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

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

QUESTIONS PRESENTED

1. Does a Stored Communications Act order requiring disclosure of a suspected terrorist's cellular location information place an "undue burden" on the suspect's cell phone provider where compliance would take one week of reimbursable work?
2. Does the Fourth Amendment allow the government to obtain a cell phone provider's records showing a suspected terrorist's whereabouts during three terrorist attacks?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Constitutional Provisions

PRELIMINARY STATEMENT

The facts in this case are dire, but they are not complicated. A terrorist organization has carried out three attacks and promised more. Papaya Cellular holds critical information about the prime suspect's location during the attacks. The government seeks a court order directing Papaya to disclose the suspect's location records. With the clock ticking, the government's best chance to prevent another attack depends on Papaya's compliance.

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Ames Circuit is reproduced at page 2 of the Joint Appendix. The order of the United States District Court for the District of Ames granting Papaya's motion to quash is reproduced at page 36 of the Joint Appendix. The district court's original order is reproduced at page 22 of the Joint Appendix.

JURISDICTION

The judgment of the Ames Circuit was entered on June 4, 2016. The petition for a writ of certiorari was granted on September 6. This Court has jurisdiction under 28 U.S.C. § 1254(1) (2012).

CONSTITUTIONAL AND STATUTORY PROVISIONS

All relevant provisions are reproduced in the Appendix.

STATEMENT OF THE CASE

For the past year, the people of Ames have lived in constant fear. Three times, Ames has suffered a devastating terrorist attack. Three times, the same group has claimed responsibility. And three times, the terrorists have promised more to come. After months of fruitless investigation, the FBI has identified a prime suspect.

The suspect's cell phone provider, Papaya Cellular, has critical information about his location during the attacks. But Papaya refuses to provide that information.

The Ames City Massacre

Last Halloween, a bomb tore through a packed dance club in Ames City. J.A. 16. Fourteen people died, and over forty more were rushed to the hospital. *Id.* The next day, a terrorist group called "Redemption" claimed responsibility. *Id.* This group was new, but its tactics were not: Redemption sent a video to a major news outlet and promised another attack, this time targeting children. *Id.*

The Clarksville Attack

In December, Redemption made good on its word. It set off a bomb at a crowded ice skating rink in Clarksville on a Sunday afternoon. *Id.* Six people, including three children, died. *Id.* Once again, Redemption claimed responsibility and threatened more attacks. *Id.*

The White Pine Middle School Bombing

In March, Redemption bombed a middle school science fair. The explosion killed three children, three faculty members, and the school's principal. *Id.* Several dozen more suffered serious injuries. *Id.* In the immediate aftermath, Redemption vowed to attack again. J.A. 17. But this time, the FBI had a lead.

The Breakthrough

Three days after the attack on White Pine Middle School, the FBI received an anonymous tip. The source had inside knowledge about the first bombing that was never made public. *Id.* He identified one of Redemption's active members — "John Doe" — who may have planted at least one of the bombs. J.A. 3. The source also corroborated Redemption's plans for a fourth attack. *Id.*

The FBI Calls on Papaya

The FBI acted quickly to determine Doe's whereabouts during the three attacks. It sought Doe's location data from his cell phone provider, Papaya Cellular. Any time a cell phone user like Doe makes a call or sends a text, his phone must connect to a nearby cell tower to access the cellular network. J.A. 33. Papaya has records of Doe's connections to its towers. *Id.* The records do not reveal Doe's precise location — only the tower to which his phone connected and the time of

the connection. *Id.* The government needs the records to approximate Doe's whereabouts during each attack.

Like other cell providers, Papaya uses its customers' data on a regular basis. And like other providers, Papaya tells its customers that it will disclose their data to enforce its subscriber contracts, obtain payment from delinquent accounts, and comply with court orders. J.A. 29. But unlike other providers, Papaya uses encryption software to aggregate its users' data and strip it of all identifying information. J.A. 25. Disaggregating user data and isolating Doe's location information would require a software program that only Papaya can build. J.A. 35. Papaya could develop that software in less than a week using a team of three engineers. *Id.*

The Government Seeks an Order

The government applied for a court order under the Stored Communications Act ("SCA") to compel Papaya to provide Doe's information. J.A. 14. The district court issued the order. J.A. 22. But Papaya moved to quash, arguing that (1) complying with the order would cause an "undue burden" under the SCA and (2) disclosing Doe's approximate location data would violate the Fourth Amendment. J.A. 24. The district court granted Papaya's motion. J.A. 36.

The government immediately appealed, and the Ames Circuit set the case for expedited argument "[i]n light of the national security

concerns at stake." J.A. 6. On June 4, the Ames Circuit affirmed the district court, J.A. 3, and the government petitioned for a writ of certiorari. On September 6, this Court granted certiorari. J.A. 1.

SUMMARY OF ARGUMENT

In the past year, terrorists have struck the United States repeatedly. From San Bernardino to Orlando to Chelsea, the attacks are as frequent as they are shocking. Each one is a reminder that as our enemies become more organized and more sophisticated, the government faces new challenges in protecting our nation. Ames now faces a series of coordinated terror attacks carried out by a group that promises to strike again. Papaya Cellular has information that may prevent the next attack. The law gives the government the authority to access that information.

I. The Stored Communications Act offers law enforcement a powerful tool to keep the public safe: it compels cell phone service providers to disclose information that will help the government fight crime. *See* 18 U.S.C. § 2703 (2012). Once the government has shown "reasonable grounds to believe" that the records are "relevant and material to an ongoing criminal investigation," the service provider must produce them. *Id.* § 2703(d). The provider may escape compliance only by showing that the sought-after information is "unusually voluminous" or that compliance imposes an "undue burden." *Id.*

No one questions that the government has reasonable grounds to believe that John Doe's records are relevant and material to

investigating the terrorist attacks in Ames. But Papaya claims that producing the records would impose an undue burden by (1) leading to future court orders, (2) harming Papaya's business model, and (3) violating Papaya's corporate free speech rights. Each argument misapprehends the sort of burdens envisioned by the SCA.

A straightforward reading of "undue burden" defeats Papaya's objections. First, the statute does not leave room for burdens that include future orders, because the statute speaks only to the burdens associated with the *specific* order before the court. Second, the statute does not contemplate burdens related to a provider's business model because the phrase "undue burden" encompasses only the *resources* spent on compliance, like time, labor, and office space. An undue burden must therefore be resource-specific and order-specific: it includes only the *resources* spent to comply with a *single* order.

Whatever Papaya's burdens, they do not exist in a vacuum. To determine whether the order is *unduly* burdensome, this Court must view Papaya's burdens in light of the government's interest in protecting its citizens from future acts of violence. Papaya need only assign three of its engineers to less than a week of work — at a cost fully reimbursable by the government. Ames, by contrast, has already endured three attacks and waits in fear of another. Papaya's burdens

pale in comparison to the government's interest in preventing another attack.

The Court's treatment of similar orders issued under the All Writs Act confirms that this order is lawful. This Court has approved of orders directing a third party to assist in criminal investigations where the third party's compliance was necessary, where its compliance entailed only routine operations, and where the government reimbursed all reasonable costs. *See United States v. N.Y. Tel. Co.*, 434 U.S. 159 (1977). All of those conditions are met here. The order provides for reimbursement, entails minimal effort, does not require Papaya's engineers to do anything out of the ordinary, and is — above all — necessary to help stop another terrorist attack.

Finally, the order raises no "grave" constitutional questions under the First Amendment. *See Rust v. Sullivan*, 500 U.S. 173, 191 (1991). Requiring Papaya to build a software program to isolate Doe's location information does not encroach on Papaya's corporate free speech rights. Papaya's engineers would not communicate by building the program; they would only deconstruct data. Thus, the order calls for conduct, not content, and Papaya's engineers are free to structure their code however they wish. Papaya must therefore comply with the SCA order.

II. Papaya cannot avoid that obligation by invoking the Fourth Amendment. The government violates the Fourth Amendment's prohibition against "unreasonable searches" only when it (1) conducts a search and (2) that search is unreasonable. U.S. Const. amend. IV. Here, neither condition is met. Obtaining Papaya's records of Doe's approximate location would not be a search because Doe maintains no reasonable expectation of privacy in this information. And even if it were a search, that search would be reasonable in light of the threat posed by an imminent terrorist attack.

Papaya's constitutional argument fails to clear the first hurdle. A search occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). But under the Court's third-party doctrine, an individual has "no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

Doe is just the type of individual that *Smith* described. Every time Doe uses his cell phone, he conveys his location information to Papaya's nearest cell tower. Doe knows location disclosure is necessary for cell technology to work, and he knows Papaya can collect that information for whatever purpose it desires. Doe thus voluntarily conveyed his location information to Papaya, forfeiting any expectation

of privacy he may have had in it. Now that the information is in Papaya's hands, the government does not violate the Fourth Amendment by collecting it.

Applying the third-party doctrine here does more than just resolve this case. It also assures consistency with forty years of this Court's jurisprudence and delivers other significant benefits. By declining to protect voluntarily disclosed information, the third-party doctrine ensures that new technology does not render previously public conduct private. It preserves expectations of privacy in the content of private communications. And it strikes a sensible balance between privacy and security that leaves Congress free to respond to new crises and new technologies.

Even if disclosing a third party's location information did effect a search, that search would be reasonable. Searches are reasonable where "legitimate governmental interests" outweigh "the degree to which [the search] intrudes upon an individual's privacy." *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999). Because the search in this case would be minimally intrusive and the government's interest in preventing a fourth attack is paramount, the balance favors the government.

The search here would be minimally intrusive. It would not involve any physical intrusion on the suspect's person, nor would it

invade any area — like the home — traditionally associated with increased privacy concerns. It would not seize any property or interfere with any possessory interest Doe might have in his data. Nor would it reveal the sort of personal information that people expect to be kept private. The Court has long held that a person does not hold strong expectations of privacy in his whereabouts. *See United States v. Knotts*, 460 U.S. 276 (1983). And the data sought here would reveal only Doe's *approximate* location, mitigating any concerns that the government could use it to deduce other, more private information about Doe.

By contrast, the government's interest in stopping another attack is of the highest order. *See Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010). It transcends a general interest in solving crime or gathering evidence. The Court has upheld far more invasive searches based on far less dire threats. A search of Doe's location data is the government's best hope to protect its citizens from the next attack. Comparing that weighty interest with Doe's expectation that his approximate location remain hidden leads to a commonsense and necessary result: the reasonable response is to allow the search.

ARGUMENT

I. This order does not impose an undue burden under the SCA.

The Stored Communications Act is a staple of modern law enforcement. When the government needs to access information relevant to an ongoing investigation, the SCA authorizes a court to order a service provider to turn over subscriber information. 18 U.S.C. § 2703(d) (2012). A service provider must comply with the order unless the records requested are "unusually voluminous" or compliance would otherwise "cause an undue burden." *Id.*

The order in this case does not unduly burden Papaya. Basic principles of statutory interpretation show that courts deciding whether an order imposes an "undue burden" should consider only the resources spent to comply with that specific order. That limitation is necessary to make the SCA workable and preserve its intended reach. And even if § 2703(d) allows consideration of Papaya's business model and the costs of future orders, the government's interests in capturing the suspected bomber and preventing a fourth attack on Ames outweigh Papaya's burdens.

Granting the order here would also comport with this Court's treatment of similar orders issued under the All Writs Act. *See United States v. N.Y. Tel. Co.*, 434 U.S. 159 (1977). The Court has required a third party to assist in criminal investigations where, as here, the third party's compliance is necessary, its compliance would entail

routine operations, and the government would reimburse all reasonable costs.

Finally, asking Papaya to build software to comply with this order presents no First Amendment concerns because the order focuses on function, not content.

A. Only resources spent on a single order qualify as burdens.

Section 2703(d)'s text and context demonstrate that burdens under the SCA are both resource-specific and order-specific: a court deciding whether an order imposes an "undue burden" should consider only the *resources* spent to comply with a *single* order. The "undue burden" standard must be read in context with the immediately preceding reference to "compliance with such order," which indicates that Congress intended a court to consider only the *specific* order before it. Another adjacent phrase, "unusually voluminous," shows that the only relevant burdens are the resources spent on compliance, such as labor, time, and office space.

Considering only the resources spent to comply with a single order yields three benefits. First, courts can easily tally the resources spent to comply with a specific order. Second, focusing on the specific order before the court incentivizes providers to comply efficiently. Third, declining to consider damage to a company's brand prevents

companies from manipulating their marketing strategies to evade the SCA's reach.

1. Text and context show that "undue burden" includes only the resources spent to comply with a single order.

"[T]he starting point for interpreting a statute is the language of the statute itself." *Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc.*, 447 U.S. 102, 108 (1980). Here, the language of § 2703(d) reveals that "undue burden" describes only those burdens that are order-specific and resource-specific. Section 2703(d) provides in pertinent part:

> **(d) Requirements for court order.** — . . . A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are *unusually voluminous* in nature or *compliance with such order* otherwise would cause an *undue burden* on such provider.

18 U.S.C. § 2703(d) (emphasis added).

The phrase "undue burden" must be read "in its context and in light of the terms surrounding it." *Leocal v. Ashcroft*, 543 U.S. 1, 9 (2004). Here, "compliance with such order" and "unusually voluminous" inform the meaning of "undue burden."

Reading "undue burden" in context shows that it is order-specific. The SCA authorizes a court to quash an order if "compliance with *such* order otherwise would cause an undue burden." 18 U.S.C. § 2703(d) (emphasis added). Any "undue burden" must therefore flow

from a *specific* order. An interpretation of "undue burden" that encompasses the speculative cost of future orders reads the words "compliance with such order" out of the statute altogether. But Congress does not waste its breath when it speaks. *See, e.g.*, *Duncan v. Walker*, 533 U.S. 167, 174 (2001). And Congress has shown that, where it wants courts to consider both immediate and future costs, it knows how to say so. *See, e.g.*, 42 U.S.C. § 9607(k)(6)(C)(ii) (2012) (instructing courts to assess "current and future costs" associated with waste treatment facilities).

What's more, the statute expressly ties the burden to "compliance" with a specific order — not to the granting of the order. 18 U.S.C. § 2703(d). Papaya worries that the order will "open the door" to future requests. J.A. 26. But this worry fails to distinguish between the court's *granting* of the order and Papaya's *compliance* with it. Only the district court's action, the granting, sets a legal precedent. And only the legal precedent, not Papaya's compliance, might lead to future orders.

Other words around "undue burden" bolster the conclusion that it is order-specific. The "undue burden" exception immediately follows the "unusually voluminous" exception, which must apply only to the *present* order. *See* 18 U.S.C. § 2703(d). An order-specific limitation on "unusually voluminous" is the only sensible reading. If the

"voluminous" carve-out allowed companies to tally the cumulative volume of information requested in future orders, they could always claim the voluminous exception. And there is no reason for the order-specific limitation to apply to one exception but not the other. The Court seeks to "fit, if possible, all parts" of a statute "into a harmonious whole." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000). The only way to harmonize "undue burden" with "unusually voluminous" is to conclude that the former, like the latter, is order-specific.

"Unusually voluminous" adds something else to the meaning of "undue burden." It limits the burdens considered to the resources needed to comply. The full phrase — "if the information or records requested are unusually voluminous" — conjures images of files, folders, binders, and boxes. "Undue burden" is a catchall for similar resources needed to comply with a specific court order, such as time, labor, and office space. Before this case, the sole court to have denied a § 2703(d) order for being unduly burdensome considered only these resource-specific costs. *See In re Search of Google Email Accounts*, 99 F. Supp. 3d 992, 996 (D. Alaska 2015). And the only other court to have considered the phrase "undue burden" also looked only to resource-specific costs. *See People v. Harris*, 36 Misc. 3d 868, 873 (N.Y. Crim. Ct. 2012) (holding that a § 2703(d) order did not impose an

undue burden because "it [did] not take much to search and provide the data to the court"). "Undue burden" in § 2703(d) thus includes the resources spent on compliance with a single order — nothing more.

The neighboring "Cost Reimbursement" provision of the SCA supports this interpretation. Section 2706(c) allows a court to order "a payment as described in subsection (a)" if producing the sought-after information "causes an undue burden on the provider." 18 U.S.C. § 2706(c). To "reimburse" is to "repay (a person who *has spent* or lost money)." *New Oxford American Dictionary* 1472 (3d ed. 2010) (emphasis added). No wonder, then, that the payment "described in subsection (a)" covers only the resources *already spent* to achieve compliance — that is, those costs "directly incurred in searching for, assembling, reproducing, or otherwise providing" the information. 18 U.S.C. § 2706(a). It follows that the burdens described in § 2706(c) are similarly confined to only those resources spent on compliance with a single order. And since "identical words used in different parts of the same act are intended to have the same meaning," § 2703(d)'s "undue burden" must refer to the same costs. *Atl. Cleaners & Dyers v. United States*, 286 U.S. 427, 433 (1932).

This understanding of "undue burden" also comports with the use of the same phrase in two Federal Rules of Civil Procedure governing discovery. Rule 26(b)(2)(B) exempts from discovery

electronic information that is not "reasonably accessible" because a party faces an "undue burden" in producing it. Fed. R. Civ. P. 26(b)(2)(B). A court facing this kind of objection will consider whether the request lacks "sufficient detail regarding the time, money, and procedures required to produce the requested documents." *Shaw v. Experian Info. Sols., Inc.*, 306 F.R.D. 293, 301 (S.D. Cal. 2015). Likewise, Rule 45(d)(1) bars a litigant from "issuing and serving" a subpoena in a way that imposes an "undue burden" on the recipient. Fed. R. Civ. P. 45(d)(1). This determination depends on factors like "the breadth of the document request, the time period covered by it, [and] the particularity with which the documents are described." *Cohen v. City of New York*, 255 F.R.D. 110, 117–18 (S.D.N.Y. 2008). In other words, the burdens contemplated by both Rules are the resources spent on compliance with a single request. Section 2703(d)'s "undue burden" test is the same.

2. A resource-specific and order-specific reading of "undue burden" preserves the SCA's workability and intended reach.

Considering only the resources spent to comply with a single order achieves three key benefits. First, it makes the statute simple to administer. The resources needed to comply with one order are easy to identify and easy to quantify. In Papaya's case, for instance, the district court already has all the information it needs: compliance will take three engineers, working less than a week, on a few company

computers. And whatever the cost, the government has agreed to reimburse Papaya. J.A. 23.

An order-specific reading also avoids needless speculation about the effect of future requests. Papaya's fear that compliance would result in "regular requests" for new software, J.A. 31, is not much more than guesswork. It also raises a host of questions: How many future orders should a court consider? How far into the future should a court look? Should a court assume that each future order will consume the same amount of labor, time, and other resources? Faced with these questions, courts have declined to consider cumulative costs in analogous contexts. *See, e.g.*, *Mich. Bell Tel. Co. v. DEA*, 693 F. Supp. 542, 546 (E.D. Mich. 1988) (considering § 2706(c)).

The second benefit is that an order-specific reading holds a provider accountable for its own inefficient choices. Papaya admits that its engineers are more than capable of designing a single program that can disaggregate any user's information. J.A. 31. But Papaya would rather build software to disaggregate Doe's information, use it once, and then destroy it. A company following that plan is like a law clerk who throws away her Bluebook each time she proofreads an opinion — and then complains that she has to buy a new Bluebook each time a new opinion crosses her desk. This Court should not credit Papaya for its own self-defeating choice.

Third, a resource-specific reading prevents cell phone providers from branding their way out of the SCA. Papaya is a case in point: because it bills itself as a privacy-protector, it claims that reputational harm stemming from compliance makes it immune from a § 2703(d) order. But that interpretation of "burden" would pave the way for companies to avoid SCA compliance by claiming special treatment to protect their particular brands. What constitutes a burden under the SCA should reflect whether a company is *capable* of complying with an order, not whether a company is *amenable* to complying with an order.

The Court should be especially reluctant to credit marketing strategies that contravene a statute's purpose. Imagine a statute requiring gun dealers to perform a fifty-state background check unless doing so would impose an "undue burden" on the gun seller. And imagine "QuickDraw" — a giant chain of gun emporiums that banks on its slogan "Get Your Gun Fast!" Surely QuickDraw could not opt out of background checks by complaining that compliance would undercut its marketing strategy. The same reasoning applies here. Congress designed § 2703(d) specifically so that telephone providers could *reveal* subscriber information relevant to government investigations. This Court should not entertain Papaya's argument that its marketing strategy depends on *hiding* it.

Courts have long recognized that a party's concerns about its reputation do not permit it to withhold important information. A journalist must reveal her sources when disclosing them would help resolve a criminal investigation — even if the journalist might lose future sources as a result. *Branzburg v. Hayes*, 408 U.S. 665 (1972). A cigarette company must warn potential buyers of the dangers that come with smoking — even if the company might lose sales. *Disc. Tobacco City & Lottery, Inc. v. United States*, 674 F.3d 509 (6th Cir. 2012). And a criminal suspect must produce a handwriting sample when an order demands it — even if that sample might implicate him in a crime. *United States v. Li*, 55 F.3d 325 (7th Cir. 1995). Disclosing important information is not always pleasant, and not always without consequence. But the public has a "right to every man's evidence," whether Papaya likes it or not. *Branzburg*, 408 U.S. at 688. Section 2703(d) safeguards that right.

B. The government's interest in thwarting terrorism means that the burden on Papaya is not undue.

In deciding whether the order imposes an *undue* burden, this Court cannot overlook the stark reality confronting Ames. This order does not exist in a vacuum. It exists to apprehend a man suspected of killing 27 people — and to stop his organization from fulfilling its promise to kill more.

The word "undue" means that this Court should consider the dire circumstances giving rise to the order. Every definition of "undue" involves reasonableness, appropriateness, or proportionality. *See, e.g.*, *New Oxford American Dictionary* 1886 (3d ed. 2010) (defining "undue" as "unwarranted or inappropriate because excessive or disproportionate"). The Court cannot determine whether this order is reasonable, appropriate, or proportionate without considering the context in which it was issued.

The SCA's history confirms the need to consider this order in light of surrounding circumstances. The Act strikes a "fair balance" with respect to the "legitimate needs of law enforcement agencies." S. Rep. No. 99-541, at 5 (1986). More specifically, § 2703(d)'s "undue burden" language instructs courts to consider the "appropriateness of the government's request" in its entirety, not just the costs borne by one party. *Id.* at 39.

The Court has consistently read "undue burden" this way. The "undue burden" test requires courts to weigh "the burdens a law imposes" with "the benefits those laws confer." *Whole Woman's Health v. Hellerstedt*, 136 S. Ct. 2292, 2309 (2016). For example, in determining whether a state law imposes an "undue burden" on interstate commerce, the Court weighs the law's "interference with interstate commerce" against the law's "safety purpose." *Kassel v.*

Consol. Freightways Corp. of Del., 450 U.S. 662, 670 (1981). Likewise, to determine whether an SCA order imposes an "undue burden," this Court should weigh the burden the order imposes against the benefits the order confers.

That side-by-side comparison avoids absurd results. Imagine that complying with an SCA order would cost Verizon Wireless $100,000. If the order would help the government investigate a minor Medicare fraud worth only $1000, then the burdens imposed by the order might well be undue. But if the same order would stop a terrorist from setting off a pressure-cooker bomb at a major sporting event, then the "undue" calculus would most certainly change. In other words, an order that is unduly burdensome in one setting may not be in another. But a court has no way of making that determination without considering an order's benefits to society.

Here, those benefits are weighty. Ames has never faced a threat like Redemption. Dozens have died; scores more are injured; and countless others live in constant fear. Redemption is actively planning its next attack, and the government has an unparalleled interest in preventing it. *See Haig v. Agee*, 453 U.S. 280, 307 (1981).

On the other side of the ledger, Papaya's burden amounts to one week of work by three engineers, fully reimbursed by the government. And even if marketing concerns were "burdens" under the SCA,

Papaya's deserve little weight. It is unclear whether Papaya's public image would suffer if the company helped thwart the next attack. And if Papaya did comply with the order, it would not upset its subscribers' expectations. Papaya's privacy policy contemplates the exact situation before this Court. Papaya announces to all its users that it will "share [their] information" to "comply with court orders." J.A. 29. This Court should not buy an argument that Papaya's customers did not see this order coming.

Papaya's CEO protests that this order "would strike a devastating blow" to his company. J.A. 26. Yet Ames has already suffered a far more "devastating blow," and its citizens live under constant threat of another. If Papaya faces a burden, it is in no way undue.

C. This Court's decision in *United States v. New York Telephone Co.* bolsters that conclusion.

Though the SCA settles this dispute, the government recognizes the dearth of cases interpreting the phrase "undue burden" in § 2703(d). But this Court is not in completely uncharted waters. In *New York Telephone Co.*, the Court approved of a similar order under the All Writs Act ("AWA"), which gives courts the power to grant orders "agreeable to the usages and principles of law." *N.Y. Tel. Co.*, 434 U.S. at 172 (quoting 28 U.S.C. § 1651(a) (2012)). The *New York Telephone Co.* order ("NYTC order") required the company to help the

government install a pair of pen registers — devices that record the numbers dialed on a phone — to investigate a gambling ring. *Id.* at 161.

New York Telephone Co. demonstrates that the Papaya order is on solid footing. The Court approved the NYTC order on four grounds: (1) the order required minimal effort and provided for the company's reimbursement; (2) the order did not require the company to do anything outside of its standard operations; (3) the company was not far removed from the government's investigation; and (4) the company's assistance was necessary to the investigation. *Id.* at 174–75. The Papaya order meets all four criteria.

1. The government will reimburse Papaya for the minimal effort needed to comply.

The Court concluded the NYTC order was not "in any way burdensome" because it "provided that the Company be fully reimbursed at prevailing rates, and compliance with it required minimal effort on the part of the Company and no disruption to its operations." *Id.* at 175.

The Papaya order is no different. First, it directs the government to reimburse Papaya. J.A. 23. Second, complying with the order would take next to no effort on Papaya's part. To comply, Papaya need only assign three of its 650 employees to less than a week of work. J.A. 35. Surely this constitutes a minimal effort. *Cf. Mich.*

Bell Tel. Co., 565 F.2d at 387 (requiring twenty days of assistance). Third, Papaya has never indicated that compliance with this order would disrupt its day-to-day operations.

Future costs do not enter the equation. *New York Telephone Co.* considered only the resources spent to comply with the order at hand. 434 U.S. at 175. The Court never considered all the costs that might result after compliance had been achieved. *See id.* *New York Telephone Co.* thus precludes Papaya's arguments about its business model. *See Application of United States for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities*, 616 F.2d 1122, 1132 (9th Cir. 1980) (reading *New York Telephone Co.* to foreclose phone company's argument that order would increase risk of system failure and impair "the company's ability to correct such problems"). It also precludes Papaya's argument that it may be subject to similar orders in the future. *See Ivey v. Haney*, No. 92 C 6875, 1994 WL 401098, at *4 (N.D. Ill. July 29, 1994) (reading *New York Telephone Co.* to foreclose "floodgates argument" that compliance with a single order would lead to a "wave of requests for similar [orders]").

2. Papaya develops software as part of its everyday business.

New York Telephone Co. noted that the company regularly installed and used pen registers. 434 U.S. at 174–75. The NYTC order, the Court reasoned, was thus in no way "offensive" to the

company. *Id.* at 174. Likewise, Papaya constantly develops new software to "keep[] pace with evolving technology." J.A. 32. Building software is so routine at Papaya that it has created a director position devoted to improving its code, J.A. 30, developed a sizable team of programmers, J.A. 32, and implemented a quality assurance process solely for new software, J.A. 30.

The Ames Circuit relied on *In re Apple, Inc.* to reach a contrary conclusion. *See* J.A. 6–7 (citing *In re Apple, Inc.*, 149 F. Supp. 3d 341, 369 (E.D.N.Y. 2016)). In *Apple*, the district court declined to grant an order under the AWA compelling Apple to unlock one of its user's phones. 149 F. Supp. 3d at 375. The *Apple* court reasoned that the order would be "offensive" to Apple's business practices. *Id.* at 369. In doing so, the *Apple* court misinterpreted the word "offensive" as *New York Telephone Co.* used it. The *Apple* court yanked the word from its context to conclude that the government cannot compel a private party to do anything that it finds disagreeable. *Id.* at 372. But *New York Telephone Co.* did not use the word "offensive" to mean "disagreeable." It used the word to mean "out of the ordinary." The Court reasoned that pen registers were not offensive because the company "regularly employ[ed] such devices." *N.Y. Tel. Co.*, 44 U.S. at 174–75.

True, the *Apple* court also ruled that the order was "offensive" because it required Apple to do something outside the regular conduct

of its business. 149 F. Supp. 3d at 369. But the court framed that regular conduct at the wrong level of generality. Instead of asking whether Apple regularly designed software, the court asked whether Apple regularly "bypass[ed] a security measure that Apple affirmatively market[ed] to its customers." *Id.* The question is not that specific. *New York Telephone Co.* considered whether the company "regularly employ[ed]" pen registers, not whether the company regularly installed pen registers without its customers' knowledge to assist in the investigation of gambling rings. *N.Y. Tel. Co.*, 434 U.S. at 174–75. Similarly, the appropriate question here is not whether Papaya regularly builds software to disaggregate its user records. The question is whether Papaya regularly develops software related to its user records at all. And the answer is yes.

3. Papaya is close enough to Doe to support its involvement in this case.

The SCA puts Papaya close to this case. Congress enacted the SCA specifically to permit the government to access records held by a "provider of electronic communication service." 18 U.S.C. § 2703(c). Papaya has stipulated that it fits that description. J.A. 35. It is therefore not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." *N.Y. Tel. Co.*, 434 U.S. at 174. Additionally, by aggregating its users' data, Papaya

strategically placed itself between the government and the information it needs.

Moreover, in the context of terrorism, the closeness inquiry casts a wider net. For example, Congress imposes criminal penalties on organizations that provide even "benign" support to terrorists. *See Holder v. Humanitarian Law Project*, 561 U.S. 1, 36 (2010). If that sort of attenuated support for a terrorist group is sufficient to hold a corporation criminally liable, surely Papaya's ongoing relationship with Doe is enough to compel its assistance in investigating him.

4. Papaya's assistance is necessary.

New York Telephone Co. gave considerable weight to the government's need for assistance. It explained that by refusing to comply, the company had "threatened obstruction of an investigation." *N.Y. Tel. Co.*, 434 U.S. at 174. Papaya's noncompliance threatens to do the same thing here. The government cannot investigate Doe further unless Papaya disaggregates his location data. Thus, just as the New York Telephone Company's assistance "was essential" to busting the gambling ring, *id.* at 175, Papaya's assistance is essential to preventing a fourth attack.

D. This case raises no grave First Amendment doubts.

In reaching its decision on the meaning of the phrase "undue burden," the Ames Circuit invoked the canon of constitutional

avoidance: "The First Amendment concerns raised by the Order fortify our conclusion that Papaya would be subject to an undue burden." J.A. 7. But this case raises no "grave and doubtful" First Amendment questions, *Rust v. Sullivan*, 500 U.S. 173, 191 (1991), because this order does not compel Papaya to speak.

This Court need not decide whether computer code is speech. The government takes no position on that question, which has long confounded courts. *See, e.g.*, *Def. Distributed v. U.S. Dep't of State*, No. 15-50759, 2016 WL 5383110 (5th Cir. Sept. 20, 2016); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001). Instead, this Court can give a narrower answer to an easier question: this order does not compel speech because it does not compel any particular code.

The order focuses on function, not message. Orders aimed at "result[s]," not "content," pose no First Amendment concerns. *Rumsfeld v. Forum for Acad. & Institutional Rights, Inc.* (*FAIR*), 547 U.S. 47, 57 (2006). Ordering Papaya to disaggregate Doe's data is like ordering a locksmith to make a key: the end result must achieve a particular function, not communicate any particular message. The code is simply a key to unlock Doe's location data.

FAIR forecloses Papaya's First Amendment claim. There, a statute required law schools to give military recruiters equal access to career services, which meant "sending e-mails and distributing flyers"

on behalf of the military. *Id.* at 60. This Court upheld the requirement because it affected "what law schools must *do* — afford equal access to military recruiters — not what they may or may not *say*." *Id.* The same reasoning applies here: the order affects what Papaya must *do* — disaggregate Doe's location information — not what specific code Papaya must *use* to achieve that result. J.A. 23. As Papaya's own engineers averred, each one codes "in her own unique way." J.A. 32. Two Papaya engineers complying with the order would come up with entirely different programs. The order asks for a specific result, not a specific code.

Even if this order did compel speech, it would still be narrowly tailored to a compelling state interest. *See Williams-Yulee v. Fla. Bar*, 135 S. Ct. 1656, 1665–66 (2015). Papaya has stipulated that it "has the exclusive technological means" to unlock Doe's location information, J.A. 35, and the government seeks this information to prevent an imminent terrorist attack. "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig*, 453 U.S. at 307 (quoting *Aptheker v. Sec'y of State*, 378 U.S. 500, 509 (1964)).

This Court should therefore hold that the order does not impose an "undue burden" under the SCA.

II. The Fourth Amendment allows the government to acquire Papaya's records of Doe's location.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches." U.S. Const. amend. IV. This Court has repeatedly emphasized that the government does not violate the Fourth Amendment if:

(1) the government does not conduct a search; *or*

(2) the government conducts a reasonable search.

See, e.g., *Maryland v. King*, 133 S. Ct. 1958, 1968–69 (2013). Obtaining Papaya's records of Doe's location is not a search, and even if it were, obtaining that data would be reasonable. Papaya's constitutional claim therefore fails.

First, Doe voluntarily disclosed his location information to Papaya. Under the third-party doctrine, Doe lost any expectation of privacy in that information, so the government would not conduct a search by collecting it. *See Smith v. Maryland*, 442 U.S. 735, 745–46 (1979); *United States v. Miller*, 425 U.S. 435, 442 (1976). Second, even if retrieving Papaya's records constituted a search, that search would be reasonable. Obtaining that data poses a minimal intrusion to Doe's already-diminished expectation of privacy, and the SCA's framework provides adequate protection for Doe. Given the likelihood of another

devastating attack, the Fourth Amendment balance tilts decidedly in the government's favor.

A. Obtaining location data from a third party is not a search.

A Fourth Amendment search "occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). But when an individual "voluntarily turns over" information to a third party, he loses any "legitimate expectation of privacy" in it. *Smith*, 442 U.S. at 743–44. The government may thus obtain an individual's information from a third party without conducting a Fourth Amendment search. *Id.* at 745–46 (allowing government to collect phone records); *see also Miller*, 425 U.S. 435 (bank records); *California v. Greenwood*, 486 U.S. 35 (1988) (curbside garbage).

The third-party doctrine resolves this case: Papaya's subscribers, by voluntarily disclosing their location data to Papaya, give up any legitimate expectation of privacy in it. By holding that the third-party doctrine bars Papaya's Fourth Amendment claim, the Court also assures that the use of technology does not arbitrarily expand Fourth Amendment protection, preserves privacy expectations in the contents of communications, and strikes a sensible balance between privacy and security.

1. The third-party doctrine defeats Papaya's Fourth Amendment claim.

Smith v. Maryland controls this case. In *Smith*, the police asked a phone company to install a pen register to track the phone numbers dialed by a robbery suspect. 442 U.S. at 737. The police then collected the suspect's phone records from the company. *Id.* Applying the third-party doctrine, the Court held that the government did not conduct a Fourth Amendment search. *Id.* at 746. The Court reasoned that, by dialing the phone numbers, the suspect had "exposed" information to the company's "equipment" in the company's "ordinary course of business." *Id.* at 744. In doing so, he "voluntarily conveyed" that information to the phone company and lost any expectation of privacy in it. *Id.*

Smith's reasoning maps onto the facts of this case. Just as a landline user conveys the numbers dialed to the telephone company's switching equipment, *id.* at 744, a Papaya subscriber conveys location information to Papaya's nearest cell tower, J.A. 33. If the switching equipment in *Smith* was "merely the modern counterpart of the operator," 442 U.S. at 744, cell towers are the modern counterpart of switching equipment; both automatically collect information from their users. And like the landline users who knew they exposed the numbers they dialed to the company, *see id.* at 742, cell users are constantly reminded that they expose their location information to

providers whenever they experience dropped calls and "no service" indicators. Papaya customers are especially aware that they convey their location information to the company. They are told precisely that in the company's privacy policy: "Your wireless device generates information about your location whenever you use it over our network, and we need to gather that information to improve our coverage and provide you with the best service possible." J.A. 28.

In addition, both landline providers and Papaya keep permanent records of the information disclosed to them for routine business reasons, such as detecting fraud. *Compare Smith*, 442. U.S. at 742, *with* J.A. 28. The government seeks only Papaya's records of the location information that Doe voluntarily disclosed, activity that falls comfortably within *Smith*'s ambit. Most courts of appeals to have considered the issue have confirmed that *Smith*'s reasoning extends to location information. *See, e.g.*, *United States v. Graham*, 824 F.3d 421, 427 (4th Cir. 2016) (en banc) ("The Supreme Court's reasoning in *Smith* controls."); *United States v. Carpenter*, 819 F.3d 880, 888 (6th Cir. 2016) ("On this point, *Smith* is binding precedent.").

The factual distinctions between *Smith* and this case make no difference for the third-party doctrine. The Ames Circuit nevertheless held that subscribers "do not 'voluntarily' share their location information." J.A. 9. That conclusion rested on two faulty arguments:

first, that Papaya's subscribers do not know the "particular information" they convey; and second, that Papaya's subscribers are not "actively choosing" to disclose that information. *Id.* Neither contention can dislodge this case from *Smith*'s grip.

a. Papaya's users know that Papaya collects their information.

The Ames Circuit emphasized that subscribers may not know "the particular information they are conveying — that is, which cell [towers] their activity is routed through." *Id.* But *Smith* never required the suspect to have such exacting knowledge. The suspect did not need to know *how* the company tracked his information or *which calls* the company chose to record. That is why the Court was unmoved by the suspect's argument that because only long-distance calls appeared on his monthly bill, he did not know the phone company recorded local calls. *Smith*, 442 U.S. at 745. Instead, all that mattered was that the suspect knew that every time he made a call, he was conveying a phone number to the company. *Id.* at 742. Similarly, all Doe must know is that, by using his phone, he is conveying location information to Papaya. He need not know which cell towers Papaya uses to receive that information. He need not even know that Papaya uses cell towers at all.

Rather than impose some strict knowledge threshold, the voluntariness requirement serves to exclude those cases where the

government "conducts surreptitious surveillance" or where a third party "steals private information." *Graham*, 824 F.3d at 431. That is why, for instance, the government's conduct in *United States v. Jones* — a trespass case involving direct surveillance — constituted a search. 132 S. Ct. 945, 949 (2012).

That is not this case. The government did not conduct surreptitious surveillance or compel Papaya to collect location information. And Papaya did not "steal" location information from its subscribers. In fact, Papaya told subscribers that they would disclose their location information to Papaya, that Papaya would record it, and that Papaya might turn over that information to law enforcement. *See* J.A. 27–29; *cf. In re Application of United States for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013) (emphasizing that cell providers inform customers that they collect and use location information).

Papaya's pledge to aggregate user data after collecting it does not alter the analysis. All that matters for purposes of the third-party doctrine is that individuals voluntarily convey information, not what the third party "elects" to do with the data after it is conveyed to them. *See Smith*, 442 U.S. at 745. *Smith* recognized that a rule allowing strategic business decisions to dictate the scope of the third-party doctrine would make a "crazy quilt of the Fourth Amendment." *Id.*

Hence, the third-party doctrine applies even where, as here, "information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Miller*, 425 U.S. at 443. What matters, therefore, is that Papaya's subscribers know they convey location information to Papaya.

Papaya's promise to conceal user information finds its closest analogue in Internet networks that vow to hide IP addresses. *See, e.g.*, *United States v. Broy*, No. 16-CR-10030, 2016 WL 5172853 (C.D. Ill. Sept. 21, 2016). These networks allow an individual to conceal his IP address by sending it through various other computers — a process that "cloaks and scrambles a user's actual IP address." *Id.* at *5. But an individual who uses these networks — even to "gain [the] feeling of anonymity" — maintains no reasonable expectation of privacy in his IP address because he "voluntarily disclosed" it to the first computer (and its operator). *Id.* The same is true of Papaya's subscribers: while they may have sought Papaya's services for secrecy, they gain the feeling of secrecy only if they disclose their information to Papaya in the first place. The Court should not permit those subscribers to use Papaya's services as a "shield to conceal" their identity and a "sword to claim a reasonable expectation of privacy." *Id.*

b. Papaya users convey their location information to Papaya.

The Ames Circuit next concluded that the third-party doctrine applies only when an individual "actively choos[es] to convey" specific information. J.A. 9. This theory suggests that *Smith* is inapposite because landline users actively convey phone numbers by dialing them, whereas cell users do not actively transmit location data when using their phones.

The idea that *Smith* authorized the government to collect only the numbers physically pressed by the phone user has no support. In fact, *Smith* implicitly authorized law enforcement to collect more specific location data than the government can get here — even though landline users did not manually convey location information by dialing a phone number. Because every landline phone number is tied to a "precise address," landline records "necessarily showed exactly where the user was." *United States v. Davis*, 785 F.3d 498, 512 (11th Cir. 2015) (en banc). Papaya's location data, which only approximates a user's location, tells law enforcement even less. *See* J.A. 33.

Federal courts have interpreted *Smith* to allow law enforcement to gather more information than what individuals actively convey. That result flows naturally from *Smith*. The Court did not share Justice Stewart's concern that allowing access to a list of phone numbers dialed could "reveal the identities of the persons and the

places called, and thus reveal the most intimate details" of the caller's life. *Smith*, 442 U.S. at 748 (Stewart, J., dissenting). No wonder, then, that federal courts have applied the third-party doctrine even to information that a person passively *receives*. *See, e.g.*, *United States v. Clenney*, 631 F.3d 658, 666 (4th Cir. 2011) (incoming calls); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007) (incoming email addresses).

Finally, even accepting the Ames Circuit's "active choice" requirement, Papaya subscribers *do* make an active choice to convey their location data. Every subscriber chooses to purchase a phone; chooses a service provider that collects location data; and chooses to carry the phone around with her throughout the day. *See In re Application of United States for Historical Cell Site Data*, 724 F.3d at 614. Once users opt in to the convenience of cell service, they necessarily accept that none of its benefits — including the ability to receive calls — are possible without location disclosure.

2. The Court should retain the third-party doctrine.

Because a "respect for precedent is, by definition, indispensable," the Court should not displace the third-party doctrine without first considering its time-tested virtue. *Planned Parenthood of Se. Pa. v. Casey*, 505 U.S. 833, 854 (1992). And even then, the Court should not disturb settled doctrine unless "necessity and propriety"

demand it. *Patterson v. McLean Credit Union*, 491 U.S. 164, 172 (1989). That high bar is not met here. Quite the contrary: for forty years, the doctrine has provided courts with a manageable Fourth Amendment framework. Undoing that doctrine now would disrupt, not improve, American life. *Cf. Dickerson v. United States*, 530 U.S. 428, 443 (2000) (declining to overrule *Miranda* because its warnings had "become part of our national culture").

On top of these deep historical roots, the doctrine boasts strong normative appeal. It ensures that the use of technology does not arbitrarily expand Fourth Amendment protection; preserves the privacy of the contents of communications; and allows Congress to respond to changing security and privacy concerns.

a. The third-party doctrine keeps the Fourth Amendment technology neutral.

The Court's continued embrace of the third-party doctrine recognizes that technological advances "do not give individuals a Fourth Amendment right to conceal information that otherwise would not have been private." *Graham*, 824 F.3d at 436. The Court has long emphasized this rationale. The suspect in *Smith* admitted that if "he had placed his calls through an operator," he would have had no Fourth Amendment claim; the Court declined to reach a "different constitutional result" simply "because the telephone company ha[d] decided to automate." *Smith*, 442 U.S. at 744–45. The third-party

doctrine thus prevents "savvy criminals" from substituting "a hidden third-party exchange for a previously public act." Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 561 (2009).

Consider the facts of *Smith* without telephones. To harass his victim, Smith "would have been forced to stalk [her] the old-fashioned way." *Id.* at 577. He would have "left his house, walked to his car, and driven to his victim's home to harass her in person" — and the police could have lawfully watched him every step of the way. *Id.* at 577–78. The third-party doctrine provides symmetrical Fourth Amendment treatment in both instances. "Smith's physical presence was not protected in the physical world version of the crime," just as his "virtual presence is not protected in the third-party environment of the telephone network." *Id.* at 578. The third-party doctrine maintains that equilibrium.

b. The third-party doctrine preserves privacy expectations in the contents of communications.

The third-party doctrine does not sweep indiscriminately. The government cannot invoke the doctrine to obtain the *contents* of private communications from a third-party carrier. *Smith*, 442 U.S. at 741; *accord United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). This limitation prevents the government from collecting individuals' most sensitive information — the "private thoughts and speech" included in emails, text messages, photos, videos, and other means of

electronic communication. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan L. Rev. 1005, 1018 (2010).

Instead, the third-party doctrine applies only to *non-content* information that an individual voluntarily discloses. Non-content information includes things like identity, location, and time — the types of information the government has always been able to access. *Smith*, 442 U.S. at 745–46 (telephone records); *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (exterior of letters and packages). As with phone numbers and letter addresses, location information "facilitate[s] personal communications" but is not "part of the content of those communications themselves." *Carpenter*, 819 F.3d at 887. The distinction between content and non-content preserves an appropriate level of privacy.

c. The third-party doctrine allows Congress to respond to changing privacy and security concerns.

Even if changes to the third-party doctrine were desirable, that decision is best left to the legislature. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring). Congress has proven that it can limit the third-party doctrine's reach: one year after *Miller* authorized law enforcement to inspect bank records, Congress passed the Right to

Financial Privacy Act "in direct response to" *Miller*. *State v. Schultz*, 850 P.2d 818, 831 (Kan. 1993).

Congress acted similarly when it passed the Stored Communications Act to provide numerous privacy-enhancing safeguards in the electronic data context. The Court's intervention now would "scuttle the laborious efforts of the Congress [in the SCA] to balance privacy and law enforcement interests." *Graham*, 824 F.3d at 439 (Wilkinson, J., concurring). It would also keep Congress from undertaking similar efforts in the future. The Court should therefore reject Papaya's attempt to wield a "constitutional club that ends the conversation and severely limits opportunities for legislative reforms and responses in what is a rapidly evolving field." *Id.* at 439 n.*. If the modern implications of the third-party doctrine are unpalatable to the American people, Congress can respond accordingly — just as it did when public outcry compelled it to curtail the NSA's metadata collection program. *See* U.S.A. Freedom Act, Pub. L. No. 114-23 (2015). The Court should facilitate that national conversation, not end it.

B. Even if there were a search, the SCA order is a reasonable response to an imminent threat.

In the past year, twenty-seven people have been killed and dozens more injured in three acts of terrorism. After each strike, Redemption has promised — and delivered — more to come. The FBI's

pursuit of the suspected bomber is a reasonable and necessary measure to prevent Redemption's next attack.

1. The Fourth Amendment permits the government to conduct a reasonable warrantless search.

"The touchstone of the Fourth Amendment is reasonableness." *United States v. Knights*, 534 U.S. 112, 118 (2001). Although the reasonableness requirement is typically satisfied by a showing of probable cause, this Court has repeatedly held that "a lesser degree [of probability] satisfies the Constitution when the balance of governmental and private interests makes such a standard reasonable." *Id.* at 121. In conducting that balance, the Court looks to the totality of the circumstances and weighs "the degree to which [the search] intrudes upon an individual's privacy" against "the promotion of legitimate governmental interests." *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999).

The government's paramount interest in preventing an imminent deadly attack dwarf Doe's expectation that his approximate whereabouts remain hidden. Indeed, any "search" in this case — conducted pursuant to a court order — would be far less intrusive than other warrantless searches this Court has upheld, even absent an imminent threat to public safety. And Congress's independent constitutional judgment reflected in the SCA should not lightly be cast aside.

2. Doe's privacy interests pale in comparison to the government's interest in preventing terrorism.

The order does not authorize the sort of intrusive search that has traditionally aroused this Court's suspicion. First, Doe has, at most, a diminished expectation of privacy in his location information. Second, the government is not "seizing" any of Doe's property or otherwise interfering with any possessory interest. *Cf.* Note, *Digital Duplications and the Fourth Amendment*, 129 Harv. L. Rev. 1046 (2016) (concluding that data duplication is properly analyzed as a potential search, rather than a seizure). Third, accessing location data does not involve any physical intrusion on the person of the suspect. *Cf. Birchfield v. North Dakota*, 136 S. Ct. 2160, 2184 (2016) (blood-alcohol tests are "significantly more intrusive" because they invade the body); *Safford Unified Sch. Dist. #1 v. Redding*, 557 U.S. 364, 375 (2009) (intrusive bodily searches, such as strip searches, require greater justification). Fourth, the search does not reach an area traditionally associated with increased privacy concerns, such as the home. *See Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) ("[W]hen it comes to the Fourth Amendment, the home is first among equals."). And fifth, the SCA "incorporates additional privacy protections that keep any intrusion minimal." *Davis*, 785 F.3d at 517.

Besides, an individual's whereabouts have never been viewed as particularly personal information. Whenever a person leaves his house, everyone in the immediate area knows his location. *See United States v. Knotts*, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). The use of technology to ascertain a person's location does not change the analysis. *Id.* at 282 ("Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.").

In fact, the location information gathered in this case is even less extensive than the information gathered in *Knotts*. Here, the location data the government seeks would reveal only Doe's *approximate* location, with the degree of specificity varying based on the cell tower's coverage area. J.A. 33. Unlike exacting GPS data, it would not reveal "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring). Nor could it be used to reconstruct "[t]he sum of an individual's private life." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). And the government's use of Doe's location data

would serve only the limited purpose of approximating Doe's whereabouts over the course of the three prior attacks. *Cf. King*, 133 S. Ct. at 1967 (limited use of DNA for identification purpose contributes to its reasonableness).

By contrast, the order is backed by the highest of government interests: protecting Ames from an imminent terrorist attack. *See Haig,* 453 U.S. at 307. This is not merely a generalized interest in solving crime or accumulating evidence to prosecute a particular defendant. Rather, the government is pursuing a suspected bomber in an effort *to prevent* a threatened massacre of children. The government has presented specific and articulable facts, supported by a credible source with non-public information about the prior attacks, that Doe is an active member of Redemption. J.A. 17. It is hard to imagine a greater need for an SCA order than the one in this case.

The upshot is that whatever expectation of privacy Doe claims in his approximate location pales in comparison to the government's interest in preventing a fourth attack. Under the circumstances, the government's application for the SCA order was reasonable.

3. Collecting location data is the digital equivalent of a Terry *stop.*

This Court has long held that a police officer may stop a suspect on the street based on reasonable suspicion. *Terry v. Ohio*, 392 U.S. 1 (1968). And, once the suspect is stopped, an officer's reasonable belief

that the suspect poses a danger to people in the surrounding area justifies a preventive search for weapons. *Id.* at 27.

The order in this case is the digital analogue of a *Terry* stop. The SCA first requires reasonable suspicion that the target of the search is relevant to a criminal investigation. *Compare* 18 U.S.C. § 2703(d) (requiring "specific and articulable facts" tying target of search to "an ongoing criminal investigation"), *with Terry*, 392 U.S. at 21 (requiring "specific and articulable facts" warranting the stop). As in *Terry*, the government's interest in searching Doe is based on the immediate danger he poses. *Compare* J.A. 16 (government faced with credible threat of a fourth attack), *with Terry*, 392 U.S. at 26 (officer faced with a "reasonable apprehension of danger"). And, as in *Terry*, the scope of the search is carefully limited to avoid intruding on the suspect's privacy beyond what is necessary. *Compare* 18 U.S.C. § 2703 (constructing a detailed statutory framework to limit the type of information the government may obtain), *with Terry*, 392 U.S. at 29 (confining the scope of the search to "an intrusion reasonably designed to discover" weapons).

This Court's subsequent interpretations of *Terry* further support the order here. In *Hayes v. Florida*, the Court explained that "seizures for the purpose of fingerprinting" were within the permissible scope of a *Terry* stop where the government reasonably suspected that

fingerprint identification would "establish or negate the suspect's connection with [a] crime." 470 U.S. 811, 817 (1985); *see also Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty.*, 542 U.S. 177, 188 (2004) (reaffirming that proposition). The government has an identical purpose here: obtaining Doe's location data could "reveal pertinent information" about Doe's "involvement in the deadly attacks." J.A. 17. Indeed, the government's interest here is even stronger than the interest put forward in *Terry* and *Hayes*: not merely arrest and prosecution for past crimes, but also prevention of a threatened future terrorist attack. The *Terry* stop thus finds a modern counterpart in the order here.

4. The Court has long upheld more intrusive warrantless searches, even without an imminent threat to public safety.

In *United States v. Knights*, the Court held that reasonable suspicion is sufficient to justify searching a probationer's home. 534 U.S. at 121. There, a police detective searched Knights's home based on reasonable suspicion that Knights had engaged in vandalism. *Id.* at 114–15. The search here, also based on reasonable suspicion, does not concern Doe's home or any of his physical property. And Doe is far more than a vandal — he is the FBI's prime suspect in a string of terrorist attacks whose casualties reach triple digits. If it was

reasonable to search the home of a suspected vandal, it must surely be reasonable to obtain location data for a suspected terrorist.

Nor is the Court's approval of warrantless searches limited to individuals, like probationers, with a particular legal status. In *Vernonia School District 47J v. Acton*, 515 U.S. 646 (1995), this Court approved the programmatic random drug testing of high school student-athletes. The Court's conclusion rested on the "sharp increase in drug use" and development of a "drug culture" that the school district had to address. *See id.* at 650. This drug problem, the Court held, justified random urine tests in which a "monitor" would observe while the high school student urinated into a plastic cup. *Id.* at 651.

Ames faces a far greater threat. A terrorist group is systematically striking Ames's citizens, with no sign of stopping. In response, the FBI has sought information about Doe — not randomly, as in *Vernonia*, but based on reasonable suspicion that Doe is the bomber. The order does not authorize a programmatic search of every *possible* perpetrator; it is, rather, limited to the prime suspect in a yearlong investigation. And it does not involve anything nearly so invasive as compelled urination under the watch of a government "monitor." If a local drug problem justifies the suspicionless targeting of high school students for an invasive and embarrassing search, then

a series of bombings with the threat of another justifies the limited disclosure of location data for the lead suspect in the investigation.

5. The SCA adequately safeguards privacy interests.

The SCA "creates a set of Fourth Amendment–like privacy protections." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1212 (2004); *see also Davis*, 785 F.3d at 517; *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1179 (9th Cir. 2013). The SCA lays out specifically what information the government can obtain and what procedures the government must follow. 18 U.S.C. § 2703. A neutral arbiter stands between the government and the information sought. *Id.* § 2703(d). The government can obtain location data, but it cannot obtain the contents of electronic communications without a warrant. *Id.* § 2703(a), (c). It cannot obtain information that is "unusually voluminous in nature." *Id.* § 2703(d). It cannot subject service providers to an undue burden in obtaining the information. *Id.* It cannot obtain anything at all without demonstrating "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* And even after the government has obtained the information it seeks, "[t]he SCA guards against the

improper . . . use of any personal information theoretically discoverable from such records." *Davis*, 785 F.3d at 517.

The Court should accord a measure of deference to Congress's considered judgment that the SCA's detailed framework strikes an appropriate Fourth Amendment balance. Even apart from Congress's coequal status as a separate branch, two factors counsel in favor of deference. First, in areas of new technology, Congress should lead the way. Doctrine and history "teach that courts should place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new technologies." Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805 (2004); *see also Riley*, 134 S. Ct. at 2497–98 (Alito, J., concurring in part and concurring in the judgment) (arguing that legislatures should lead the way in crafting sensible privacy protections for new technologies). Second, the political branches' "informed judgment" deserves special deference when fact-sensitive decisions about counterterrorism policy are at stake. *Cf. Holder*, 561 U.S. at 34–35 (noting, in First Amendment context, that Congress's assessment of the effects of its counterterrorism policy is entitled to deference). Congress did not act unconstitutionally when it passed the SCA.

This Court should therefore hold that the Fourth Amendment allows the government to obtain Doe's location records.

CONCLUSION

It has been a year since Redemption first struck. Ever since, the people of Ames have languished in fear while those responsible plan further attacks. Now, the government has a chance to bring the killing to an end. The SCA requires Papaya to provide Doe's location data, and Papaya cannot reforge the Fourth Amendment to evade that command.

The judgment of the court of appeals should be reversed.

October 7, 2016

Respectfully submitted,

The Daniel J. Meltzer Memorial Team

Luke Beasley

Benjamin Burkett

William Ferraro

Amanda Mundell

Trenton Van Oss

Connor Winn

APPENDIX

United States Constitution

U.S. Const. amend. IV.

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Stored Communications Act, 18 U.S.C. § 2703 *et. seq.* (2012)

(selected provisions)

§ 2703 - Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.—
A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.—

> **(1)** A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
>
> > **(A)** without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or
> >
> > **(B)** with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
> >
> > > **(i)** uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena;
> > > or
> > >
> > > **(ii)** obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.—

(1) 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—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.—
A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue

burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.—
No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.—

> **(1) In general.—**
> A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
>
> **(2) Period of retention.—**
> Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.—
Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

* * *

§ 2706 - Cost Reimbursement

(a) Payment. —
Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount. —
The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception.—
The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

All Writs Act 28 U.S.C. § 1651 (2012)

§ 1651 - Writs

(a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

(b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.

Selected Provisions from 42 U.S.C. § 9607 (2012)

§ 9607(k)(6)(C)(ii) - Liability

(k) Transfer to, and assumption by, Post-Closure Liability Fund of liability of owner or operator of hazardous waste disposal facility in receipt of permit under applicable solid waste disposal law; time, criteria applicable, procedures, etc.; monitoring costs; reports

. . . .

(6) Study of options for post-closure program

. . . .

(C) Assessments.—The study under this paragraph shall include assessments of treatment, storage, and disposal facilities which have been or are likely to be issued a permit under section 3005 of the Solid Waste Disposal Act [42 U.S.C.A. § 6925] and the likelihood of future insolvency on the part of owners and operators of such facilities. Separate assessments shall be made for different classes of facilities and for different classes of land disposal facilities and shall include but not be limited to—

(i) the current and future financial capabilities of facility owners and operators;

(ii) the current and future costs associated with facilities, including the costs of routine monitoring and maintenance, compliance monitoring, corrective action, natural resource damages, and liability for damages to third parties; and

(iii) the availability of mechanisms by which owners and operators of such facilities can assure that current and future costs, including post-closure costs, will be financed.

Federal Rules of Civil Procedure

Rule 26. Duty to Disclose; General Provisions Governing Discovery

. . . .

(b) Discovery Scope and Limits.

(1) ***Scope in General***. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

(2) ***Limitations on Frequency and Extent.***

(A) *When Permitted.* By order, the court may alter the limits in these rules on the number of depositions and interrogatories or on the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.

(B) *Specific Limitations on Electronically Stored Information.* A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Rule 45. Subpoena

. . . .

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction--which may include lost earnings and reasonable attorney's fees--on a party or attorney who fails to comply.