at 869-70.
74. Id. at 870-71.
75. Id. at 871 (arguing that location information is not unique to telephone call CSLI, as calling a landline home or work telephone would still reveal the call recipient’s location). What has changed is the mobility of the telephone. The “patchwork of location points” is “less intrusive than the patchwork of personal affiliations that can be learned from traditional telephone records." Id.
76. Id. at 871.
77. Id. at 874.
On this understanding, a student’s disclosure to a public school in *Buccella* was not voluntary because it was compelled by law. And the defendant’s disclosure of CSLI in *Augustine* was not voluntary because it was made out of ignorance. Ignorance of how cellular communications technology actually works is what takes *Augustine* out of the traditional third-party doctrine framework and puts it into the same category as *Buccella*: a disclosure that cannot be considered to be voluntary. In this light, *Augustine* is an illustration of an exception to the third-party doctrine, and does not necessarily foreshadow its rejection; in other words, in a future case in which a defendant’s disclosure to a third party was neither compelled nor the result of ignorance, *Augustine* offers little support for the argument that the third-party doctrine should not control.

This analysis elides the fact that *Augustine* quite voluntarily entered into a contract with a cell phone service provider. And so we ought to ask: would the result in *Augustine* have been the same if the record showed that the service provider had explicitly informed the defendant his phone would be revealing geolocation information to it when his phone was in use, without any overt action on his part? If that had been the case, the defendant could not be said to have acted out of ignorance when he purchased the phone, entered into a contract with a service provider, and proceeded to make calls. Rather, he would have acted out of neither ignorance nor compulsion, and the third-party doctrine would apply to the CSLI generated by his phone. Indeed, going forward the government could undermine the utility of *Augustine* and similar cases simply by mandating that cellular phone service providers prominently disclose to purchasers what information their phones will be broadcasting to providers when in use.

---

80. See *Augustine*, 4 N.E.3d at 862 (stating cellular telephone user does not voluntarily convey CSLI “in the sense that he or she first identifies a discrete item of information or data point like a telephone number”); see also State v. Earls, 70 A.3d 630, 641 (N.J. 2013) (holding that disclosure of CSLI “is not a voluntary disclosure in a typical sense”).
81. Indeed, the U.S. Court of Appeals for the Fifth Circuit has suggested that cell phone customers in fact know they need to connect to a cell tower to complete a call, and that service providers save geolocation information. See *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013).
82. See, e.g., State v. Earls, 70 A.3d 630 (N.J. 2013).
83. Cf. Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (observing that “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”).
The problem here is that voluntariness is simply too expansive (or elusive, as the case may be) a concept to encompass all the ways in which we might reveal information to third parties on a daily basis—actions that most of us likely regard as necessary to living our lives, but which aren’t the product of either ignorance or compulsion. As U.S. Supreme Court Justice Thurgood Marshall put it in his dissent in *Smith*, “[i]t is idle to speak of ‘assuming’ risks in contexts where, as a practical matter, individuals have no realistic alternative.” Justice Liacos, of the Supreme Judicial Court, echoed this sentiment in his dissent in *New England Telephone*, observing that “the reality of modern life precludes a rational argument” that certain decisions to convey information like “telephone numbers to the telephone company” should be considered to be “voluntary.”

Because constitutional text, unlike ordinary legislation, cannot be readily altered in the face of changed circumstances, it necessarily falls to the judiciary to ensure that a particular constitutional provision will continue “to accommodate the needs of different historical ages.” Absent such accommodation, a constitutional provision may be diminished to the point of irrelevance. Accommodation is accomplished through the development and refinement of doctrinal frameworks: whether addressing an equal protection challenge to a legislative classification or a Fourth Amendment challenge to a search, courts assess the constitutionality of state action through the lens of a doctrinal test designed to implement the constitutional commitment at issue. When the application of a doctrinal framework effectively and predictably results in the denial of a particular protection, the doctrine has failed of its purpose: a constitutional command should not be rendered irrelevant by the deficiencies inherent in a court’s effort to operationalize that very command.

A continued reliance upon the third-party doctrine poses precisely this threat to the constitutional protection of information privacy as against the government—at least in cases in which the existence of a reasonable expen-
tation of privacy turns on the determination whether an individual voluntarily disclosed the information at issue. It is time for the courts to revisit the third-party doctrine: there must be a better doctrinal path than the one spelled out by Smith and Miller, one that does not leave privacy protection to be enjoyed only by those few who legitimately can claim to have acted out of ignorance or compulsion. We need a test that recognizes the important distinction between sharing information with the world—by, say, wearing a shirt emblazoned with your social security number—and sharing it in the context of a relationship of trust, the kind of structured relationship we enjoy with friends or family members or health care providers or banks. Such relationships are bounded by an expectation—sometimes informal, sometimes express—that certain information, in the interests of both parties, will not be subject to disclosure outside the relationship absent some kind of notice and mutual agreement.

Of course, trust can be misplaced, and all of these relationships hold the potential for betrayal. Indeed, that potential underlies the reasoning of the 1966 case, Hoffa v. United States, upon which Smith and Miller rely. In Hoffa, the U.S. Supreme Court casually observed that “[t]he risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak.”

This observation appears to state a simple truth, but it overlooks the fact that the risk of betrayal is not foremost in mind when we communicate within relationships of trust, precisely because they are relationships of trust. Disclosures within such relationships are different, due to the legitimate foundational expectations of the parties. And, we have the ability to address such betrayal within the context of the relationship—by, for example, shaming the friend or family member who betrayed us, or by ceasing to do business with the bank that disclosed our account information against our wishes. There is even the possibility in some cases of a suit in tort or contract. Such remedies are not available when one simply broadcasts in-

89. See Alex Kozinski & Eric S. Nguyen, Has Technology Killed the Fourth Amendment?, 2011-2012 CATO SUP. CT. REV. 15, 29-30 (“If the courts continue to apply [the third-party] rationale, then pretty much nothing will be private . . . .”).


92. See, e.g., Helen Nissenbaum, Privacy as Contextual Integrity, 79 WASH. L. REV. 119, 141-42 (2004) (noting that “[c]onfidentiality is generally the default [in a friendship]—that is, friends expect what they say to each other to be held in confidence a not arbitrarily spread to others”).

93. See, e.g., Neil M. Richards & Daniel J. Solove, Privacy’s Other Path: Recovering
formation to the world; in that case, the actor has taken no steps whatever to limit access to the information, and has no cause to complain when it is seen or heard by anyone, including the government or its agents.

Importantly for constitutional purposes, absent an agreement to expand the relationship of trust to others, no one else—much less the government—is necessarily privy to any disclosure made within the relationship itself. It therefore is not reasonable to assume that a piece of information, once disclosed by a party in the relationship, automatically should become fair game to anyone outside the relationship. When our friends or family members or doctors or banks betray us, the betrayal reflects no intention on our part to authorize further disclosure to someone outside the relationship—after all, we did not authorize the initial betrayal.

All of this is to say that it does not seem impossible to differentiate, for the purpose of deciding when the constitutional protection against searches and seizures ought to be triggered, between those instances in which disclosures to others eliminate constitutional protection and those instances when disclosures do not. Simply put, not all disclosures to third parties are the same. And a doctrine that reflected this point would better fit with how we humans function in today’s interconnected world, which is one in which information-sharing within relationships of trust has become an accepted part of everyday life.94

This understanding of the third-party doctrine offers a more forward-looking explanation for why, in Augustine’s case, law enforcement should have secured a search warrant for his cell-phone geolocation information. Augustine shared that information with his cell phone service provider as an aspect of the contractual relationship into which the parties entered. It would not be unreasonable for individuals in his position to expect that sharing information with a cell service provider in the context of a contractual relationship did not mean they had thereby made that information available to anyone else who might find it useful, including the government.95

94. See Kozinski & Nguyen, supra note 89, at 29.
95. Adoption of the approach to the third-party doctrine I sketch here would necessitate a new look at the misplaced trust cases, too, to see whether the relationships in which disclosures occurred in those cases would qualify as relationships of trust.
Of course, revisiting the third-party doctrine along the lines suggested here could be seen as a radical move, because of the potential to provide privacy protection to criminal activity. Orin Kerr has defended the third-party doctrine on the ground that it maintains the Fourth Amendment balance between privacy and security by serving two important purposes. First, it prevents criminal suspects from acting “opportunistically to effectively hide their criminal enterprises from observation” through the use of third parties that allow them to shield from observation what would have been observable, thereby preventing law enforcement from developing the evidence of crime needed to get probable cause to secure a warrant. Second, he argues the third-party doctrine fosters ex-ante clarity in search-and-seizure rules. Under the doctrine, he reasons, “the history of information is erased when it arrives,” so “the law can impose rules as to what the police can or cannot do based on the location of the search instead of the unknown history of the information obtained.” This means that law enforcement will not, having stumbled across information held by a third-party, struggle to determine whether that information is available to it then, or whether it must secure a warrant before seizing the information.

Kerr’s arguments in support of the third-party doctrine appear to be premised upon the assumption that courts should strike a balance between privacy and security in assessing the legitimacy of an asserted individual privacy interest. It is far from clear, though, that a concern for security should be relevant to the initial determination whether the Fourth Amendment or one of its state constitutional analogs is applicable. Under the test derived from Justice John Harlan’s concurring opinion in *Katz v. United States*, whether a claim of privacy is objectively reasonable turns on the nature of the circumstances and the individual’s actions in respect to the information the government seeks to obtain. On this analysis, either there is or is not a legitimate privacy interest at stake, regardless whether judicial recognition of the existence of that interest might somehow impede law enforcement.

97. See id. at 576.
98. See id. at 581.
99. Id. at 582.
100. Id.
103. Cf. id. at 362 (noting that, even when an individual discloses information in a
At a basic level the trigger for the constitutional protection of privacy under the Fourth Amendment functions no differently in practice than the triggers for other individual rights protections. Consider the test to determine when the First Amendment’s free speech guarantee applies to conduct. There, the existence of protection depends upon whether “[a]n intent to convey a particularized message was present, and [whether] the likelihood was great that the message would be understood by those who viewed it.”104 It does not matter that the recognition of a legitimate expressive component might undermine some governmental interest. Rather, the governmental interest factors into the next analytical step: whether it is sufficiently important to outweigh the individual’s speech interest—or, in the Fourth Amendment context, whether it is sufficient to justify a search.105 Absent either a legitimate speech or privacy interest, of course, the government may regulate the conduct in question or search as it will, without regard to the relative importance of its reasons for doing so.106

To be sure, Kerr is right that a third-party doctrine that distinguished between different kinds of disclosures would not have the ex-ante clarity of the current doctrine. But some greater clarity likely would develop over time. As discussed in this essay, there are principled ways in which law enforcement can tell that certain information in the hands of third-parties will require a warrant—as, for example, when the police seek information being held by a third-party that has a relationship of trust with the suspect, such as an ISP or a cell phone service provider.107 In Augustine, law enforcement knew who held the records containing the geolocation information and they knew the history of how that information came to be in the cell service provider’s possession. There was no mystery—and there would be no mystery in many cases—about the provenance of this information, or about the reasonable expectations the parties to the relationship held about requests from others to disclose it.

V

At bottom, Augustine rests on ignorance by individuals about how digital communications technology actually works. That is a fragile thread up

---

105. See, e.g., Texas v. Johnson, 491 U.S. 397, 407 (1989) (whether a restriction on expression is valid depends upon “the governmental interest at stake”).
106. As Shaun Spencer has observed, even given a legitimate privacy interest, the concern for security typically will prevail. See Shaun Spencer, Security Versus Privacy: Re-framing the Debate, 79 DENV. U. L. REV. 519 (2002).
107. See supra notes 89-90, 92-94 and accompanying text (discussing relationships of trust).
on which to hang the protection of privacy in the face of technology that allows us to enter into new information-sharing relationships with third-parties on a daily basis. *Augustine* is a step toward reconsideration of the implications of the traditional third-party doctrine, but it really just postpones to another day a reckoning that may shape the future of the constitutional protection against unreasonable searches and seizures.