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

JOINT APPENDIX

TABLE OF CONTENTS

SUPREME COURT OF THE UNITED STATES
ORDER LIST

Certiorari Granted

September 6, 2016

16-611 United States of America v. Papaya Cellular, Inc.

The petition for a writ of certiorari is granted on the following two questions:

1. Whether the court of appeals erred in concluding that it would cause an "undue burden" on Papaya Cellular, within the meaning of 18 U.S.C. 2703(d), to require it to write software to override its encryption technology and disaggregate a particular subscriber's historical cell site information to assist in an ongoing terrorism investigation.

2. Whether the court of appeals erred in concluding that disclosure of the historical cell site information would violate the Fourth Amendment.

UNITED STATES COURT OF APPEALS
FOR THE AMES CIRCUIT

UNITED STATES OF AMERICA	
v.	Docket No. 16-1005
PAPAYA CELLULAR, INC.	

Before Jenkins, Michael, and McFarland, Circuit Judges.

OPINION OF THE COURT BY JUDGE McFARLAND:

This case implicates weighty issues concerning technology, privacy, and national security. Following a series of terrorist attacks in Ames, the federal government received an anonymous tip linking a suspect to the crimes and indicating that future acts of violence were planned. To investigate those allegations and determine whether the suspect was in the vicinity of the attacks at the relevant times, the government sought to obtain data known as historical cell site information from the suspect's cellular telephone service provider, Papaya Cellular, Inc. ("Papaya"). The district court initially granted an ex parte order directing Papaya to release those records under 18 U.S.C. § 2703(d) ("Order"). Papaya then filed a motion to quash, arguing that compliance with the Order would constitute an "undue burden" within the meaning of Section 2703(d) and would violate the Fourth Amendment by permitting the government to obtain the cell site records without a warrant supported by probable cause. The district court agreed on both counts and granted Papaya's motion to quash. The government has appealed.[1]

This is a close and difficult case, and we recognize that there are reasonable arguments on both sides. But we cannot permit shortcuts around the statute or the Constitution, even in

[1] Although the government's Section 2703(d) application and the district court's order were initially sealed, the parties have subsequently agreed on appropriate redactions to permit the public filing of all district court documents relevant to this appeal.

perilous times. We conclude that, on the facts of this case, an order requiring Papaya to release the cell site records would constitute an undue burden under Section 2703(d) and, alternatively, would violate the Fourth Amendment. We accordingly affirm the district court's decision to grant Papaya's motion to quash.

I.

On October 31, 2015, residents of Ames suffered the first of three deadly terrorist attacks when a bomb exploded at Beats Night Club in Ames City, Ames, during a packed Halloween celebration. Fourteen individuals were killed and dozens more were injured in the attack. A group calling itself Redemption, which expressed sympathy with "homegrown" terrorist organizations, took responsibility for the attack and threatened additional acts of violence within Ames. On December 27, 2015, Redemption attacked again by placing a bomb at Blades, an ice skating rink in Clarksville, Ames. Six people were killed in the Sunday afternoon attack, including three children. Finally, on March 8, 2016, a bomb exploded during the annual science fair at White Pine Middle School in Harristown, Ames. Seven individuals were killed in that attack, including three students, two faculty members, and the school principal, Joan Fry. Redemption again claimed responsibility for the attack.

Several days after the attack at White Pine, investigators for the Federal Bureau of Investigation ("FBI") received an anonymous tip from a person who claimed to have knowledge regarding the attacks. The tipster identified an individual, whom the parties refer to as "John Doe" in their briefs because his name is redacted in public filings, as a member of Redemption and possibly the person who placed the bomb at one or more of the crime scenes. The tipster further stated that Redemption intended to commit additional attacks, including one that would threaten young children. FBI investigators took the tipster's allegations seriously because he

provided details about the Beats bombing which had not been publicized and which investigators believed would be known only to those with inside knowledge of the attack.

In response to the tip, the government filed a sealed application under the Stored Communications Act ("SCA") for an order directing Doe's cellular telephone service provider, Papaya, to disclose information, including cell site location records, pursuant to 18 U.S.C. § 2703(c)(1)(B) and (d). As one court has explained, "[c]ell phones work by communicating with cell-sites operated by cell-phone service providers." *In re Matter of Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011). "Each cell-site operates at a certain location and covers a certain range of distances," and "[i]f a user's cell phone has communicated with a particular cell-site, this strongly suggests that the user has physically been within the particular cell-site's geographical range." *Ibid.* By obtaining historical records of which cell sites a subscriber's phone has communicated with, the government may ascertain the subscriber's physical location at various points in time. *See ibid.*

Section 2703(c)(1)(B) states that "[a] governmental entity may require a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communication)" if the government "obtains a court order for such disclosure under subsection (d) of this section." 18 U.S.C. § 2703(c)(1)(B). Section 2703(d) states that a court shall issue such an order "if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that" the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The statute further provides that "[a] court issuing such 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." *Ibid.*

Like other service providers, Papaya keeps records of its subscribers' cell site location data. Unlike other providers, however, Papaya uses proprietary encryption technology to aggregate that information for each cell site, such that Papaya's records do not disclose each individual subscriber's location data. The government's application accordingly sought a court order directing Papaya to disaggregate Doe's records from other subscribers' records. Compliance with such an order, the parties agree, would require Papaya to write software to override its encryption technology and extract Doe's individual data from the aggregate records.

On March 18, 2016 the district court granted the government's application and issued an order requiring Papaya to disclose Doe's cell site location information for the six-month period spanning September 14, 2015, to March 14, 2016. The court further directed Papaya to take technologically feasible steps to disaggregate Doe's records to comply with the Order. The court required the government to reimburse Papaya for the reasonable costs associated with developing the software necessary to comply.

Papaya promptly moved to quash the Order under Section 2703(d). Papaya contended that compliance with the Order would constitute an undue burden by requiring it to write software at odds with its privacy-oriented business model. Alternatively, Papaya contended that provision of Doe's disaggregated cell site location data would violate the Fourth Amendment because it would constitute a warrantless search without a showing of probable cause.

On April 4, 2016, the district court granted Papaya's motion to quash, agreeing that compliance with the Order would constitute an undue burden and would violate the Fourth Amendment. The government now appeals, contending that the district court was wrong on both

counts and that Papaya should be required to comply with the Order. In light of the national security concerns at stake, we ordered expedited briefing and argument in the case. We now issue this decision affirming the district court's decision to quash the Order.

II.

The first issue the parties dispute is whether the Order's directive that Papaya write software to extract Doe's cell site location information from its aggregated records would subject Papaya to an "undue burden" within the meaning of Section 2703(d). The parties disagree on the proper legal standard to apply to adjudicate a claim that an order under Section 2703(d) creates an undue burden, and they further disagree regarding what kinds of burdens are cognizable under that provision. We have found very little case law addressing this issue under Section 2703(d), but courts have considered similar issues in somewhat analogous contexts, including under the All Writs Act ("AWA"). *See, e.g.*, *United States v. New York Telephone Co.*, 434 U.S. 159, 172 (1977) (observing that a court exercising its authority under the AWA may not impose "unreasonable burdens" on parties subject to an order). Applying that case law here, we are persuaded that Papaya would face an undue burden.

Three considerations compel our conclusion that requiring Papaya to write software to comply with the Order would be unduly burdensome. First, Papaya aggressively markets itself as a company committed to protecting user privacy. Indeed, that privacy-oriented business model prompted Papaya to develop encryption technology to aggregate its customers' data in the first place. In our view, an Order requiring Papaya to undermine its own technology and contradict its central business focus constitutes an undue 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 (E.D.N.Y. 2014) (citing company's concern with "tarnish[ing] [its] brand" in

concluding that order requiring it to bypass security features on its device would be unreasonably burdensome).

Second, although the government emphasizes that Papaya could comply with the Order with a minimal investment of resources and that it will be fully reimbursed for its efforts, we are concerned about the burdens Papaya would face if it were routinely subjected to orders like the one at issue here. We see no reason why we should not consider the potential cumulative burden, and we are persuaded that it could quickly become unreasonable. *See id.* at 370 (considering possible cumulative burden on company).

Third, an Order requiring a company to write software is different in kind from other types of discovery orders because the creation of software is an expressive activity entitled to First Amendment protection. *See, e.g., Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001). The Order thus may be viewed as compelling speech, which passes constitutional muster only if it is narrowly tailored to a compelling state interest. *See Turner Broad. Sys. v. FCC*, 512 U.S. 622, 662 (1994). The First Amendment concerns raised by the Order fortify our conclusion that Papaya would be subject to an undue burden.

For these reasons, we conclude that the district court was right to grant Papaya's motion to quash under Section 2703(d).

III.

Even if Papaya would not face an undue burden in complying with the Order, we hold in the alternative that the disclosure of Doe's cell site location information would violate the Fourth Amendment.[2] The Fourth Amendment protects "[t]he right of the people to be secure in their

[2] The government has not argued that Papaya lacks prudential standing to raise a Fourth Amendment argument on Doe's behalf, and we therefore deem any such argument waived. We note that the government's ex parte filing prevented Doe from asserting his own Fourth Amendment rights and that lower courts have considered whether an

persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. The Supreme Court has recognized that "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). If the government engages in such a search, it generally must obtain a warrant supported by probable cause. In this case, the government seeks to obtain cell site location data without a warrant pursuant to Section 2703(d). We therefore must determine whether that action would constitute a search and, if so, whether it would be unreasonable.

Invoking the so-called third-party doctrine, the government maintains that obtaining the data would not constitute a search because individuals do not have an expectation of privacy in location records created by their cellular telephone providers in the ordinary course of business. Under the third-party doctrine, individuals do not have a reasonable expectation of privacy in information that they voluntarily turn over to a third party because, by "revealing [their] affairs to another," they "take the risk . . . that the information will be conveyed by [the third party] to the Government." *United States v. Miller*, 425 U.S. 435, 443 (1976); *see also Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). Several of our sister circuits have relied on the third-party doctrine to conclude that the government does not violate the Fourth Amendment when it obtains historical cell site location data from a service provider without a warrant. *See United States v. Graham*, 2016 WL 3068018, at *1-*2 (4th Cir. May 31, 2016) (en banc); *United States v. Carpenter*, 819 F.3d 880, 887-89 (6th Cir. 2016); *United States v. Davis*, 785 F.3d 498, 511-13

---

order to disclose historical cell site information under Section 2703(d) violates the Fourth Amendment even when the subscriber is not a party to the proceedings. See, *e.g.*, *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 605-15 (5th Cir. 2013).

(11th Cir. 2015) (en banc); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013).

In our view, however, cell phone subscribers do not "voluntarily" share their location information in the manner contemplated by the third-party doctrine. The concept of voluntary conveyance requires that an individual know that he is "communicating particular information" and that he "act[] in some way to submit the particular information that he kn[ows]." *Graham*, 2016 WL 3068018, at *16 (Wynn, J., concurring in the judgment and dissenting in part). That standard is not satisfied here. While some subscribers may know that their phones generate location information (at least if they happen to read Papaya's privacy policy), they are unlikely to know the particular information they are conveying—that is, which cell sites their activity is routed through. Nor are they actively *choosing* to convey this information to Papaya; rather the information is automatically generated when they use their phones and sometimes even without their participation, such as when they receive a call but do not answer. *See id.* at *18-*19. We therefore agree with the Third Circuit that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 313 (3d Cir. 2010).

Because we conclude that the third-party doctrine does not apply here, we must consider whether the Order permitting the government to obtain six months of cell site location data without a showing of probable cause would constitute an unreasonable search. We believe that it would based on the quality and quantity of the information sought. Although cell site location data currently is not as precise as, for example, GPS tracking information, it still discloses a substantial amount about a person's movements. The data sought here therefore could "enable

the Government to ascertain, more or less at will, [Doe's] political and religious beliefs, sexual habits, and so on." *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). As cell site technology changes, moreover, location data may become increasingly more granular—possibly covering "a very specific area, such as one floor of a building, the waiting room of an office, or a single home." *In re Application for Telephone Information Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015); *see Kyllo*, 533 U.S. at 36 (observing that the Fourth Amendment inquiry "must take account of more sophisticated systems that are already in use or in development"). The intrusion on privacy is further intensified by the sheer volume of data sought. In light of the frequency with which cell site location data is generated, it is possible that Papaya's records could contain thousands—if not tens of thousands—of data points about Doe's location over the six-month period covered by the Order. By obtaining that information, the government would intrude on reasonable expectations of privacy. And because that search would be warrantless, we conclude that it would violate the Fourth Amendment.

IV.

For the reasons stated above, the judgment of the District Court quashing the Order is

AFFIRMED

DISSENTING OPINION BY MICHAEL, J.:

In my view, the District Court was right when it initially issued the Order requiring Papaya to disclose Doe's historical cell site location data and to take technologically feasible steps to comply. The Order did not subject Papaya to an undue burden or violate the Fourth Amendment. I would therefore deny Papaya's motion to quash.

I.

The majority commits four critical errors in concluding that Papaya would face an undue burden if it were required to comply with the Order. First, the majority places weight on alleged burdens that are not cognizable under the statute, including a company's interest in maintaining its users' privacy. I would hold that Section 2703(d) focuses only on the direct costs of compliance—that is, *financial* burdens. Any other rule would permit a company to evade its duty to comply with lawful court orders simply by marketing itself as providing privacy protections that make it infeasible to aid ongoing governmental investigations. Here, Papaya would not have to divert significant resources to comply with the Order, and the government must reimburse it for its reasonable expenses. On those facts, no unreasonable burden can be found. *See United States v. New York Telephone Co.*, 434 U.S. 159, 175 (1977).

Second, the majority concludes that it may consider the possible *future* burden on Papaya in complying with *other* orders in determining that the Order here imposes an undue burden. I do not think the speculative burdens threatened by unrelated orders should factor into the analysis. *See id.* at 165 n.6, 174 (recognizing that the company would likely be "subjected to similar orders in the future," but considering only the costs associated with the particular order at issue in the case).

Third, the majority suggests that an order requiring a company to write software is materially different from other types of orders that require third parties to provide information to the government to assist with ongoing criminal investigations. But there is nothing particularly novel about requiring a company to create code, produce unencrypted records, or assist in accessing a cell phone's files. *See, e.g.*, *In re Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc'n over Telephone Facilities*, 616 F.2d 1122, 1126-29 (9th Cir.

1980); *In re Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone*, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1135, 1137 (D. Colo. 2012). Nor does the order raise any issue under the First Amendment. The compelled-speech doctrine is inapplicable to the "essential operations of government," such as "in the case of compulsion to give evidence in court." *West Virginia Bd. of Educ. v. Barnette*, 319 U.S. 624, 645 (1943) (Murphy, J., concurring). In any event, to the extent creation of the software would include expressive elements, Papaya may express whatever it wants. The Order is concerned only with the software's functionality—not its message. Viewed in that light, the Order compels conduct, not speech. *See Rumsfeld v. Forum for Academic & Institutional Rights, Inc.*, 547 U.S. 47, 62 (2006).

Finally, the majority does not give any consideration to the government's weighty interest in obtaining Doe's cell site location data. In measuring whether a burden is "undue," it is appropriate to consider context. This is not an ordinary criminal investigation, but rather an investigation into a truly extraordinary series of terrorist attacks, which have claimed 27 innocent lives, injured dozens of additional individuals, and devastated Ames. Moreover, the government is facing a credible threat that another attack could occur in the near future. Granting the government's application therefore could truly be a matter of life and death. Under these circumstances, the burden imposed on Papaya cannot properly be characterized as unreasonable.

II.

The majority also takes a wrong turn in concluding that the Order would violate the Fourth Amendment by permitting a warrantless search. That conclusion is foreclosed by the third-party doctrine, which establishes that the Fourth Amendment grants no protection to

information voluntarily disclosed to a third party. Under that doctrine, subscribers have no reasonable expectation of privacy in cell site location data because they voluntarily disclose that information to their service providers. The majority has no authority to overturn or limit the third-party doctrine; that power rests with the Supreme Court alone.

The majority's analysis further ignores that the statutory scheme at issue here provides proper protection to privacy interests by distinguishing between the contents of communications and non-content material. See 18 U.S.C. 2703(c)(1)(B) (authorizing the mechanism for the government to obtain records that do "not includ[e] the contents of communications"). The government does not seek to obtain the expressions, thoughts, or ideas Doe communicated using his phone; rather, it seeks only the routing information used to convey those expressions, thoughts, and ideas. And that routing information is ultimately found in business records that are entitled to no greater privacy protections than the address and postmark on an envelope.

Even if some novel Fourth Amendment interest were recognized in this context, I would find a warrantless search permissible by "balanc[ing] the privacy-related and law enforcement-related concerns." *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) (internal quotation marks omitted). Because a subscriber does not own, possess, or create the business records at issue here, any expectation of privacy he has in them is diminished. On the other side of the balance, the government has a compelling interest in obtaining cell site records under the mechanism established by Section 2703(d), rather than by obtaining a warrant. I would therefore conclude that "a traditional balancing of interests amply supports the reasonableness of the § 2703(d) order at issue here." *United States v. Davis*, 785 F.3d 498, 518 (11th Cir. 2015) (en banc).

For these reasons, I respectfully dissent.

FILED: June 4, 2016

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF AMES

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d) REQUIRING PAPAYA CELLULAR, INC. TO DISCLOSE HISTORICAL CELL SITE INFORMATION	Misc. No. _____ **Filed Under Seal** **[Public Redacted Version]**

APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(D) REQUIRING PAPAYA CELLULAR, INC. TO DISCLOSE HISTORICAL CELL SITE INFORMATION

The United States of America, by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an order pursuant to 18 U.S.C. § 2703(d) requiring Papaya Cellular, Inc., a cellular telephone service provider located in Ames City, Ames, to disclose certain records pertaining to the cellular telephone described in Attachment A to this Application ("Target Device"), which has been assigned call number [**REDACTED]**. The records to be disclosed are described in Attachment B to this Application. In support of this Application, the United States asserts:

BACKGROUND

1. Papaya Cellular, Inc. ("Papaya") is a provider of electronic communication service, as defined in 18 U.S.C. § 2510(15). The United States may therefore use a court order issued under 18 U.S.C. 2703(d) to require Papaya to disclose the items described in Attachment B, as those records pertain to a subscriber of electronic communications service and are not the contents of communications. *See* 18 U.S.C. § 2703(c)(1).

2. This Court has jurisdiction to issue the proposed Order because it is a "court of competent jurisdiction," as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically, the Court is a district court of the United States that has jurisdiction over the terrorism-related offenses being investigated. *See* 18 U.S.C. § 2711(d)(3)(A)(i). Additionally, the Court is a district in which Papaya is located or in which the items described in Attachment B are stored. *See* 18 U.S.C. § 2711(3)(A)(ii).

3. A court order under Section 2703(d) "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought . . . are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). This application therefore sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records described in Attachment B are relevant and material to an ongoing terrorism investigation.

FACTS

4. The United States is investigating three terrorist attacks that occurred in various cities in Ames between October 2015 and March 2016. Specifically, the United States is investigating the bombing of Beats Night Club on October 31, 2015; the bombing of Blades Ice Rink on December 27, 2015; and the bombing of White Pine Middle School on March 8, 2016. A total of 27 individuals were killed in the attacks, and dozens more were injured. The investigation concerns possible violations of first-degree murder, in violation of 18 U.S.C. §§ 1111 & 1114 and 18 U.S.C. § 2(a) & (b); conspiracy to use a weapon of mass destruction, in violation of 18 U.S.C. § 2332a and 18 U.S.C. § 2(a) & (b); use of a weapon of mass destruction, in violation of 18 U.S.C. § 2332a and 18 U.S.C. § 2(a) & (b); and destruction by explosives in violation of 18 U.S.C. § 844(f) and 18 U.S.C. § 2(a) & (b); as well as other terrorism-related offenses.

5. The first terrorist attack occurred at Beats Night Club in Ames City, Ames, on October 31, 2015. Beats was hosting its annual Halloween party and the club was packed. Fourteen people were killed in the attack and more than 40 other individuals were rushed to the hospital with serious medical conditions.

6. The day after the Beats attack, a group calling itself "Redemption" took responsibility for the bomb. Redemption released a video to a major media outlet, explaining that it had been inspired by other "homegrown" acts of domestic terrorism. In the video, Redemption threatened additional acts of terrorism and stated that it planned to target children and other young people.

6. On December 27, 2015, a second bomb exploded at Blades Ice Rink in Clarksville, Ames. The skating rink was particularly crowded that Sunday afternoon because schools were on break for the winter holidays. Six people were killed in the attack, including three children under the age of 10. The bomb used at Blades was designed in a similar fashion and used similar materials to the bomb used at Beats. Redemption again took responsibility for the attack and stated that additional acts of terrorism would occur.

7. On March 8, 2016 a third bomb exploded at White Pine Middle School in Harristown, Ames. The school was hosting a science fair in the cafeteria, which was full of students with their projects, parents, and faculty. The bomb went off at the beginning of the event, when principal Joan Fry was making remarks on stage welcoming everyone to the school. Seven individuals were killed in the attack, including three children, three faculty members, and Principal Fry. In addition, 37 individuals were taken to the hospital and treated for injuries related to the attack. Two individuals remain in critical condition at the hospital. The bomb used at White Pine was designed in a similar fashion and used similar materials to the bombs

used at Beats and Blades. Redemption again took responsibility for the attack and stated that additional acts of terrorism would occur.

8. On March 11, 2016, the Federal Bureau of Investigation (FBI) received an anonymous tip on a phone line it had established for members of the public to report any information relevant to the investigation into the bombings. The person providing the tip stated that he had information regarding the bombings. Specifically, he stated that [**REDACTED**] ("Suspect") is a member of Redemption and may have been responsible for placing at least one of the bombs described above. The person providing the tip further offered details regarding the Beats bombing, including that [**REDACTED**]. That information had not been reported in the media, was not publicly known, and, upon information and belief, would only have been known to individuals with some inside knowledge of the terrorist attack. The FBI Special Agents assigned to investigate the tip believed the information it contained was credible.

9. After receiving the tip, the FBI ascertained that the Suspect uses the Target Device and subscribes to Papaya's services. The government now seeks to obtain the records associated with the Target Device listed in Attachment B. Those records are relevant and material to the investigation into the bombings because, among other things, they would reveal location data that could help to confirm the Suspect's location during the bombings. The information may also show where the Suspect may have traveled to and from before and after the bombings, which could reveal pertinent information about the Suspect's and others' involvement in the deadly attacks. Thus, obtaining the records could aid efforts to identify all of the individuals responsible for the terrorist attacks to bring them to justice and prevent future acts of violence.

10. The FBI is in possession of information suggesting that an additional attack by Redemption may occur in the near future. Specifically, [**REDACTED**]. Obtaining records

associated with the Target Device would therefore aid the investigation into a possible future terrorist attack.

REQUEST FOR ORDER

11. The facts set forth above demonstrate that there are reasonable grounds to believe that the records and other information described in Attachment B are relevant and material to an ongoing criminal investigation. Specifically, those items will help the United States to identify and locate the individuals who are responsible for the events described above, and to determine the nature and scope of those individuals' criminal activity. In addition, those items may help to prevent a future terrorist attack.

12. The United States further requests that the order require that Papaya disaggregate the Suspect's records from its other subscribers' information. Papaya uses proprietary encryption software to automatically aggregate its subscribers' cell site location records and strip all identifying information from it. Upon information and belief, Papaya has the exclusive technological means to write software to extract the Suspect's individual data from its aggregate records. The United States agrees to compensate Papaya for its reasonable expenses in complying with an order to disaggregate the Suspect's records.

13. The United States further requests that the order require that Papaya not notify any person, including the Suspect, of the existence of the order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service . . . to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.* In this case, such an order would be appropriate because the requested order relates to an ongoing criminal investigation

that is not known to the Suspect, and its disclosure may alert the Suspect and other targets of the investigation to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the order would jeopardize the investigation.

14. The United States further requests that the Court order that this Application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is not known to the Suspect or other targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may jeopardize the investigation.

Respectfully submitted,

GINA A. ALLEN
UNITED STATE ATTORNEY

Jermaine Plank

Jermaine Plank
Assistant U.S. Attorney

ATTACHMENT A

The cellular telephone ("Target Device") that is the subject of this Application is made by [**REDACTED**] and is model number [**REDACTED**], with IMSI number [**REDACTED**]. It has been assigned the call number [**REDACTED]**.

ATTACHMENT B

The United States seeks the following records from Papaya for the Target Device described in Attachment A for the period beginning September 14, 2015, to and including March 14, 2016:

1. Names (including subscriber names and user names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and any e-mail addresses associated with the Target Device);

3. Length of service (including start date) and types of service utilized;

4. Means and source of payment for such service (including any credit card or bank account number) and billing records.

5. All records (not including the contents of communications) relating to electronic communications sent from or received by the Target Device while it is being actively used to make or receive calls, send or receive texts, access web sites, or use applications that require the use of cellular data, including the date and time of the communication, the method of communication, and the source and destination of the communication, as well as information regarding the cell towers and sectors through which the communication was sent or received.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF AMES

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d) REQUIRING PAPAYA CELLULAR, INC. TO DISCLOSE HISTORICAL CELL SITE INFORMATION	Misc. No. 16-109 **Filed Under Seal** **[Public Redacted Version]**

ORDER PURSUANT TO 18 U.S.C. § 2703(d) REQUIRING PAPAYA CELLULAR, INC. TO DISCLOSE HISTORICAL CELL SITE INFORMATION

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Papaya Cellular, Inc. ("Papaya"), an electronic communications service provider located in Ames City, Ames, to disclose records and other information associated with the cellular telephone that is made by [**REDACTED**], is model number [**REDACTED**], is assigned the IMSI number [**REDACTED**], and has been assigned to call number [**REDACTED]** ("Target Device").

The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation.

The Court determines that there is reason to believe that notification of the existence of this Order will jeopardize the ongoing investigation, including by giving targets an opportunity to tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5).

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2703(d), that Papaya shall, within 14 days of the date of this Order, disclose to the United States the following records and information associated with the Target Device:

1. Names (including subscriber names and user names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and any e-mail addresses associated with the Target Device);

3. Length of service (including start date) and types of service utilized;

4. Means and source of payment for such service (including any credit card or bank account number) and billing records;

5. All records (not including the contents of communications) relating to electronic communications sent from or received by the Target Device while it is being actively used to make or receive calls, send or receive texts, access web sites, or use applications that require the use of cellular data, including the date and time of the communications, the method of communication, and the source and destination of the communications, as well as information regarding the cell towers and sectors through which the communications were sent or received ("Cell Site Location Information").

IT IS FURTHER ORDERED that Papaya shall take technologically feasible steps to disaggregate Cell Site Location Information for the Target Device from other subscribers' data, including writing software to extract that data. The United States shall reimburse Papaya for the reasonable expenses associated with compliance with this aspect of the Court's Order.

IT IS FURTHER ORDERED under 18 U.S.C. § 2705(b) that Papaya shall not disclose the existence of the Application of the United States, or the existence of this Order, to the subscriber who uses the Target Device, or to any other person, unless and until otherwise authorized to do so by the Court, except that Papaya may disclose this Order to an attorney for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the Application and this Order are sealed until otherwise ordered by the Court.

Dated: March 18, 2016

E. Gideon Ellison

United States District Court
For the District of Ames

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF AMES

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d) REQUIRING PAPAYA CELLULAR, INC. TO DISCLOSE HISTORICAL CELL SITE INFORMATION	Misc. No. 16-109 **Filed Under Seal** **[Public Redacted Version]**

PAPAYA CELLULAR, INC.'S MOTION TO QUASH ORDER

Papaya Cellular, Inc. ("Papaya"), by and through its counsel of record, hereby files this Motion to Quash this Court's Order, dated March 18, 2016, requiring Papaya to disclose certain records pursuant to 18 U.S.C. § 2703(d), and further requiring Papaya to write software to override its own encryption technology to enable such disclosure.

This Court should grant the motion to quash because compliance with the aspect of the Order requiring Papaya to disaggregate one individual subscriber's historical cell site location information will subject Papaya to an "undue burden" within the meaning of 18 U.S.C. § 2703(d). Specifically, compliance with the Order will: (1) require Papaya to destroy its business model by invading privacy that Papaya has promised to its customers; (2) risk compromising privacy more broadly by compelling the creation of software that could then be used to avoid Papaya's encryption technology in other circumstances; and (3) violate Papaya's First Amendment right not to engage in the expressive act of writing software.

Alternatively, the Court should grant the motion to quash because the Order violates the Fourth Amendment by permitting the government to conduct an unreasonable, warrantless search without probable cause.

This Motion is based upon a memorandum of points of authorities, as well as the attached declarations of Eric T. Thornton, Juliet Cray, Anna Kelp, and Raphael Stevens; all other records of the case; and such further evidence and argument as the Court may permit.

Respectfully submitted,

Allison James

Dated: March 25, 2016

Allison James
Counsel for Papaya Cellular, Inc.

DECLARATION OF ERIC T. THORNTON

I, Eric T. Thornton, declare as follows:

1. I am over the age of 18 and am competent and authorized to make this declaration. I have personal knowledge of the facts set forth herein, except as to any facts set forth upon information and belief. As to those facts, I believe them to be true. If called as a witness, I would and could testify to the statements and facts contained herein, all of which are true and accurate to the best of my knowledge and belief.

2. I am the founder and Chief Executive Officer ("CEO") of Papaya Cellular, Inc. ("Papaya"). I founded Papaya in June 2008 and have served as CEO from that date to the present.

3. In my role as Papaya's CEO, I am responsible for strategic oversight, including developing and managing the company's business model. From the beginning, I have sought to distinguish Papaya from its competitors by prioritizing user privacy. I recognized that cellular telephone technology posed tremendous potential, but also a grave threat to privacy because it could reveal the most intimate details of an individual's life, from the contents of his contacts directory to which web sites he visits to his location at any given moment. At Papaya, we have designed our service to give subscribers the convenience of cellular technology without asking them to sacrifice their privacy in exchange.

4. More specifically, Papaya has invested in a vast infrastructure of cell sites. That infrastructure allows us to provide reliable service throughout the country without relying on our competitors' networks. We are unique in the industry in that we do not have roaming agreements with other carriers and do not use their networks. That allows us to maintain control of our subscribers' private information. It also eliminates the need to keep individualized records to account for roaming charges.

5. A subscriber who uses Papaya's services generates a substantial amount of location data, which we believe creates significant privacy concerns. For business reasons, we need to keep records of cell site usage. Those records enable us to track the volume of activity at each site, preserve our network's integrity, and monitor the quality of the service we are providing. We rely on that data to, among other things, choose new locations for cell sites and diagnose and repair service-related issues.

7. Although we have business-related reasons to track aggregate subscriber activity at each cell site, we have no need for individualized subscriber data. We believe that collecting that data intrudes on privacy interests and so runs counter to the guiding principles of our business. Accordingly, we have developed proprietary encryption software, which aggregates all subscriber information for a particular cell site and strips it of identifying information that could be used to track the movements, habits, or personal lives of our subscribers.

8. We advertise our commitment to user privacy because it sets us apart from our competitors. Our company slogan is "Prioritizing Privacy." Our focus on privacy has enhanced

our brand and permits us to market ourselves to subscribers who appreciate our commitment to privacy. To provide an example of our marketing strategy, attached as Exhibit A to this Declaration is a true and correct copy of one of our print advertisements, which appeared in the Ames Gazette on April 27, 2015.

9. Our privacy policy memorializes our pledge to our subscribers to protect their privacy. The policy informs subscribers that we collect information about their location, but further describes our encryption technology, which eliminates identifying information from our records. Attached as Exhibit B to this Declaration is a true and correct copy of relevant excerpts of our privacy policy, which was in effect during the time covered by the Court's order dated March 18, 2016 ("Order").

10. Compliance with the Court's Order would strike a devastating blow to our company. It would require us to override our own encryption software, disclose detailed location data that we vowed would remain private, and open the door to future court-ordered privacy breaches. Disclosure in compliance with the Court's Order would run counter to everything Papaya has stood for since I founded the company.

11. Based on the information detailed above, it is my sincere belief that compliance with the Court's Order would cause Papaya to suffer an undue burden.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 24th day of March 2016 in Ames City, Ames.

By: Eric T. Thornton

Eric T. Thornton
Chief Executive Officer of Papaya Cellular, Inc.

Exhibit A to Thornton Declaration

Papaya Cellular
** Prioritizing Privacy **

Clear calls, reliable service, and, always our priority, protecting your privacy.

Whether you communicate by text or by call, through an app or by surfing the web, your communications are yours — and we respect your privacy. Privacy of your communications *and* your location.

Our cell towers connect your calls, but, unlike our competitors, we do not seek to obtain individualized data about your location or usage. Instead, when you use our services, our proprietary software immediately encrypts your data and strips it of individualized information so that our records contain only aggregate data from all our subscribers. That lets Papaya know the total usage of a tower so that we can provide you with the best service—and fewer dropped calls——while protecting your privacy.

With Papaya Cellular, Your Privacy Comes First

Exhibit B to Thornton Declaration

Papaya Cellular, Inc. Privacy Policy — Relevant Excerpts

Our Policy — A General Overview

At Papaya Cellular, we take your privacy seriously. Because your privacy is our priority, this policy explains how information is generated from your use of our services and how we protect that information. This policy applies to your use of all products, services, and web sites offered by Papaya Cellular.

Our Privacy Promises

We pledge to:

- Keep your personal information safe. We use appropriate security controls to protect your information on our system.

- Keep your personal information within your control. We never sell your information to anyone at any time for any reason. Ever.

- Keep your personal information private. Your information belongs to *you*.

Information Collection And Usage

Whenever you do something like make or receive a call, send or receive a text, or access a web site, that activity creates digital information. We need to collect that information to ensure the integrity of our network, prevent fraud, and address technical and security issues. But we have no need to view or analyze your personal data, and we recognize that you may wish to keep that information private. Here is a summary of the information we collect and how we use that information:

- Information about your account: this information includes your name, address, telephone number, e-mail address, and service-related information. We use this information to provide service to you, send you bills for that service, and respond to any questions you have about our service.

- Information about your location. 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. However, we use proprietary encryption software to aggregate that information with data generated by other subscribers. That means we don't maintain records of your individual movements.

- Information about web browsing and TV viewing. Your wireless device generates information about the websites you visit and the programs you watch and record

when you use our networks. We collect this information to make informed marketing decisions and to ensure we are providing our subscribers with relevant advertising. However, we use proprietary encryption software to aggregate that information with data generated by other subscribers. That means we don't keep records of your individual usage and activity on our network.

Sharing Your Information

We do not share your information with third parties except in the following circumstances:

- To enforce our contractual agreement with you and our property rights.
- To obtain payment for our services from delinquent accounts.
- To comply with court orders that have been obtained in accordance with all relevant laws, including the Constitution.

DECLARATION OF JULIET CRAY

I, Juliet Cray, declare as follows:

1. I am over the age of 18 and am competent and authorized to make this declaration. I have personal knowledge of the facts set forth herein, except as to any facts set forth upon information and belief. As to those facts, I believe them to be true. If called as a witness, I would and could testify to the statements and facts contained herein, all of which are true and accurate to the best of my knowledge and belief.

2. I have worked at Papaya Cellular, Inc. ("Papaya") for more than seven years. I am currently the Director of User Privacy at Papaya, and I have served in that capacity for the past five years. In that role, I have primary responsibility for the privacy features of Papaya's products and services. In particular, I work to maintain and improve our proprietary encryption software, which automatically aggregates our subscribers' location and usage data and strips our records of information that can be used to identify individual subscribers.

3. I attended Ames University, where I obtained a B.S. and an M.S. in Computer Science. I have spent my entire professional life focusing on software engineering, with a particular focus on privacy and security.

4. As I understand it, the Court's Order dated March 18, 2016 ("Order") requires that Papaya create software to override our encryption technology and disaggregate one individual subscriber's location data from our records, which currently contain that information only in an aggregated form. To the extent Papaya is required to create that software, I will likely have responsibility for planning and executing the project.

5. To my knowledge, Papaya has never attempted to override its encryption software and extract the data for an individual subscriber. Accordingly, it is difficult to know exactly how long such a project would take and what resources it would entail. With that said, I estimate that the design, creation, and implementation of the software necessitated by the Order would require that a team of three engineers work for three to six days. The team would likely include me, a second software engineer, and a quality assurance engineer.

6. The first step in the process would be to design and create the software. Papaya does not currently possess software than can extract data for an individual subscriber from our aggregated data files. In creating such a program, we would need to tailor the software to the target cellular device so that it can be used only to extract data regarding that device. We would also need to code features that prevent the software from being easily adapted to other devices. I estimate that this step would take one to three days.

7. Next, we would need to run the newly created software through our quality assurance process. During this stage, we would identify and fix any bugs, as well as test the security features we have built into the program. I estimate that this stage would take one to two days.

8. Finally, after we run the program and extract the data, we would need to attempt to eradicate the software from our system. It is difficult to irretrievably destroy something in the digital world. And even if it were possible to fully remove all traces of the software from Papaya's servers, the individuals who created the software would have knowledge of the program's design, coding, and debugging. I estimate that eradication efforts would take one day, with no guarantee that the effort would be fully successful.

9. The burdens associated with complying with the Order would increase exponentially if Papaya faces similar requests in the future. Because Papaya would comply with the Order by writing software for the particular target device and would then act to eradicate any record of that software, Papaya would have to follow the steps listed above every time it received a new request for cell site location data. If Papaya received regular requests for such data, it would constitute a substantial drain on company resources. The other option would be for Papaya to write software that can be used to disaggregate *any* individual user's data. Maintaining custody of such software would pose a significant threat to privacy and the integrity of Papaya's encryption technology. We do not consider this a viable option.

10. Based on the information detailed above, it is my sincere belief that compliance with the Court's Order would cause Papaya to suffer an undue burden.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 24th day of March 2016 in Ames City, Ames.

By: *Juliet Cray*

Juliet Cray
Director of User Privacy

DECLARATION OF ANNA KELP

I, Anna Kelp, declare as follows:

1. I am over the age of 18 and am competent and authorized to make this declaration. I have personal knowledge of the facts set forth herein, except as to any facts set forth upon information and belief. As to those facts, I believe them to be true. If called as a witness, I would and could testify to the statements and facts contained herein, all of which are true and accurate to the best of my knowledge and belief.

2. I have worked at Papaya Cellular, Inc. ("Papaya") since May 2013. I am currently the Lead Software Engineer in the Strategic Growth group. My primary responsibility in that role is to design and create software that keeps pace with evolving technology.

3. I consider writing software to be a creative endeavor. Each person approaches the task of writing code in her own unique way. I tend to map out a complete design for a program before I begin the actual coding process, so that I have my blueprint ready to go before I write my first line of code. But some of my colleagues follow a very different process. One colleague starts writing code early on and lets the design of the program evolve with the code itself. Another colleague begins with a list of features and uses that sketch as a guide for the program as a whole.

4. There are any number of creative choices to be made while writing code. To begin, the programmer needs to choose her language. I tend to gravitate to C++; some of my colleagues prefer to code in Python or Java; and yet other colleagues like to code in other languages. From there, the programmer makes expressive choices about how to manipulate data, what vocabulary to use in the process, and how to construct a user interface.

5. There are many ways to code to achieve different functions. I pride myself on writing elegant, logical code. It is an iterative process and I am constantly revising, refining, and improving my code until I am satisfied with the final product.

6. For these reasons, I consider writing software to be an extremely creative and expressive activity.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 24th day of March 2016 in Ames City, Ames.

By: *Anna Kelp*

Anna Kelp
Lead Software Engineer, Strategic Growth

DECLARATION OF RAPHAEL STEVENS

I, Raphael Stevens, declare as follows:

1. I am over the age of 18 and am competent and authorized to make this declaration. I have personal knowledge of the facts set forth herein, except as to any facts set forth upon information and belief. As to those facts, I believe them to be true. If called as a witness, I would and could testify to the statements and facts contained herein, all of which are true and accurate to the best of my knowledge and belief.

2. I have worked at Papaya Cellular, Inc. ("Papaya") since January 2010. I am currently the Chief Cell Site Manager. My primary responsibility in that role is to coordinate Papaya's acquisition and maintenance of cell sites.

3. Papaya maintains a comprehensive network of cell sites. In rural areas, our cell towers are spaced farther apart, with an average coverage range of approximately 3.5 miles. In urban environments, our cell sites are placed much closer together, with each cell site covering a range of .5 mile or less. Our closest cell sites are located in dense urban areas and cover an area of approximately one block.

4. I have reviewed our cell sites surrounding the locations of the three bombings that occurred in Ames between October 2015 and March 2016. In the area around Beat Night Club in Ames City, Ames, our cell sites are closer together and cover a range of approximately three blocks. In the area around Blades Ice Rink in Clarksville, Ames, our cell sites cover a range of approximately .75 miles. In the area around White Pine Middle School in Harristown, Ames, our cell sites cover a range of approximately one mile.

5. Cell site location information is generated any time a subscriber uses his telephone to make or receive a call, send or receive a text, or use any application requiring the use of cellular data. Each time a subscriber uses his phone for one of these purposes, the phone must establish a connection with a nearby cell site. I would estimate than an average cell phone user generates at least 100 connections per day. Each of those connections is recorded (although aggregated by our system) and so can reveal information about the subscriber's location at the time of the connection.

6. To provide the best possible service, our network sends a signal to the satellite receiver of our subscribers' phones every 7 minutes to ascertain the location of the phone for the proper routing of incoming calls. This process is known as "pinging." We do not currently keep records of the location data generated by pinging but it would theoretically be possible to keep such records.

7. Papaya is not yet making use of smaller cell site technology, such as microcells, picocells, and femtocells. We are exploring that technology, however, and anticipate possibly using it in the future as we grow our network.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 24th day of March 2016 in Ames City, Ames.

By: *Raphael Stevens*

Raphael Stevens
Chief Cell Site Manager

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF AMES

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d) REQUIRING PAPAYA CELLULAR, INC. TO DISCLOSE HISTORICAL CELL SITE INFORMATION	Misc. No. 16-109 **Filed Under Seal** **[Public Redacted Version]**

JOINT STIPULATION

The United States of America and Papaya Cellular, Inc. ("Papaya") hereby stipulate that, for the purpose of Papaya's motion to quash only, the following facts may be taken as true.

1. Papaya is a provider of electronic communication service within the meaning of the Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B).

2. Papaya employs over 650 individuals.

3. Papaya retains cell site location data only in an aggregate form that is stripped of information that can be used to tie that data to an individual phone number.

4. Papaya does not currently possess technology that would permit it to disaggregate an individual subscriber's location data.

5. It is technologically feasible to create software that would disaggregate an individual subscriber's location data from the records Papaya has maintained. Papaya has the exclusive technological means to create that software, which requires knowledge of Papaya's proprietary encryption technology.

6. Creating software to extract an individual subscriber's information from Papaya's aggregate records and then taking steps to eradicate the software would likely take a team of three engineers three to six days.

Agreed this 29th day of March, 2016

Jermaine Plank
Assistant U.S. Attorney

Allison James
Attorney for Papaya Cellular, Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF AMES

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d) REQUIRING PAPAYA CELLULAR, INC. TO DISCLOSE HISTORICAL CELL SITE INFORMATION	Misc. No. 16-109 **Filed Under Seal** **[Public Redacted Version]**

ORDER GRANTING PAPAYA CELLULAR, INC.'S MOTION TO QUASH

Before the Court is a Motion to Quash filed by Papaya Cellular, Inc. ("Papaya"), which asks this Court to quash an order dated March 18, 2016 ("Order"), requiring Papaya to disclose certain records pursuant to 18 U.S.C. § 2703(d), and further requiring Papaya to take technologically feasible steps to comply, including writing software to override its encryption technology. Having considered the motion, the case law, and the record, the Court concludes that the motion should be granted because compliance with the Order would subject Papaya to an undue burden within the meaning of Section 2703(d) and, alternatively, because the government's procurement of the records would amount to a warrantless search in violation of the Fourth Amendment.

Accordingly, Papaya's Motion to Quash is **GRANTED**. The clerk is directed to issue an appropriate judgment and to close the docket of this case.

Dated: April 4, 2016

E. Gideon Ellison
United States District Court
For the District of Ames

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF AMES

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d) REQUIRING PAPAYA CELLULAR, INC. TO DISCLOSE HISTORICAL CELL SITE INFORMATION	Misc. No. 16-109 **Filed Under Seal** **[Public Redacted Version]**

NOTICE OF APPEAL

The United States of America hereby gives notice that it is appealing the judgment entered on April 4, 2016 in the above-captioned matter to the United States Court of Appeals for the Ames Circuit.

Respectfully submitted,

The United States of America

By: *Jermaine Plank*

Jermaine Plank
Assistant U.S. Attorney

Dated: April 6, 2016