No. 16-611

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

PAPAYA CELLULAR, INC.,

Respondent.

ON WRIT OF CERTIORARI TO THE
UNITED STATES COURT OF APPEALS
FOR THE AMES CIRCUIT

REPLY BRIEF FOR PETITIONER

The Daniel J. Meltzer Memorial Team

LUKE BEASLEY
BENJAMIN BURKETT
WILLIAM FERRARO
AMANDA MUNDELL
TRENTON VAN OSS
CONNOR WINN

Counsel for Petitioner

NOV. 1, 2016, 11:45 A.M.
AMES COURTROOM
HARVARD LAW SCHOOL

Oral Argument

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

This case presents a statutory question Congress already answered and a constitutional question this Court's precedent resolves. Under the Stored Communications Act, an order does not impose an "undue burden" unless the resources spent to comply with a single order outweigh the government's interest in the information sought. And under longstanding Fourth Amendment precedent, individuals retain no expectation of privacy in information they voluntarily convey to a third party. Those principles pave the way to the answer here: Papaya must provide Doe's location data.

Papaya does not challenge these principles. It concedes that the SCA requires a balancing test, ignores the government's textual arguments, and instead raises "burdens" foreign to the SCA's detailed scheme. And rather than seriously contest the government's application of the third-party doctrine, Papaya would abandon five decades of Fourth Amendment jurisprudence. Because these arguments do not respond to the questions this case presents, they do not change the answers.

ARGUMENT

I. The § 2703(d) order is not unduly burdensome.

Papaya cannot escape the text of the SCA or the context of this case. The SCA's text bars consideration of Papaya's novel burdens. And, as Papaya agrees, the phrase "undue burden" requires examining the government's interest in preventing a fourth terrorist attack. Because that interest outweighs the minimal effort it would take Papaya to comply, the order is not unduly burdensome.

A. The district court's interpretation of "undue burden" is reviewed de novo.

This Court granted certiorari on the question whether the order imposes an "undue burden . . . within the meaning" of 18 U.S.C. § 2703(d). J.A. 1. Papaya admits that the Court must "interpret" the phrase "undue burden" to answer this question. Resp't's Br. 6. Questions of statutory interpretation are reviewed de novo. *See, e.g.*, *Firestone Tire & Rubber Co. v. Bruch*, 489 U.S. 101, 117 (1989).

Papaya relies on a single district court case to suggest that interpretation of the phrase "undue burden" should be reviewed for abuse of discretion. *See* Resp't's Br. 11. But that case never *interpreted* a statutory term; it merely *applied* the (well-understood) "specific and articulable facts" requirement in § 2703(d). *See In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 126 (E.D. Va. 2011). Papaya's argument

that this Court should defer to the district court's statutory interpretation has no support in the law.

B. "Undue burden" includes only the resources spent to comply with a single order.

Papaya must comply with the order unless "the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden." 18 U.S.C. § 2703(d) (2012).

Papaya does not address the government's textual argument that the phrase "compliance with *such* order" in § 2703(d) indicates that courts may look only to burdens relating to the *sole* order before the court. Pet'r's Br. 15–16. Nor does Papaya address the government's argument that the phrase "unusually voluminous" implies an order-specific reading of undue burden, since the "unusually voluminous" exception makes sense only when it applies to the order under consideration. In total, the government has provided five reasons why the plain text of the SCA indicates that "undue burden" is order- and resource-specific. Papaya disputes only two.

Papaya argues that the word "otherwise" expands the category "undue burden" to include more than resource-specific costs. Resp't's Br. 18–19. But this interpretation reads "unusually voluminous" out of the statute. Under Papaya's reading, "unusually voluminous" would neither add to "undue burden" (since "undue burden" would already

include voluminous requests) nor limit it (to resource-specific costs). By contrast, reading "unusually voluminous" to limit "undue burden" comports with how this Court interprets enumerated lists. *Cf. Yates v. United States*, 135 S. Ct. 1074 (2015) (limiting "tangible object" in list "record, document, or tangible object" to objects similar to records and documents).

Papaya next argues that "undue burden" cannot be resource-specific because resources spent on compliance are "always reimbursed." Resp't's Br. 29. In Papaya's view, that means a company would never face an "undue burden" because reimbursement would always cancel out its costs. But that argument mischaracterizes the SCA's reimbursement section, which provides reimbursement only for *reasonable* costs, not *actual* costs. 18 U.S.C. § 2706(a). There may be circumstances where a court does not compel compliance because reimbursement will not replenish the resources spent to comply. For example, if compliance would take a software engineer one week, the government would reimburse one week's salary at the market rate. *Cf. Hensley v. Eckerhart*, 461 U.S. 424, 447 (1983) (reasonable attorney's fee calculated using prevailing market rates). If the engineer had a salary greater than the market rate, the government would not reimburse the difference — and that shortfall could impose an undue

burden. But none of this changes the fact that the burdens considered in this calculus are the resources spent, and nothing more.

C. "Undue burden" does not include Papaya's claimed burdens.

Papaya concedes it faces no substantial resource-specific burdens. Resp't's Br. 29. Instead, it urges this Court to adopt an unprecedented reading of § 2703(d)'s "undue burden" standard to include Papaya's status as a non-party to the government's investigation, future effects of compliance, and damage to Papaya's brand. Resp't's Br. 18.

To begin, Papaya must comply with the order precisely *because of*, not *in spite of*, its non-party status. The SCA was specifically designed to reach non-parties, *see* 18 U.S.C. § 2703(c), and the "undue burden" inquiry proceeds under that assumption. Papaya admits that it is a "provider of electronic communication service within the meaning of the Stored Communications Act." J.A. 35. Papaya's status as a non-party cannot be a burden.

Papaya's argument about future effects similarly misses the mark. Papaya worries that hackers will acquire its software, even though Papaya intends to destroy it. J.A. 31. Accepting that argument demands four speculative leaps. First, the Court must assume that Papaya cannot erase the software from its servers. Second, it must believe that hackers care about the location

information the software unlocks, as opposed to more valuable information like financial records. Third, the Court must presume the hackers will successfully breach Papaya's servers. And fourth, it must assume the hackers can repurpose the software to target any user, even though Papaya will develop a program that targets only Doe. J.A. 30. The SCA does not subject courts to this guessing game.

Papaya next asks the Court to speculate about the cumulative burdens of future orders, without providing any way to quantify the number of future orders or the burdens they would impose. On top of that, Papaya asks the Court to count those future burdens *now*, when assessing the current order, and again *later*, when assessing each future order. Resp't's Br. 20. But Papaya concedes that the burdens of future orders must be weighed against the governmental interest at stake. *Id.* So unless Papaya would extend its double-counting to the government's future interests, this regime is not just speculative but also profoundly unfair.

Finally, Papaya's attempt to brand its way out of the SCA demonstrates the danger of reading "burden" to include brand. If "burden" includes brand damage, companies can adopt marketing strategies that place them beyond the SCA's reach. Pet'r's Br. 21. Rather than respond to this incentive problem, Papaya offers the perfect illustration of it: Papaya defines its brand as privacy, claims

that compliance would undermine that brand, and thereby escapes the SCA's reach. *See* Resp't's Br. 21. This Court should not let Papaya commandeer the SCA.

D. The government's interest outweighs Papaya's burdens.

Papaya concedes that the Court must balance Papaya's burdens with the government's interest. Resp't's Br. 13. It also admits that it faces no substantial resource burdens; three of its engineers could build the decryption program in a week. J.A. 30. That burden pales in comparison to the government's "interest in stopping future attacks in Ames." *See* Resp't's Br. 13. Papaya cannot alter the balance by claiming the sought-after information lacks "known utility" or is overbroad. Resp't's Br. 15.

Under the SCA, the government need not prove the "known utility" of Doe's information before obtaining it. Courts grant § 2703(d) orders even if there is a "probability that some gathered information will not be material." *In re Application for Order*, 830 F. Supp. 2d at 130. And the district court — which Papaya urges this Court to affirm — already found that the government has "reasonable grounds to believe" that Doe's records are "relevant and material" to investigating the bombings. J.A. 22.

Papaya's claim that the government's request is overbroad fails to grasp the calculated nature of terrorism. *See* Resp't's Br. 16. The

average planning cycle for a terrorist attack is ninety-two days. Brent Smith, *A Look at Terrorist Behavior: How They Prepare, Where They Strike*, National Institute of Justice (July 15, 2008), http://www.nij.gov/journals/260/pages/terrorist-behavior.aspx. Over those ninety-two days, terrorists conduct surveillance, raise funds, manufacture weapons, and perform dry runs. *Id.* Assuming each of the three Ames attacks took ninety-two days to plan, the government's request for just six months of location data is not overbroad.

To secure that data, the government needs Papaya's assistance. Contrary to Papaya's suggestion, Resp't's Br. 17, the government cannot interview everyone who saw Doe use his phone over a six-month period. Nor could the government guarantee that those witnesses would be truthful or accurate. In any event, interviewing witnesses could alert Doe and "jeopardize the ongoing investigation." J.A. 22. Since there is no realistic alternative to Papaya's assistance, this order is justified. *Cf. United States v. N.Y. Tel. Co.*, 434 U.S. 159, 175 (1977) (justifying an order under the All Writs Act because the company's assistance was necessary to access information).

E. The order raises no First Amendment concerns.

The order seeks a specific result — unlocking Doe's data — not specific content. Papaya does not dispute this. Instead, it argues that coding is "expressive conduct" that says to the world, "Papaya endorses

governmental intrusion into its customers' private information." Resp't's Br. 25–26. It does no such thing.

Papaya's broad conception of expressive conduct blurs the distinction between building the program and disclosing Doe's information. The actual conduct that Papaya worries would endorse government intrusion is the act of disclosing information. But disclosing information under a court order does not express Papaya's endorsement of the investigation any more than filling out a tax return expresses one's endorsement of a government policy.

Moreover, if writing code communicates anything at all, the order is merely an "incidental limitation[] on First Amendment freedoms." *United States v. O'Brien*, 391 U.S. 367, 376 (1968). The government may regulate conduct where it has "an important or substantial" interest that is "unrelated to the suppression of free expression." *Id.* at 377. Here, the government's substantial interest in obtaining information to thwart another terrorist attack is unrelated to any particular content- or viewpoint-based message. The order is therefore valid.

II. Obtaining Doe's location data comports with the Fourth Amendment.

Papaya fails to show that the government seeks an unreasonable search. It advances a warped reading of the SCA, rewrites decades of Fourth Amendment doctrine, and imagines a privacy intrusion the government does not propose. None of these arguments rebuts the conclusion that Doe has no expectation of privacy in information he conveys to a third party, and none of them makes the government's attempt to prevent another attack any less reasonable.

A. The SCA does not require a warrant to obtain Doe's location records.

Invoking constitutional avoidance, Papaya claims that Congress intended to require a warrant whenever the government seeks location information under the SCA. But the constitutional avoidance canon applies only where a statute is "susceptible of more than one construction." *Clark v. Martinez*, 543 U.S. 371, 385 (2005). The SCA is not. It plainly allows disclosure of location records pursuant to an order under subsection (d). Section 2703(c)(1)(B) states:

> A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity . . . obtains a court order for such disclosure under subsection (d) of this section.

18 U.S.C. § 2703(c)(1)(B).

Papaya concedes that Doe's location records qualify as "record[s] or other information." Resp't's Br. 32. That leads to a clear statutory directive: the government "may require" Papaya to "disclose [Doe's] record[s]" upon obtaining "a court order for such disclosure under subsection (d)." 18 U.S.C. § 2703(c)(1)(B).

Papaya's attempt to inject ambiguity into the statute fails. Because § 2703(c) lists five ways to obtain subscriber information, Papaya finds the statute ambiguous as to which is required. *See* Resp't's Br. 32. But when Congress listed alternative means to obtain subscriber information, it did not render ambiguous its statement that "a court order for such disclosure under subsection (d) of this section" sufficed. 18 U.S.C. § 2703(c)(1)(B).

Papaya suggests that reading the text to mean what it says would not properly incentivize the government to seek a warrant when it could get a § 2703(d) order instead. *See* Resp't's Br. 35. As an initial matter, the government may have reasons to seek a warrant even though the standard for getting one is higher. It may want to avoid protracted litigation by getting a warrant where none is required. Or it may believe in some cases that a warrant *is* required — where, for instance, its interests are less compelling, or where the disclosure would be more intrusive. Or, in cases where the government seeks both content information under § 2703(a) (which requires a warrant)

and non-content information under § 2703(c) (which does not), it may promote judicial economy to apply for one warrant authorizing both disclosures.

The more fundamental problem, though, is that Papaya's alternative regime is not the scheme that Congress crafted. Papaya proposes that courts pinpoint different types of disclosure on a "spectrum of information" and require "progressively more stringent" procedures for more private information. *See* Resp't's Br. 34–35. But § 2703 does not create a spectrum of information; it contains two clear poles. On one end, Congress situated content information and required a warrant. 18 U.S.C. § 2703(a). On the other, it situated all other "record[s] or other information . . . (not including the contents of communications)" and required only a court order. *Id.* § 2703(c)(1). Papaya concedes that Doe's information falls in the second category, Resp't's Br. 32, and the Court should decline to create a third.

B. Under the third-party doctrine, obtaining Doe's location records from Papaya is not a search.

The third-party doctrine resolves this case: when Doe voluntarily conveyed his location information to Papaya, he forfeited any expectation of privacy in it. *See Smith v. Maryland*, 442 U.S. 735, 744 (1979). The government would therefore not conduct a Fourth Amendment search by collecting that information from Papaya. In a

single paragraph, Papaya advances two arguments to rebut this conclusion. Resp't's Br. 49–50. Neither is persuasive.

Papaya first argues that an individual cannot voluntarily convey information without knowing precisely what that information is. Resp't's Br. 49. Yet *Smith* demonstrates that, under the third-party doctrine, all a Papaya subscriber must know is that he conveys his location information to Papaya. *See* 442 U.S. at 745. Papaya subscribers know that fact. Papaya's argument that its users are unaware that Papaya records their location, Resp't's Br. 49, cannot be squared with its claim that giving the government Doe's data would damage Papaya's privacy brand, Resp't's Br. 21. If Papaya's customers picked Papaya because it promised to protect their data, they must know they are conveying that data to Papaya in the first place.

Papaya also claims that an individual must take an "affirmative step to convey the information." Resp't's Br. 49. But that too runs counter to *Smith*: while landline users do not affirmatively convey the caller's or the recipient's location by dialing a number, law enforcement can still deduce location information from landline records. Regardless, Papaya's argument fails on the facts. Cell phone users *do* take several affirmative steps to disclose their location: getting a phone, selecting a service provider that collects location information, and carrying the phone with them throughout the day. The third-

party doctrine therefore applies, and Doe has no reasonable expectation of privacy in his location data.

Faced with the reality that the third-party doctrine defeats its claim, Papaya urges this Court to radically reshape its Fourth Amendment jurisprudence. But instead of suggesting that this Court overrule the third-party doctrine, Papaya takes aim at the *Katz* reasonable-expectation-of-privacy test. *See* Resp't's Br. 36 (arguing the test leads to "arbitrary results," "provides inadequate protection for individuals," and "erodes Fourth Amendment protection"). It is curious that Papaya wants to disturb *Katz* at all, since that test was "*added to*, not *substituted for*, the common-law trespassory test." *United States v. Jones*, 132 S. Ct. 945, 952 (2012) (discussing *Katz v. United States*, 389 U.S. 247 (1967)). In any event, this Court should reject Papaya's plea to displace the "touchstone of Fourth Amendment analysis." *California v. Ciraolo*, 476 U.S. 207, 211 (1986).

Papaya's proposed replacement for *Katz* reveals the error in pushing it aside. With *Katz* gone, Papaya urges a drastic expansion of the term "person" in the Fourth Amendment. It argues that "[a]n individual's actions, including his movements from one place to another, are as much a part of his 'person' as [his] body." Resp't's Br. 42. Papaya thus claims that "a search of [Doe's] 'person' extends to a search of his actions, including his movements." Resp't's Br. 43.

Papaya's interpretation would prove utterly unworkable. If a person's "actions" were an extension of his "person," then accessing *any* information — no matter how trivial or out-in-the-open — would be a search, since nobody produces information without "acting." This analysis has no stopping point, unless Papaya would protect only those "actions" in which individuals harbor reasonable expectations of privacy. But that would simply revive *Katz* in everything but name.

C. Even if obtaining Doe's location data were a search, it would be reasonable.

If the Court holds that the government would effect a search by collecting location information, it should nevertheless deem that search reasonable: it is a minimal intrusion in an effort to stop yet another terrorist attack in Ames.

Seeking to avoid that conclusion, Papaya misconstrues the Fourth Amendment's reasonableness inquiry. It claims that this Court conducts a balancing test only when the target of a search has a privacy-diminishing status. Resp't's Br. 54. That argument confuses the test for its application: the Court engages in balancing when privacy interests are diminished or other concerns eliminate the need for a warrant. Status is *one* way to demonstrate that a warrant is unnecessary, but the Court has never said that status is the *only* way.

In fact, it has said the opposite: "When faced with special law enforcement needs, diminished expectations of privacy, minimal

intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable." *Illinois v. McArthur*, 531 U.S. 326, 330 (2001). Papaya highlights cases in which a warrant was unnecessary because of the target's status as an inmate, student, parolee, or probationer. Resp't's Br. 54–55. It leaves out the cases approving warrantless searches and seizures of drug suspects' cars, *Pennsylvania v. Labron*, 518 U.S. 938 (1996); drivers at a DUI checkpoint, *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444 (1990); travelers' luggage, *United States v. Place*, 462 U.S. 696 (1983); and robbery suspects, *Terry v. Ohio*, 392 U.S. 1 (1968). In these cases and others, considerations other than "status" led the Court to conclude that a warrantless search, on balance, was reasonable.

The Court should do so again here. The government's interest in preventing another attack is compelling, and obtaining Doe's location data involves only a minimal intrusion. Papaya claims that the order poses "an even greater intrusion" than in cases like *Jones* where the government accessed precise GPS data. Resp't's Br. 44–45. But Papaya's records are worlds apart from GPS data. GPS technology continuously pinpoints an individual's exact location. Papaya's technology, by contrast, provides only a rough estimate of Doe's location — and only when he uses his phone. J.A. 33.

The most precise data the government seeks from Papaya would show the three-block range Doe was in when he used his cell phone. *Id.* Consider a three-block range in Portland, Oregon, a city with smaller-than-average blocks:

Portland, Oregon, *Google Maps*, https://www.google.com/maps/@45.5182101,-122.675813,17.55z.

At most, Papaya's technology could indicate that a user was somewhere within the circle, which contains: one adult bookstore, one park, three medical offices, three law firms, three political organizations, eleven local businesses, fourteen restaurants and bars, and forty-one retail stores. The government would thus struggle to

determine Doe's shopping preferences, much less his "familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

Moreover, Doe's expectation of privacy in this information is diminished. As an empirical matter, only five percent of Americans are "very confident" that the information kept by cellular providers is truly private. Pew Research Center, Americans' Views About Data Collection and Security 7 (2015). And as for location information in particular, this Court has never recognized strong expectations of privacy in a person's public movements. *See United States v. Knotts*, 460 U.S. 276, 281 (1983). Whatever Doe's expectation of privacy, the government's interest in protecting Ames justifies this minimal intrusion. Any search would therefore be reasonable.

CONCLUSION

The judgment of the court of appeals should be reversed.

October 21, 2016

Respectfully submitted,

The Daniel J. Meltzer Memorial Team

_____
Luke Beasley

_____
Benjamin Burkett

_____
William Ferraro

_____
Amanda Mundell

_____
Trenton Van Oss

_____
Connor Winn