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 RESPONDENT

The Lucy Stone Memorial Team

MICHELLE G. ADLER
VICTORIA L. HARTMANN
HELEN M. RAVE
CAROLINE M. TRUSTY
STEFANIE A. TUBBS
MENGJIE ZOU

Counsel for Respondent

November 1, 2016, 11:45 a.m.
Ames Courtroom
Harvard Law School

Oral Argument

QUESTIONS PRESENTED

1. The Stored Communications Act allows a court to quash an order requiring a cell service provider, a non-party, to disclose a user's location information to the government when compliance with such order would cause the provider an "undue burden." Under an abuse of discretion standard, was it reasonable on balance for a court to find an undue burden where the requested information is of questionable necessity and compliance would cause the provider severe reputational harm?

2. The Fourth Amendment protects "persons" from unreasonable searches. An unreasonable search occurs when the government intrudes on an individual's "person" by engaging in extensive surveillance of that individual's public and private movements without a warrant. Would disclosure of six months of an individual's location information, without a warrant, violate the Fourth Amendment?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Constitutional Provisions

OPINIONS BELOW

The opinion of the U.S. Court of Appeals for the Ames Circuit is reproduced at page 2 of the Joint Appendix. The order of the U.S. 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.

STATEMENT OF JURISDICTION

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

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

All relevant provisions are reproduced in the Appendix to this brief.

STATEMENT OF THE CASE

The "most intimate details of an individual's life" are captured by his cell phone. J.A. 25. Among those details is an individual's location. J.A. 25. The modern cell phone tracks its user's location every time it connects to a cell tower, J.A. 27, and on average generates 100 connections per day, J.A. 33. When the tower and the phone connect, that connection generates cell site location information ("location information"). J.A. 33. Whenever a user makes or receives a call, or uses any application that requires use of cellular data, his location information is created. J.A. 33.

Location information is specific: depending on how many cell sites are in an area, location information can pinpoint a user's position down to a specific city block. J.A. 33. Added up, location information has the potential to "track movements, habits, or personal lives" of cell phone users. J.A. 25.

With this twenty-first-century reality in mind, Eric Thornton founded Papaya Cellular, Inc. ("Papaya"), a cell service provider where "privacy comes first." J.A. 27. Papaya stands alone in the industry in its commitment to privacy. J.A. 25. It has invested in infrastructure, advertising, and company policies to build on its bedrock principle: cell phone users should not have to sacrifice their privacy just to own a cell phone. J.A. 25.

Papaya's motto, "Your Privacy Comes First," is not just lip service; unlike other cell service providers, Papaya has built proprietary encryption software to strip the location information it collects of any identifying information. J.A. 5. Papaya only collects anonymized location information from its users and then aggregates the information to protect its users' privacy. J.A. 27.

This security feature is impossible to reverse without coding entirely new software. J.A. 30. A programmer would have to write the code. J.A. 32. Such writing is a "creative" and "expressive" process, and each programmer "approaches the task of writing code in her own unique way." J.A. 32. The programmer would have to choose the language, how to manipulate the data, what code vocabulary to use, and how to construct a user interface. J.A. 32. After all of that, in the name of its business model, Papaya would have to try to destroy the software. J.A. 31. But Papaya might not be able to destroy it; it is "difficult to irretrievably destroy something in the digital world." J.A. 31. To disaggregate an individual subscriber's location information in the future, Papaya would have to repeat this process. J.A. 31.

But Papaya has never disaggregated an individual user's location information. J.A. 30. Papaya built its brand on its commitment to privacy, and pledges to its users that not only does it not collect their individualized information, but also that it will never

share that information with third parties, unless required by law. J.A. 29. Papaya has never broken that pledge. J.A. 30.

Recently, Ames suffered three attacks. J.A. 3. A group calling itself "Redemption" claimed responsibility. J.A. 3–4. In all, the attacks killed 27 people and injured dozens more. J.A. 3. After the third attack, an anonymous caller phoned an FBI tip line claiming that a man, "John Doe," had been involved in one or more of the attacks. J.A. 17. The anonymous caller had information that investigators believed indicated he had "inside knowledge" of the attacks. J.A. 4. The anonymous caller said that Redemption was planning additional attacks. J.A. 3.

In response to this anonymous call, the government decided to investigate Doe. It filed an ex parte application under the Stored Communications Act (SCA) to compel Papaya to provide six months of Doe's location information. J.A. 14. The government hoped to "identify all of the individuals responsible for the terrorist attacks . . . and prevent future acts of violence." J.A. 17. The District Court issued the order compelling Papaya to disclose the information ("Order"), but Papaya immediately moved to quash because the Order posed an undue burden under 18 U.S.C. § 2703(d) and also violated the Fourth Amendment by permitting the government to conduct an unreasonable, warrantless search. J.A. 24. The District Court granted

Papaya's motion to quash for both of these reasons, J.A. 36, and the Ames Circuit affirmed, J.A. 3. The government petitioned for a writ of certiorari, which this Court granted. J.A. 1.

SUMMARY OF ARGUMENT

I. The SCA allows the government to request information from electronic communications providers, but limits those requests to ones that do not cause an "undue burden" on the provider. *See* 18 U.S.C. § 2703(d) (2012). The Ames District Court found such an undue burden and granted Papaya's motion to quash. J.A. 36. The Circuit Court affirmed. Because such orders are within the discretion of district courts, this Court should defer to the lower court's determination of undue burden. *See Highmark Inc. v. Allcare Health Mgmt. Sys., Inc.*, 134 S. Ct. 1744, 1748 (2014).

Furthermore, the District Court's finding of undue burden is reasonable. Since "undue burden" is not defined in the SCA, this Court should consider common law jurisprudence in analogous contexts, such as the All Writs Act (AWA), 28 U.S.C. § 1651 (2012), and discovery motions, to interpret the phrase. In considering these contexts, determining the appropriateness of a § 2703(d) order invites a balancing of the government's interest against Papaya's burden. *See, e.g.*, *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 149 F. Supp. 3d 341, 369–71 (E.D.N.Y. 2016) [hereinafter *In re Apple*].

The government overstates the known correlation between its interest and the information it seeks. *See* Pet'r's Br. 9 (stating that the Order is "necessary to help stop another terrorist attack"). Allowing the government to use national security as a trump card would disregard the considerations

that weigh against its request. First, the information it seeks is based solely on information from an anonymous caller. Second, the government has requested six months' worth of location information on Doe, which will likely yield much information not directly relevant to the investigation of the attacks. Finally, there are other methods by which the government could approximate Doe's whereabouts during the attacks. These considerations together indicate that, although the government has a strong interest in preventing future attacks, its desperation to find a potential lead in its investigation does not mitigate the deficiencies in its request.

To properly complete the balancing of undue burden under § 2703(d), the Court must consider Papaya's burdens. *See In re Apple*, 149 F. Supp. 3d at 369. First, the future effects of the Order — hacking threats and subsequent similar government requests — impose a heavy burden on Papaya. Second, compliance with the Order would cause Papaya severe reputational harm by communicating to its customers that Papaya does not prioritize their privacy. Third, writing decryption code is not within Papaya's ordinary course of business. Fourth, Papaya, as a non-party to the government's investigation, deserves additional protection from unwarranted impositions. Finally, the First Amendment is implicated because this Order would compel speech from Papaya.

Given the balance of the diminished government interests against the heavy burden imposed on Papaya, as well as the fact that cost-shifting does

not preclude a finding of undue burden, the District Court reasonably found that the Order would cause an undue burden. Therefore, this Court should affirm that finding. Nevertheless, if this Court finds that alternative considerations factor into the undue burden calculus, then this Court should remand to the Ames District Court.

II. The government seeks six months of Doe's comprehensive location information. The Fourth Amendment prohibits this without a warrant.

This Court should apply constitutional avoidance to interpret the SCA to require a warrant for location information. *See Jones v. United States*, 529 U.S. 848, 857 (2000). Section 2703(c) is ambiguous as to when the government must obtain a warrant or merely a court order. 18 U.S.C. § 2703(c)(1). Only one plausible interpretation of § 2703(c) — requiring a warrant for location information — avoids serious constitutional doubt in resolving this ambiguity. Interpreting § 2703(c) to require a warrant is not contrary to Congress's intent and comports with the structure of § 2703. Accordingly, the Court should apply constitutional avoidance to require a warrant for location information.

Even if the Court declines to employ this canon, the government's request constitutes an unreasonable search. In the past, to determine whether there was a search, courts have analyzed whether the government violates an individual's "reasonable expectation of privacy." *Kyllo v. United States*, 553 U.S. 27, 33 (2001). This Court should not apply the reasonable

expectation test for three reasons. First, it causes arbitrary results. *See, e.g.*, *Kyllo*, 533 U.S at 34. Second, it supports the expectations of the majority rather than individuals. *See Smith v. Maryland*, 442 U.S. 735, 743 (1979). Third, the test erodes Fourth Amendment protections. *See id.* at 752 n.5.

This Court should instead find a search when the government intrudes into one of the enumerated categories of the Fourth Amendment: "persons, houses, papers, and effects." U.S. Const. amend. IV. Movements are an extension of the "person." By requesting six months of Doe's location information, the government seeks to track the totality of his movements, which intrudes into his "person" and thus is a search.

Even under the reasonable expectation test, Doe has a reasonable expectation of privacy in his location information. The third-party doctrine does not apply because Doe did not voluntarily convey his location information to Papaya. He took no affirmative steps and lacked knowledge of the exact information Papaya received. *See Smith*, 442 U.S. at 744. Even if he voluntarily conveyed the information, the third-party doctrine is ill fitted to modern digital technology and this Court should not apply it. *See United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). Without the third-party doctrine, Doe maintains a reasonable expectation of privacy in his location information because it allows the government to track him while he is at home. *See Kyllo*, 553 U.S at 34.

Finally, the government's search is unreasonable. A search is presumptively unreasonable unless it falls into an exception to the warrant requirement. *See, e.g.*, *Arizona v. Gant*, 556 U.S. 332, 338 (2009). The government did not obtain a warrant. *See* J.A. 8. The only relevant exception to the warrant requirement — exigent circumstances — does not apply because there is no immediate and urgent need for the law enforcement action here. *See Michigan v. Tyler*, 436 U.S. 499, 509 (1978). Thus, the search is unreasonable.

Because the government obtaining Doe's location information would constitute an unreasonable search, the government must obtain a warrant.

ARGUMENT

I. THIS ORDER IMPOSES AN UNDUE BURDEN ON PAPAYA.

A. The District Court's decision should be reviewed under an abuse of discretion standard.

Generally, appellate courts defer to trial courts on matters of discretion and review these matters under an abuse of discretion standard. *See Highmark*, 134 S. Ct. at 1748. Vacating a § 2703(d) order is a matter of discretion for the issuing judge. *See In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703 (d)*, 830 F. Supp. 2d 114, 126 (E.D. Va. 2011) (deferring to a magistrate judge's denial of a motion to vacate a § 2703(d) order because it was within her discretion). Similarly, it is well established that granting subpoenas that compel non-parties to provide information is within the discretion of the trial court. *See Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 31 (1984); *United States v. Nixon*, 418 U.S. 683, 702 (1974) (leaving the decision of enforcement of a subpoena "to the sound discretion of the trial court since the necessity for the subpoena most often turns upon a determination of factual issues"). Furthermore, courts have specifically held that district courts "[have] broad discretion in determining whether a subpoena is unduly burdensome." *Linder v. Nat'l Sec. Agency*, 94 F.3d 693, 695 (D.C. Cir. 1996); *see also Orbit One Commc'ns, Inc. v. Numerex Corp.*, 255 F.R.D. 98, 109 (S.D.N.Y. 2008). Thus, because the question of undue burden is within

the discretion of the District Court, this Court should review the District Court's decision under an abuse of discretion standard.

Under this standard, a district court's determination that an order would be unduly burdensome is upheld unless it is "clearly unreasonable, arbitrary or fanciful." *Linder*, 94 F.3d at 695. Here, the District Court was reasonable in finding that the Order would cause an undue burden. Thus, this Court should affirm that finding.

B. Interpreting undue burden to require a balancing test is reasonable.

Because Congress did not explicitly define "undue burden" in the SCA, it was reasonable to interpret "undue burden" in § 2703(d) with reference to prior common law. *See Taylor v. United States*, 495 U.S. 575, 592–93 (1990) (identifying the "maxim that a statutory term is generally presumed to have its common-law meaning").

In particular, prior to the passage of the SCA in 1986, there was a significant body of AWA and subpoena case law discussing the contours of an undue or unreasonable burden. Under AWA jurisprudence, the Court may not issue an order imposing "unreasonable burdens" on non-parties. *See United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172 (1977). Similarly, the Federal Rules of Civil Procedure allow a party to quash a subpoena if it "subjects [that] person to undue burden." Fed. R. Civ. P. 45(d)(3)(iv); *see also* Fed. R. Civ. P. 26(b)(2)(B) ("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."). In both these contexts, courts determine whether there was an undue or unreasonable burden by balancing the interests at stake. *See, e.g.*, *In re Apple*, 149 F. Supp. 3d at 373; *In re Auto. Refinishing Paint*, 229 F.R.D. 482, 495 (E.D. Pa. 2005) [hereinafter *In re Auto.*]. Accordingly, applying a balancing test to determine undue burden is correct, or at least reasonable.

C. Applying the balancing test to find undue burden is reasonable.

In conducting this balancing test, courts look to a variety of factors, including the relevance and breadth of the information requested, the necessity of the imposition, and the burden imposed on the non-party. *See In re Auto.*, 229 F.R.D. at 495. Considering these factors, the District Court was reasonable to find that the Order imposed an undue burden.

1. The government's interest in accessing Doe's location information is diminished.

The government emphasizes that it has an interest in stopping future attacks in Ames. *See* Pet'r's Br. 24. Though that is undoubtedly true, the government uses the potential threat of future attacks as a trump card, putting a deciding thumb on the scale for their position. This ignores the fact that there are limits to what information the

government can appropriately request with a § 2703(d) order. The government's request pushes these limits due to the uncertain relevance and overbreadth of the information sought, which includes all of Doe's location information for an entire six-month period, and because the government fails to prove that this information is actually necessary, given alternative investigatory methods.

a. The information sought is of uncertain relevance.

One of the factors considered under the "undue burden" analysis is the relevance of the information sought. *See In re Auto.*, 229 F.R.D. at 495. If the information requested is not relevant to the underlying litigation or investigation, then the court will find an undue burden. *See, e.g.*, *Apel v. Murphy*, 70 F.R.D. 651, 653 (D.R.I. 1976). Further, in *Bank of America Corp. v. SR International Business Insurance Co.*, the court held that "there must be a high degree of marginal utility" when a subpoena required a third party to "recover electronically stored information which is inaccessible by its nature." No. 05-CVS-5564, 2006 WL 3093174, at *5 (N.C. Super. 2006). The court denied the discovery request, noting the fact that "there might be something useful and relevant in the data" was not enough. *Id.*

Similarly, here, while the location information might be useful to some degree, the government has not demonstrated the "high degree of marginal utility" required. *Id.* The government implies that this

information about Doe would be the lynchpin both to their investigation and to stopping any possibility of future attacks. Pet'r's Br. 22 (claiming that the order "exists to apprehend" Doe in order "to stop his organization from . . . kill[ing] more"). As such, the government fails to frame its request as what it is: an attempt to gather more information about a man identified by an anonymous caller.

The government's framing overstates the known utility of the location information and ignores the uncertainty of the situation. First, Doe may not have been involved in the previous attacks and the government does not provide probable cause showing such involvement. *See* J.A. 2. The only information tying Doe to the investigation comes from an anonymous caller who knew details about the attacks "which investigators believed would be known only to those with inside knowledge." J.A. 4. This evidence shows a lot about the caller, but nothing of certain value about Doe himself. The record is silent on whether the anonymous caller had "inside knowledge" because of participation in the attacks, or because of a role in law enforcement, or some other reason. Finally, there is an additional layer of uncertainty because even if Doe was involved in the attacks, his location information may still be unhelpful to the investigation. Given the

uncertainty regarding the potential usefulness of Doe's location information, the government's interest is diminished.

b. The information requested is overbroad.

The government is not simply asking for Doe's location information for the days of the attacks. Instead, it requests location information for an entire six-month period. The sheer breadth of this request makes it likely that much of the information obtained will not be directly relevant to the investigation. In an analogous context, the Eastern District of Virginia found that an overly-broad government request for information factored against the government in the "undue burden" balancing test. *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 612 (E.D. Va. 2008). In that case, the court found that the government's request for a specific individual's emails to a non-party for a six-week period was overbroad because the request was not limited to emails that were directly related to the litigation. *Id.*; *see also Theofel v. Farey-Jones*, 359 F.3d 1066, 1071–72 (9th Cir. 2003). Here, the government has not limited its requests to the times and locations of the attacks; instead, its requests cover all of Doe's movements for a six-month period. J.A. 5. The overbreadth of the request properly weighs against the government in the undue burden analysis.

c. It is not necessary to impose this burden on Papaya.

Lastly, the government is able to investigate Doe's approximate whereabouts during the attacks without imposing on Papaya. Courts have often looked to the necessity of the imposition in determining whether the burden was undue. *See e.g.*, *In re Apple*, 149 F. Supp. 3d at 344; *Application of U.S. of Am. for an Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel. Facilities*, 616 F.2d 1122, 1133 (9th Cir. 1980). If there are alternative investigative methods, then the order may constitute an undue burden. *See Wyoming v. U.S. Dep't of Agric.*, 208 F.R.D. 449, 455 (D.D.C. 2002). Here, the government states that it "needs the records to approximate Doe's whereabouts during each attack." Pet'r's Br. 5. However, there are alternative means for the government to approximate Doe's general whereabouts during those times. It can employ traditional methods such as questioning those who witnessed the attacks or those who may have seen Doe elsewhere on those days. Because the government has alternative methods of approximating Doe's whereabouts during those three days, this Order is not necessary. *Cf. In re Penn Cent. Commercial Paper Litig.*, 61 F.R.D. 453, 467 (S.D.N.Y. 1973) (refusing to compel production of a press release because it was obtainable by the requesting party's own efforts).

Because the information requested is of uncertain relevance and is overbroad, and the Order is unnecessary, the government's interest in imposing the Order is diminished.

2. The burden imposed on Papaya is heavy.

Given the diminished interest of the government, this Order imposes an undue burden because of the heavy burden placed on Papaya. As a non-party to potential government action, Papaya faces a heavy burden in complying with the Order because of: (1) the future effects of compliance, (2) the reputational harms Papaya would suffer, (3) the fact that coding this decryption is not part of Papaya's ordinary course of business, (4) Papaya's status as a non-party to the investigation, and (5) First Amendment considerations.

The government argues that the burden analysis should only weigh resource concerns, Pet'r's Br. 8, but also notes "the starting point for interpreting a statute is the language of the statute itself," Pet'r's Br. 15 (quoting *Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc.*, 447 U.S. 102, 108 (1980)). A court "may quash or modify" an order issued under § 2703(d) "if the information or records requested are unusually voluminous in nature *or* compliance with such order *otherwise* would cause an undue burden on the provider." 18 U.S.C. § 2703(d) (emphasis added). Congress specifically outlined "unusually voluminous," a resource-based limit on the order, and then provided an

additional category of "undue burden." Thus, undue burden must cover more than just resource-specific concerns. Further, courts have considered factors such as future burden and potential reputational harm in determining "undue burden." *See, e.g.*, *In re Apple*, 149 F. Supp. 3d at 369. Therefore, looking at all the relevant factors, the burden on Papaya is heavy.

a. Papaya's compliance with the Order would have burdensome future effects.

First, creating this decryption code may damage the security Papaya has against hackers. Once Papaya writes the software to decrypt Doe's information, there will be "no guarantee that [Papaya's eradication] effort[s] would be fully successful." J.A. 31. This is because "it is difficult to irretrievably destroy something in the digital world." J.A. 31. Once the software exists, hackers may be able to access and use it against any Papaya customer. *See, e.g.*, Mitch Lipka, *Percentage of Companies that Report Systems Hacked*, CBSnews.com (June 5, 2015), http://www.cbsnews.com/news/percentage-of-companies-that-report-systems-hacked/ (discussing that over 80 percent of U.S. companies have been "successfully hacked"). This modern scourge has spread to some of the world's most technologically innovative companies, including Facebook, Google, Yahoo, and Twitter. *See* Robert McMillan, *Password Hacking Forces Big Tech Companies to Act*, The Wall Street Journal (August 7, 2016)

http://www.wsj.com/articles/password-hacking-forces-big-tech-companies-to-act-1470562202.

A second, related burden is that the government may continue to apply for and receive such orders, especially as technology advances. Although these possible future orders would be individually weighed under a balancing test, the Court should still consider their cumulative effect on Papaya. *See In re Apple Inc.*, 149 F.Supp. 3d at 370 ; *cf. Semsroth v. City of Wichita,* 239 F.R.D. 630, 637 (D. Kan. 2006) (considering past orders when determining burden on the non-party). As technology advances and Papaya begins to develop even more precise technology, the government will logically increase requests for information of this kind. The government's access to this information from non-party technology companies will almost always be easier than having to engage in traditional policing to gather information. The future effect of each of these potential orders would negatively impact Papaya. J.A. 31.

b. Papaya would suffer significant reputational harm if it complied with the Order.

Papaya's encryption software and the privacy protections it offers are central to its business model and its brand. J.A. 27 ("With Papaya Cellular, Your Privacy Comes First"). Courts have found a company's brand or corporate policy to be relevant to the undue burden analysis. *See In re Apple*, 149 F. Supp. 3d at 369 (recognizing Apple's

concern that it would tarnish its brand if it were to assist the government in accessing a cell phone); *Cognex Corp. v. Electro Sci. Indus., Inc.*, No. Civ.A. 01CV10287RCL, 2002 WL 32309413, at *5 (D. Mass. 2002). Papaya has "develop[ed] encryption technology" to support its "privacy-oriented business model." J.A. 6. Because breaking through those encryption protections would undermine that business model, it is reasonable to consider this factor in the undue burden analysis. J.A. 6.

Although Papaya informs its customers that it will provide their information to authorities operating under court order, it only promises to disclose information when such orders comply "with all relevant laws, including the Constitution." J.A. 29. Here, both courts below, and Papaya, do not believe the Order is lawful because of the "undue burden" it imposes. Therefore, complying with this Order would undermine Papaya's strong commitment to its privacy model, particularly in the eyes of its customers.

c. Compliance with this Order is not within Papaya's ordinary course of business.

It is not within Papaya's ordinary course of business to create decryption software. In *United States v. New York Telephone Company*, the Court found "the use of pen registers is by no means offensive to [the company]" because the employer regularly used them in its own business. 434 U.S. at 174. The government contends that "Papaya

develops software as part of its everyday business" and, therefore, creating such software to comply with the Order conforms with its ordinary course of business. Pet'r's Br. 27–28. However, this is incorrect: in contrast to the pen registers in *New York Telephone Company*, Papaya does not regularly create decryption software. Today, "[s]oftware has become a platform on which almost all innovative companies depend." Scott Andes, *Which Industries Develop Software? All of Them*, Brookings Blog (Apr. 21, 2016), https://www.brookings.edu/blog/metropolitan-revolution/2016/04/21/which-industries-develop-software-all-of-them/. While Papaya works to "keep[] pace with evolving technology," creating decryption code goes beyond this work. J.A. 32. It is out of the ordinary for Papaya to create decryption software, and thus creating this software would burden Papaya.

d. Papaya's status as a non-party to the government investigation increases its burden.

Papaya is similar to a non-party in a subpoena action. Courts show "concern for the unwanted burden thrust upon non-parties" and give this factor "special weight in evaluating the balance of competing needs." *Cusumano v. Microsoft Corp.*, 162 F.3d 708, 717 (1st Cir. 1998). In the subpoena context, "while discovery is a valuable right and should not be unnecessarily restricted, . . . the necessary restriction may be broader when a nonparty is the target of discovery." *Dart*

Indus. Co. v. Westwood Chem. Co., 649 F.2d 646, 649 (9th Cir. 1980) (internal citation omitted). *Accord WM High Yield v. O'Hanlon*, 460 F. Supp. 2d 891, 895–96 (S.D. Ind. 2006) (finding "non-party status is a significant factor a court must consider when assessing undue burden for the purpose of a Rule 45 motion").

The government argues that Papaya is sufficiently close to the requested order as a "service provider" to Doe. *See N.Y. Tel. Co.*, 434 U.S. at 174 (finding the telephone company to be sufficiently close to the controversy to allow for an AWA request). However, this concept of closeness is inapposite to the undue burden analysis. In the AWA context, closeness is used to limit the reach of the AWA, given the broad language of that statute. 28 U.S.C. § 1651(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."). The dissent in *New York Telephone Co.* expressed concern that if the Act was read to "confer[] authority to order persons to aid the Government in the performance of its duties, . . . it [would] provide[] a sweeping grant of authority entirely without precedent in our Nation's history." 434 U.S. at 190 (Stevens, J., dissenting). Thus, the concept of closeness was used to help limit this broad reading and is unrelated to the consideration of "unreasonable burden." *See In re Apple*, 149 F. Supp.

3d at 351, 368. In contrast, Papaya's status as a non-party should properly be recognized as part of Papaya's burden in the undue burden analysis.

e. Forcing Papaya to write a decryption code presents burdensome First Amendment implications.

Courts have held that coding is protected by the First Amendment. *See, e.g.*, *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000). Here, requiring Papaya to code a work-around of its privacy systems infringes upon its right to free speech. Further, this regulation is content-based, and therefore must be narrowly tailored to further a compelling state interest. *See Riley v. National Federation of the Blind of North Carolina, Inc.*, 487 U.S. 781, 798 (1988) [hereinafter *NFB*]. This Order does not meet that strict standard. Therefore, Papaya faces a restriction on its First Amendment rights. This restriction should be factored into the § 2703(d) "undue burden" analysis. *Cf. Application of R.J. Reynolds Tobacco Co.*, 136 Misc.2d 282, 287 (N.Y. Sup. Ct. 1987) (holding that First Amendment protections shielding medical scholars from interference with their academic freedom "may properly figure into the legal calculation of whether forced disclosure would be reasonable").

i. The Order infringes on protected speech.

The coding at issue here is a type of protected expressive conduct. The First Amendment protects conduct that is inherently

expressive. *Rumsfeld v. Forum for Acad. & Institutional Rights, Inc.*, 547 U.S. 47, 66 (2006) [hereinafter *FAIR*]. Conduct is inherently expressive when it communicates a particularized message that a reasonable observer would understand and attribute to the speaker. *Id.* (finding no expressive conduct because a reasonable observer would not understand the message); *W. Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624, 632 (1943) (finding expressive conduct because the pledge of allegiance and the flag salute was symbolic).

Here, the decryption code the Papaya engineers would write communicates a particularized message: that Papaya endorses governmental intrusion into its customers' private information. Additionally, this message is one that a reasonable observer would understand and attribute to Papaya. This is different from the conduct of the law schools in *FAIR*. In that case, the Court found that "[a]n observer who sees military recruiters interviewing away from the law school has no way of knowing whether the law school is expressing its disapproval of the military" or something else. 547 U.S. at 66). In contrast, any observer seeing Papaya write and sign the decryption code would infer that Papaya endorses the decryption.

The government contends that because the code simply performs a function — namely, to disaggregate Doe's location information — it does not communicate any particular message and therefore should not

be granted First Amendment protections. Pet'r's Br. 31. This is wrong. Functional code can still express a message. In *Universal City Studios, Inc. v. Corley*, the court found that software which decrypted DVDs was an expressive communication that deserved First Amendment protection. 273 F.3d 429, 445 (2d Cir. 2001); *see also Junger*, 209 F.3d at 485 (6th Cir. 2000); *cf. Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 570 (2011). Additionally, "writing software [is] an extremely creative and expressive activity" because "the programmer makes expressive choices about how to manipulate data, what vocabulary to use in the process, and how to construct the user interface." J.A. 32. Therefore, coding can be expressive, and because creating the decryption software here communicates a particularized message, it is expressive conduct.

ii. The Order constitutes a content-based compulsion of speech.

Given that writing this code constitutes expressive conduct that is protected as speech by the First Amendment, forcing Papaya to write this code is compelled speech. Further, this compulsion is content-based because the government would force Papaya to express a view it would not otherwise express. *See NFB*, 487 U.S. at 795 ("Mandating speech that a speaker would not otherwise make necessarily alters the content of the speech. We therefore consider [that] as a content-based regulation of speech."). For example, in *Pacific Gas & Electric Co. v. Public Utilities Commission of California*,

the Court found a regulation to be content-based because it "d[id] not equally constrain both sides of the debate" and required a utility company to help disseminate views that it did not agree with. 475 U.S. 1, 14 (1986). Similarly, the Order forces Papaya to express the view that it supports government surveillance through cell site location information. It does not equally constrain the other side of the public debate that advocates for increased protection of privacy. "This kind of favoritism goes well beyond . . . fundamentally content-neutral subsidies." *Id.* at 14. Accordingly, this Order is a content-based regulation of speech.

iii. The government cannot compel speech unless there is a compelling state interest that is narrowly tailored.

Because it is content-based compulsion, the government needs to demonstrate that such compulsion is narrowly tailored to further a compelling state interest. *See NFB*, 487 U.S. at 796. This requires that the speech restriction "must be the 'least restrictive means among available, effective alternatives.'" *United States v. Alvarez*, 132 S. Ct. 2537, 2540 (2012) (quoting *Ashcroft v. Am. Civil Liberties Union*, 542 U.S. 656, 666 (2004)). The government has failed to show that here.

The government's interest is investigating the previous attacks and preventing future attacks. J.A 17. This interest can be fulfilled through alternative investigatory tactics without imposing on Papaya. *See supra I.C.3.* Even if these investigatory tactics would require the

expenditure of more government resources than simply demanding Papaya provide the information, this Court has "simply and emphatically [affirmed] that the First Amendment does not permit the State to sacrifice speech for efficiency." *NFB*, 487 U.S. at 795 (citing *Village of Schaumburg v. Citizens for a Better Environment*, 444 U.S. 620, 639 (1980); *Schneider v. State*, 308 U.S. 147, 164 (1939)). Therefore, the Order is not narrowly tailored, and it creates serious First Amendment concerns, which increase the burden imposed on Papaya.

Although the government has an interest in gathering location information on Doe, it has failed to show that the breadth of the information sought is adequately relevant and has enough marginal utility to outweigh the heavy burden placed on Papaya.

D. The district court did not abuse its discretion in quashing the Order due to an undue burden despite cost-shifting.

Even though there is cost-shifting, the Order still poses an undue burden. The government contends that the "undue burden" analysis is primarily concerned with financial and resource-specific burdens. *See* Pet'r's Br. 8. However, interpreting "undue burden" in this way would basically write the undue burden requirement out of the statute. Section 2706 dictates that a governmental entity obtaining information under § 2703 "shall pay . . . for reimbursement

for such costs as are reasonably necessary." 18 U.S.C. § 2706(a) (2012). The only exceptions to this automatic cost-shifting requirement are requests for telephone toll records and telephone listings under § 2706(c). *Id.* § 2706(c). For these exceptions, § 2706(c) specifically states that an undue burden can be overcome with cost-shifting. *Id.* This implies that for all other information, cost-shifting cannot overcome the undue burden. Thus, if the term "undue burden" only pertained to financial resources burdens, then there could never be a finding of undue burden under § 2703(d) since costs are already always reimbursed. This idea that undue burden is separate from financial and resource concerns is also present in the discovery context generally. For instance, in *Cognex Corp v. Electro Science Industries, Inc.*, the District Court of Massachusetts emphasized that there are limitations on the volume of discovery in a proceeding and "[t]here is no exception to those limitations based upon one party's willingness to pay." 2002 WL 32309413, at *5.

Cost-shifting does not reduce the burden on Papaya because the main burdens Papaya faces are not resource-specific or financial. Rather, the main burdens on Papaya are the casting aside of its privacy-focused business model and the threat to its First Amendment rights. Thus, there is an undue burden on Papaya despite cost-shifting.

E. If this Court finds that the District Court abused its discretion in concluding that the Order imposed an undue burden, it should remand.

If this Court finds an alternative framework for determining whether a burden is "undue" and, consequently, whether or not a motion to quash should have been granted in this case, then it should ultimately remand to the Ames District Court for judgment in the first instance under that new framework. This is especially necessary if new facts will be needed to make the determination. This is because "[w]hen an appellate court discerns that a district court has failed to make a finding because of an erroneous view of the law, the usual rule is that there should be a remand for further proceedings to permit the trial court to make the missing findings." *Pullman-Standard v. Swint*, 456 U.S. 273, 291 (1982); *see also DeMarco v. United States*, 415 U.S. 449, 450 (1974). If this Court believes that the District Court abused its discretion by applying an incorrect legal standard, it should remand for the District Court to apply the different legal standard, as the District Court is the most appropriate venue for determinations of fact within that framework.

This Court should defer to the lower court's reasonable finding that this Order imposes an "undue burden" on Papaya. The government's interest is diminished given the uncertain relevance and overbreadth of the information it seeks. By contrast, the burdens

Papaya would suffer properly tip the scale in the "undue burden" analysis. Therefore, this Court should affirm the lower court's decision to quash the Order.

II. THE FOURTH AMENDMENT PROHIBITS THE GOVERNMENT FROM OBTAINING DOE'S CELL SITE LOCATION INFORMATION WITHOUT A WARRANT.

A. The Court should apply the canon of constitutional avoidance to read § 2703(c)(1) of the SCA to require a warrant for location information.

If a statute is ambiguous, the Court has a duty to construe the ambiguous language to avoid serious constitutional problems unless plainly contrary to the intent of Congress. *See, e.g.*, *Jones*, 529 U.S. at 857. The canon of constitutional avoidance reflects a "prudential concern that constitutional issues not be needlessly confronted." *Edward J. DeBartolo v. Fla. Gulf Coast Bldg. and Constr. Trades Council*, 485 U.S. 568, 575 (1988).

The statute's text is ambiguous because it does not provide guidance as to when the government must obtain a warrant instead of a court order for information that falls within § 2703(c). Of the two plausible interpretations, only one — requiring a warrant for location information — avoids serious constitutional doubt. Because this interpretation is not plainly contrary to Congress's intent, the Court should employ constitutional avoidance to interpret § 2703(c) as requiring a warrant for location information.

1. Section 2703(c)(1) of the SCA is ambiguous.

Section 2703(c) covers "record[s] or other information" that "concern[] electronic communication service or remote computing service," including location and subscriber information. 18 U.S.C. § 2703(c)(1). Section 2703(c)(1) gives the government five methods to obtain information, including a warrant pursuant to the Federal Rules of Criminal Procedure, 18 U.S.C. § 2703(c)(1)(A); a court order under § 2703(d), 18 U.S.C. § 2703(c)(1)(B); and an administrative subpoena for subscriber information, 18 U.S.C. § 2703(c)(1)(E).

The government broadly asserts that the SCA "lays out specifically" what the government must do to obtain information. Pet'r's Br. 53. But statutory specificity does not rid § 2703(c)(1) of ambiguity. Indeed, the plain words of the statute fail to specify under what circumstances the government must obtain a warrant instead of a court order, and vice versa. Because of this lack of guidance, § 2703(c)(1) is ambiguous: either the government must obtain a warrant for location information, or a mere court order suffices.

2. Interpreting § 2703(c)(1) to require the government to obtain a warrant for location information erases constitutional doubt.

There are two plausible interpretations of § 2703(c)(1). The first interpretation requires the government to obtain a warrant for some

set of information that is not subscriber information. The second interpretation allows the government to only obtain a court order under § 2703(d) for all information that falls within § 2703(c)(1). The first of these is clearly constitutional; the second potentially runs afoul of the Fourth Amendment. Therefore, the Court has a duty to adopt the first. *See DeBartolo*, 485 U.S. at 575.

Under the first interpretation, the government must obtain a warrant supported by probable cause to receive location information. This interpretation ensures that § 2703(c)(1) comports with the Fourth Amendment's requirement that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. Because location information might be protected by the Fourth Amendment as an extension of the "person," *see infra* section II.C, interpreting § 2703(c)(1) to require a warrant for such information resolves the statute's ambiguity and avoids serious constitutional doubts.

The government would have this Court interpret § 2703(c)(1) to require only a court order supported by "specific and articulable facts" to obtain location information. 18 U.S.C. 2703(d); *see* Pet'r's Br. 50. This interpretation is of questionable constitutionality. Whether location information is protected under the Fourth Amendment is at

best an open question. *See infra* section II.B & C. Thus, interpreting § 2703(c)(1) to require a warrant for location information removes the serious constitutional doubts that the government's interpretation raises.

3. Requiring the government to obtain a warrant for location information is not contrary to Congress's intent.

The Court has a duty to adopt the plausible interpretation that does not raise a serious constitutional question if it is not plainly contrary to Congress's intent. *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 78 (1994). In passing the SCA, Congress sought to limit the government's "arbitrary use" of power to intrude into constitutionally-protected categories using newly-developed technologies that "expand[] dramatically the opportunity for such intrusions." S. Rep. No. 99-451, at 1-2 (1986). A special concern was "overzealous law enforcement agencies." *Id.* at 3.

The Senate Report sheds no light on when the government must obtain a warrant under § 2703(c)(1) instead of a court order under § 2703(d). *See id.* at 38-39. However, the structure of § 2703 itself provides guidance. Section 2703 mentions two types of information specifically: content of communications and subscriber information. *See* 18 U.S.C. § 2703(a)-(c). The section is structured such that it creates a spectrum of information. At one end is communication content, which requires the highest protection: a

warrant. 18 U.S.C. § 2703(a), (b). At the other end is subscriber information, which requires lower protection: an administrative subpoena. 18 U.S.C. § 2703(c)(2). Along this spectrum, the corresponding procedures for obtaining information become progressively more stringent. Congress thus recognized that not all information is the same and protected some information more than other information.

Further, interpreting § 2703(c) to allow the government to choose whether to get a warrant or court order would render the warrant provision of § 2703(c)(1) superfluous. If all the government needs is a court order, it will never seek a warrant. A warrant requires probable cause. Fed. R. Crim. P. 41(d). A § 2703(d) order, however, requires a lesser standard: "specific and articulable facts." 18 U.S.C. § 2703(d). Since a court order requires a lower standard, the government has no reason to opt for a warrant. This would render the warrant section superfluous and thus contravene Congress's intent.

In passing the SCA, Congress intended to create a framework that would protect the privacy of technology users while simultaneously protecting the government's law enforcement interests. *See* S. Rep. No. 99-451, at 3. Applying constitutional avoidance here achieves both goals. Cell phone users' privacy interests will be protected by requiring a warrant to search location information, and law

enforcement retains a mechanism for obtaining the information that raises no constitutional doubts. Because requiring a warrant for location information comports with Congress's intent and does not raise constitutional doubts, this Court should apply the constitutional avoidance canon to interpret § 2703(c)(1) accordingly.

B. The reasonable expectation test fails to ensure adequate Fourth Amendment protection.

The government conducts a search when it intrudes into an individual's person, house, papers, or effects. *See Kyllo*, 533 U.S. at 31. When there is no physical intrusion, courts ask whether the government's conduct violated the individual's "reasonable expectation of privacy." *Id.* The third-party doctrine is an application of this reasonable expectation test: under it, an individual loses any reasonable expectation of privacy for information he has voluntarily conveyed to a third party. *Smith*, 442 U.S. at 744.

This Court should not apply the reasonable expectation test for three reasons. First, it can lead to arbitrary results; second, it provides inadequate protection for individuals; and third, it erodes Fourth Amendment protection.

1. The reasonable expectation test can produce arbitrary results.

To determine whether the government has conducted a Fourth Amendment search, courts look at whether the government intruded

into an individual's reasonable expectation of privacy. *Kyllo*, 533 U.S. at 34. Under the reasonable expectation test, a search occurs if (1) the government violates an individual's subjective expectation of privacy that, (2) society deems reasonable. *Id.* In applying this test, courts have also used the third-party doctrine to determine both steps. *See, e.g.*, *Smith*, 442 U.S. at 743. Under the third-party doctrine, when an individual voluntarily conveys information to a third party, he loses any reasonable expectation of privacy for that information: either he has no subjective expectation of privacy, or else his subjective expectation is not one society deems reasonable. *Id.* Therefore, when the government applies the third-party doctrine here, Pet'r's Br. 35, it is really applying the reasonable expectation test.

The reasonable expectation test is often criticized — including by members of this Court. Many fault the test for being "circular" and "unpredictable." *Kyllo*, 533) U.S. at 34; *see also Jones*, 132 S. Ct. at 962 (Alito, J., concurring); *Minnesota v. Carter*, 525 U.S. 83, 91 (1998) (Scalia, J., concurring) (noting that the test is "fuzzy").

The government employs the reasonable expectation test by relying on arbitrary factors, which yields arbitrary results. First, the government argues that "Papaya customers are especially aware that they convey their location information to the company" because of Papaya's privacy policy. Pet'r's Br. 36. However, basing an

individual's expectations of privacy — and thus his Fourth Amendment protection — on his cell service provider's privacy policy condition an individual's Fourth Amendment protection on that policy. This would allow "strategic business decisions to dictate the scope," Pet'r's Br. 39, of the reasonable expectation test, making a "crazy quilt of the Fourth Amendment." *Smith*, 442 U.S. at 745.

Furthermore, the government argues that Doe had no reasonable expectation of privacy in his location information because "cell users are constantly reminded that they expose their location information to providers whenever they experience dropped calls and 'no service' indicators." Pet'r's Br. 35–36. The government cites no support for this generalization. It is just as reasonable to assume that cell phone users have no idea what a "no signal" message means about whether their location is conveyed. The government seems to make a mistake judges have warned is a common pitfall in applying the reasonable expectation test: "confus[ing] [its] own expectations of privacy with those of the hypothetical reasonable person." *See, e.g.*, *Jones*, 132 S. Ct. at 962 (Alito, J., concurring).

Even if the government had support for its assumption about cell phone users, its argument would mean that Fourth Amendment protection rises and falls on how much citizens understand technology. But modern technology changes rapidly. Cf. Riley v.

California, 134 S. Ct. 2473, 2484 (2014) (noting that current cell phones are "based on technology nearly inconceivable just a few decades ago"). Under the government's argument, an individual's Fourth Amendment rights come from citizens' understanding of technology, despite "perpetual technological change." Jay Stanley, American Constitution Society for Law and Policy, The Crisis in Fourth Amendment Jurisprudence 6 (2010). With such an arbitrary standard, the Fourth Amendment guarantee of security from arbitrary government intrusion would be constantly in flux.

2. The reasonable expectation test provides Fourth Amendment protection only to privacy interests that society deems worth protecting.

Under the reasonable expectation test, an expectation is "reasonable" only if society says it is. *See Smith*, 442 U.S. at 743. This structure, however, would only protect the privacy expectations of the majority. But the Bill of Rights protects individuals from the tyranny of the majority. *See United States v. Carolene Prod. Co.*, 304 U.S. 144, 152 n.4 (1938). Just as socially-accepted speech is not the only kind of speech that the First Amendment protects, neither should the Fourth Amendment only protect what society deems as a reasonable expectation of privacy. *Cf. Snyder v. Phelps*, 562 U.S. 443, 458 (2011) (holding that picketing outside a soldier's funeral was protected speech under the First Amendment).

3. The reasonable expectation test inevitably erodes the Fourth Amendment.

Under the reasonable expectation test, "people get only the privacy that they expect to get." Stanley, *supra* at 5. This circular construction allows the government to condition individuals to expect increasingly less privacy. The government contends that *Smith* controls this case. Pet'r's Br. 35. However, the *Smith* Court contemplated a future in which the reasonable expectation test "would provide an inadequate index of Fourth Amendment protection." 442 U.S. at 751 n.5. For example, the government could eliminate any expectation of privacy by "announc[ing] on nationwide television that all homes henceforth would be subject to warrantless entry." *Id.* This creates a "one-way ratchet" that erodes Fourth Amendment protection. Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 Am. U. L. Rev. 1381, 1382 (2008).

Deriving Doe's Fourth Amendment protection from his reasonable expectation of privacy would create arbitrary results and ultimately erode the Fourth Amendment's guarantee against unreasonable government intrusion. Accordingly, this court should not employ the reasonable expectation test to determine whether the government conducts a search in obtaining Doe's location information.

C. Obtaining six months of Doe's location information is a search because it represents an intrusion into his person, a protected category under the Fourth Amendment.

Because the reasonable expectation test does not ensure adequate Fourth Amendment protection, this Court should not apply it, and should instead make an objective inquiry into what the Amendment was intended to protect. *Cf. Kyllo*, 533 U.S. at 40 (noting that the Fourth Amendment analysis "must take the long view, from the original meaning of the [text]"). Such an inquiry begins with the Amendment's text. The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches." U.S. Const. amend. IV. If the government intrudes into any of these categories, a search has occurred, regardless of the presence of a third party.

Here, the government requests six months of Doe's location information. J.A. 21. This location information represents Doe's movements — movements that are an extension of his "person" under the Fourth Amendment. By accessing location information showing Doe's past movements over a six-month period, the government gains the capability to track his movements at a scale well beyond what this Court has said constitutes an intrusion, and thus a search.

1. Doe's movements are an extension of his person.

This Court has consistently held that, at a minimum, the Fourth Amendment protects the categories that are explicitly in its text: persons, houses, papers, and effects. *See, e.g.*, *Jones*, 132 S. Ct. at 952. The Court has expanded this protection beyond the physical manifestations of those categories. One example is the "curtilage" doctrine extending the "house" to areas surrounding the home. *See Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013). Another example extends the "papers and effects" category to intangible data stored both on a cell phone and remotely in the cloud. *See Riley*, 134 S. Ct. at 2491.

This same understanding applies to the "person" category. Although the typical search of a "person" under this Court's jurisprudence is a physical body search, s*ee, e.g.*, *Maryland v. King*, 133 S. Ct. 1958, 1968-69 (2013), "person" extends beyond the physical body. An individual's actions, including his movements from one place to another, are as much a part of his "person" as the body. Indeed, the Court appears to have already embraced this concept that the "person" extends beyond the physical body because the Court protects the contents of communications. *See Katz v. U.S.*, 389 U.S. 347, 512 (1967). This protection is so strong that courts uphold it notwithstanding the third-party doctrine or the reasonable expectation test. *See, e.g.*, *Smith*, 442 U.S. at 746 (Stewart, J., dissenting) (noting

that telephone conversations require transmission through telephone company equipment, but are still protected under the Fourth Amendment). The content of an individual's communication is a manifestation of what is in his mind. *See* Orin S. Kerr, *Applying Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1018 (2010). Therefore, even when those communications are not written on an individual's papers, tangible or digital, they are protected as an extension of the "person" category.

Thus, just as a search of the house is not limited to a search of the physical house and a search of a cell phone includes a search of items stored inside and remotely, a search of the "person" extends to a search of his actions, including his movements. And so, as an extension of his person, Doe's movements — as represented by his location information — fall within the enumerated "person" category.

2. Obtaining six months of Doe's location information is a significant intrusion into Doe's "person."

Given this understanding of "persons," the government attempts to conduct a search when it requests six months' worth of Doe's movements. The totality of an individual's movements is part of his actions, and therefore part of his "person." Location information allows the government to track the sum of an individual's movements, and the scale of that tracking makes it a government intrusion into Doe's "person."

One of the central underpinnings of the security guaranteed by the Fourth Amendment is "freedom from surveillance." *Johnson v. United States*, 333 U.S. 10, 14 (1948). As Justice Sotomayor stated, "[a]wareness that the Government may be watching chills associational and expressive freedoms." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). Consequently, this Court has recognized that certain types of government surveillance cross the line from observation to intrusion, depending on the scale of the surveillance. This is clear from *United States v. Knotts*, *United States v. Karo*, and *Jones*.

In *Knotts*, this Court held that when the government's use of technology is "limited" and "merely a more effective means of observing what is already public," it is not an intrusion. 460 U.S. 276, 284 (1983). The Court also noted, that if "twenty-four hour surveillance" had occurred then it might have been an intrusion. *Id.* The Court held in *Karo* that surveillance practices that monitor an individual while in a location "not open to visual surveillance," including the home, are a government intrusion. 468 U.S. 705, 714 (1984); *see also Kyllo*, 553 U.S. at 2045.

Additionally, the concurrences in *Jones* addressed the scale of the government's intrusion. 132 S. Ct. at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring). There, the government

attached a GPS device to the defendant's vehicle and tracked him for four weeks. 132 S. Ct. at 948 (majority). Both concurrences emphasized that tracking an individual for four weeks would be an intrusion, even without the GPS device. To Justice Sotomayor, such extensive surveillance gives the government the "sum of one's public movements," which implicates greater privacy concerns than isolated observation, as it both could "reveal private aspects of identity" and also evade the checks of traditional surveillance. *Id.* at 956 (concurring). To Justice Alito, the government's attempt to "track every movement the [defendant] made in the vehicle he was driving" represented such a high "degree of intrusion" that the surveillance was a search. *Id.* at 964 (concurring).

The government obtaining Doe's location information would be an even greater intrusion than the government's conduct in *Knotts*, *Karo*, or *Jones*. Here, the government requested surveillance for six times the duration of the tracking in *Jones*: six months' worth of Doe's location information — his location whenever he "made or received a call, sent or received a text, or use[d] . . . any application requiring the use of cellular data." J.A. 33. In the areas with the densest Papaya cell coverage, the government could track Doe's movements as he travels from block to block. J.A. 33. At an average of 100 connections per day, the government seeks warrantless access to approximately

18,000 references to Doe's location. J.A. 33. As the Ames Circuit noted, the government intrusion here is "further intensified by the volume of data sought." J.A. 10.

The government contends that "an individual's whereabouts have never been viewed as particularly personal information." Pet'r's Br. 48. These assertions contradict Justice Sotomayor's emphasis that the sum of an individual's movements can disclose movements of an "indisputably private nature," such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic," and so on. *Jones*, 132 S. Ct. at 955. (concurring) (citations omitted). Accordingly, Doe's location information implicates much more than just his travels "on public thoroughfares." *Knotts*, 460 U.S. at 281. As this Court has recognized, "nearly three-quarters of smartphone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Riley*, 134 S. Ct. at 2490. Access to an individual's every movement for six months would allow the government to track that individual in and out of private areas — including the home, rendering the surveillance an intrusion. *See Karo*, 468 U.S. at 714.

Furthermore, the intrusion caused by obtaining location information has none of the ordinary checks of traditional surveillance. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J.,

concurring). The government attempts to obtain Doe's location information without his knowledge, and without having to risk detection or expend resources. *See, e.g.*, *id.* at 964 (Alito, J., concurring).

This Court "need not identify with precision the point at which the tracking" of an individual becomes an intrusion that executes a search. *Id.* Brief surveillance may simply be a de minimis intrusion. But given the length of time and the quality of information cell site location information reveals, this case passes the "line . . . surely crossed before the 4-week mark" of surveillance in *Jones*. *Id.* If the government has any "uncertainty with respect to whether a certain period" of surveillance would constitute a Fourth Amendment search, it "may always seek a warrant." *Id.*

The scale of the surveillance executed through obtaining location information makes that conduct a government intrusion into Doe's movements, and thus a search under the Fourth Amendment.

3. Doe's location information was neither conveyed directly to the government, nor left in plain view of the government.

Because this analysis does not depend on reasonable expectations of privacy, whether an individual lost a reasonable expectation of privacy by conveying information to a third party is irrelevant. The presence of a third party is relevant when the target of the search conveyed information directly to the government or a

government informant, or left the information in plain view of the government. *See, e.g.*, *Lewis v. United States*, 385 U.S. 206, 210 (1966) (finding no government intrusion where the defendant invited an undercover agent into his home); *United States v. Lee*, 274 U.S. 559, 563 (1927) (finding that there was no government search of the defendant's boat where the contraband was in plain view). There is no intrusion, and thus no search, where an individual "willingly admit[s]" the government or its agent into one of the categories in his life that the Fourth Amendment protects. *Lewis*, 385 U.S. at 212.

Here, Doe neither conveyed his location information to the government, nor did he leave the information in plain view. On the contrary, Doe's cell phone generated a signal sent to only Papaya's cell towers. J.A. 25. If Papaya wanted to voluntarily give that information to the government, it could do so without violating the Fourth Amendment. The government cannot, however, demand Papaya produce the information without conducting a search under the Fourth Amendment.

D. Even under the reasonable expectation test, the government obtaining Doe's location information would constitute a search.

Doe has a legitimate expectation of privacy in his location information for three reasons. First, the third-party doctrine is inapplicable as there was no voluntary conveyance. Second, the third-

party doctrine should not apply to digital technology. Third, Doe's location information reveals information about the home, in which Doe has a legitimate expectation of privacy. Thus, the government obtaining Doe's location information would constitute a search.

1. Third-party doctrine does not apply here because Doe did not voluntarily convey his location information to Papaya.

Voluntary conveyance requires that individuals take affirmative steps to convey to the third party the information the government sought and have knowledge of the exact information. *See Smith*, 442 U.S. at 744 (dialing phone numbers); *United States v. Miller*, 425 U.S. 435, 442 (1976) (giving specific records to bank). In contrast, location information can be recorded without the cell user's action or knowledge. An incoming phone call or text — whether or not Doe answered or responded — would record Doe's location information without any action on his part. *See* J.A. 33; *see also In re Application of U.S. for an Order Directing a Provider of Electronic Communications Services to Disclose Records to the Government*, 620 F.3d 304, 317-18 (3d Cir. 2010). Additionally, he may not even be aware that his location was recorded. *See In re Application for Telephone Information Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1028 (N.D. Cal. 2015). Doe took no affirmative step to convey the information and could not have known exactly what location information was

conveyed. Thus, he did not voluntarily convey that information to Papaya.

2. Even if there was a voluntary conveyance, the third-party doctrine is inappropriate when applied to digital technology.

The third-party doctrine is "ill suited to the digital age," *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring), and this Court should not apply it here. This Court's precedent demonstrates that Fourth Amendment analysis can evolve in the face of new technology. For instance, *Riley* found that the incident to arrest warrant exception should not be blindly applied to cell phones. 134 S. Ct. at 2489 (finding the quantitative and qualitative differences between cell phones and other objects required an exception); *see also Katz*, 389 U.S. at 352. Here, the government's attempt to shoehorn location information into a case dealing with technology from the 1970s is "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 2489. Given the pervasiveness of cell phones, *id.*, "cellular service providers have records of the geographic location of almost every American" at almost all times, *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011). Rote application of the third-party doctrine to location information would allow the government to access comprehensive location information without a warrant just because individuals opted into a technology that pervades modern life.

3. Doe has a legitimate expectation of privacy in his home.

As this Court stated in *Kyllo*, with respect to the home, there is a "minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*." 553 U.S. at 34. Further, the *Karo* Court found that it was a search when the government used technology to determine "whether a particular article — or a person, for that matter — [was] in an individual's home at a particular time." 468 U.S. at 716. Here, the government's request would give it comparable information by allowing it to track when Doe's cell phone in his home and to infer when Doe is in his home. Therefore, the government obtaining Doe's location information constitutes a search.

E. The government's warrantless search is unreasonable because no exception to the warrant requirement applies.

This Court has consistently held that the rule when addressing the reasonableness of a warrantless search is that the search is presumptively unreasonable unless it falls into an exception to the warrant requirement. *See, e.g.*, *Gant*, 556 U.S. at 338; *Kyllo*, 533 U.S. at 40. Such a bright-line rule is appropriate when determining whether a search is reasonable because it provides clear guidance to police officers. *See New York v. Belton*, 453 U.S. 454, 458 (1981) (noting that a "highly sophisticated set of rules . . . may be literally impossible [to apply] by the officer in the field") (citation omitted). This rule — easily applicable by police officers in the field —

thereby protects "[t]he security of one's privacy against arbitrary intrusion by the police," which is "basic to a free society." *Wolf v. People of State of Colorado*, 338 U.S. 25, 27 (1949).

Here, the government did not obtain a warrant to search Doe's location information. *See* J.A. 8. Because no exception to the warrant requirement applies, the government's warrantless search of Doe's location information is unreasonable.

1. No exception to the warrant requirement applies, rendering the search unconstitutional.

While there are various exceptions to the warrant requirement, only one, exigent circumstances, is relevant. But here, that exception does not apply.

The exigent circumstances exception "applies when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment." *Kentucky v. King*, 563 U.S. 452, 460 (2011) (internal quotation marks and brackets omitted). Such circumstances present an immediate and urgent need for police action. *See Tyler*, 436 U.S. at 509. Exigent circumstances justifying a warrantless search include law enforcement intruding into a protected category to: provide aid to injured people or prevent immediately impending injury, *see Michigan v. Fisher*, 558 U.S. 45, 47–48 (2009) (per curiam); fight or investigate fires, *see Michigan v. Clifford*, 464 U.S 287, 293 (1984);

pursue a fleeing suspect, *see United States v. Santana*, 427 U.S. 38, 42–43 (1976); and prevent the imminent destruction of evidence, *see King*, 563 U.S. at 460. The unifying feature of these circumstances is the "compelling need for official action and no time to secure a warrant." *Missouri v. McNeely*, 133 S. Ct. 1552, 1559 (2013) (quoting *Tyler*, 436 U.S. at 509). Further, the seriousness of the offense cannot provide the exigent circumstances. *See, e.g.*, *Mincey v. Arizona*, 437 U.S. 385, 394 (1978) (declining to hold that "the seriousness of the [homicide] under investigation itself create[d] exigent circumstances").

There are no exigent circumstances in this case. The government's goals are purely investigatory and preventive: to "identify all of the individuals responsible for the terrorist attacks . . . and prevent future acts of violence." J.A. 17. The government does not seek to provide emergency aid to injured people, pursue a fleeing suspect, or prevent the destruction of evidence. Nor do the attacks that the government seeks to prevent carry the immediacy inherent in the exigent circumstances exception. This Court has "not dispensed with the fundamental Fourth Amendment prohibition against unreasonable searches and seizures simply because of a generalized urgency of law enforcement." *Torres v. Puerto Rico*, 442 U.S. 465, 474 (1979). Further, the government might argue that the exigent circumstances are created from the nature of the offenses themselves:

multiple attacks that killed 27 people. J.A. 3. But serious crimes, in and of themselves, do not create exigent circumstances. *See Mincey*, 437 U.S. at 394.

Because the government's warrantless search of Doe's location information does not fall into any exception to the warrant requirement, it is unreasonable and violates the Fourth Amendment.

2. The government's application of a balancing test to determine if the warrantless search is reasonable is inappropriate.

The government admits that "the reasonableness requirement is typically satisfied by a showing of probable cause," but then inexplicably uses a balancing test to conclude that the search is reasonable. Pet'r's Br. 46. The government used the wrong test and thus reached the wrong conclusion. The application of a balancing test is inapposite where, as here, the subject of the search lacks a status that diminishes his privacy interests.

The balancing test weighs governmental interests against private interests. *United States v. Knights*, 534 U.S. 112, 121 (2001). This Court has used the test to balance interests where the subjects of searches have diminished privacy interests due to their status: for example, searches of inmates and their cells, *Hudson v. Palmer*, 468 U.S. 517, 525 (1984); public-school students, *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652–53 (1995); and parolees, *Samson*

v. California, 547 U.S. 843, 848 (2006), and probationers, *Knights*, 534 U.S. at 119.

The government appears to argue that a balancing of interests is suitable in this case because Doe has a diminished expectation of privacy in his location information. *See* Pet'r's Br. 47. Given the government's reliance on the third-party doctrine, it is reasonable to assume that Doe's "diminished expectation of privacy" stems from the fact that Papaya, a third party, collects his location information. The third-party doctrine, however, serves no purpose when determining whether a search is reasonable. The only diminished privacy interests that play a role at this stage of the analysis stem from the subjects' status as, for example, parolees, probationers, or public-school students. Further, there is no special status reserved for what the government repeatedly calls Doe: a "suspected terrorist" and "the suspected bomber." Pet'r's Br. 46. Suspects in criminal investigations have no diminished privacy interests. More importantly, it is inappropriate to treat Doe like an inmate or parolee without due process of law.

Requiring a warrant in this case may indeed hinder a criminal investigation. Of course the "investigation of crime would always be simplified if warrants were unnecessary." *Mincey*, 437 U.S. at

393. But privacy "may not be totally sacrificed in the name of maximum simplicity in enforcement of the criminal law." *Id.*

Ultimately, the Court need not go this far. The Court can avoid this constitutional question and reasonably interpret § 2703(c)(1) to require a warrant for location information. If the Court declines to employ constitutional avoidance, the government obtaining Doe's location information constitutes a warrantless search into his person that is unreasonable because no exception to the warrant requirement applies. Thus, the search violates Doe's Fourth Amendment rights.

CONCLUSION

For the foregoing reasons, the judgment of the United States Court of Appeals for the Ames Circuit should be affirmed or alternatively remanded for further fact-finding.

October 14, 2016

Respectfully submitted,

_____
Michelle G. Adler

_____
Victoria L. Hartmann

_____
Helen M. Rave

_____
Caroline M. Trusty

_____
Stefanie A. Tubbs

_____
Mengjie Zou

The Lucy Stone Memorial Team

APPENDIX

The Fourth Amendment to the U.S. Constitution

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, 28 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.

* * *

§ 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.

Federal Rules of Civil Procedure
(selected rules)

Rule 26. Duty to Disclose; General Provisions Governing Discovery

. . . .

(b) Discovery Scope and Limits.

. . . .

(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.

(C) When Required. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;

(ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or

(iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1).

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.

. . . .

(3) Quashing or Modifying a Subpoena.

(A) When Required. On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) When Permitted. To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) Specifying Conditions as an Alternative. In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

Federal Rules of Criminal Procedure

Rule 41. Search and Seizure

. . . .

(d) Obtaining a Warrant.

(1) In General. After receiving an affidavit or other information, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.

(2) Requesting a Warrant in the Presence of a Judge.

(A) Warrant on an Affidavit. When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

(B) Warrant on Sworn Testimony. The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.

(C) Recording Testimony. Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

(3) Requesting a Warrant by Telephonic or Other Reliable Electronic Means. In accordance with Rule 4.1, a magistrate judge may issue a warrant based on information communicated by telephone or other reliable electronic means.