

Bench Memorandum

Constitutional Law Debate 1

2017-18

4th Amendment

Summary of the Case

The fact pattern was written to resemble the facts of the 2014 Supreme Court decision, *Riley v. California*, in which the Court ruled that *police officers must generally secure a warrant before conducting a search of data on a cell phone*. The fact pattern for our case, *Manmuna v. United States*, is sufficiently distinct from the facts in *Riley* to raise an arguable question as to whether *Riley* controls, and to provide a legal analysis of a broader issue as to whether cloud data may be searched by law enforcement without a warrant, as the federal Stored Communications Act allows for emails at least 180 days old. The court in *Riley* provides dicta relevant to cloud email privacy, but does not directly address this issue on the Stored Communications Act.

In *Riley*, suspects Riley and Wurie were lawfully arrested and law enforcement seized their cell phones without a warrant pursuant to the “search incident to lawful arrest” exception to the Fourth Amendment warrant requirement. Officers then searched photos, videos, call histories, and contacts to gain additional evidence. The Supreme Court held that the search of this data on the cell phones without a warrant violated the Fourth Amendment (law enforcement can seize a cell phone incident to lawful arrest, but not search through the data on the phone).

In *Manmuna*, law enforcement lawfully arrested Mr. Manmuna and seized his iPhone incident to lawful arrest. However, they did not search through data stored on his phone. They noticed that his Safari internet browser was open and logged into a Gmail account. Officers then obtained a court order under the Stored Communications Act (SCA) and retrieved Mr. Manmuna’s emails from Google. The SCA allows search of an individual’s emails held by a third party for more than 180 days by law enforcement with “specific and articulable facts 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.” This standard is easier to satisfy than the probable cause standard needed for a warrant of “a reasonable basis for believing that a crime may have been committed (for arrest) or there is a reasonable basis for believing that evidence of the crime is present in the place to be searched.”

Federal law enforcement used evidence discovered in Mr. Manmuna’s emails to convict him in federal District Court under the Chemical Weapons Convention Implementation Act. Manmuna appealed the decision to the United States Court of Appeals, District of Columbia, claiming that the search of his emails under the Stored Communications Act was

a violation of his Fourth Amendment rights. The Court of Appeals upheld the conviction. Mr. Manmuna then appealed the case to the United States Supreme Court.

Petitioner attorneys represent Mr. Manmuna. Petitioners will argue that the search of Mr. Manmuna's Gmail emails without a warrant constituted a violation of his Fourth Amendment right against unreasonable searches and seizures, and that his conviction should thus be overturned. Petitioners will also argue that the Stored Communications Act, 18 United States Code § 2701, violates the Fourth Amendment's prohibition against unreasonable searches and seizures in that it allows the search of emails 180 days old or older without a warrant.

Respondents are attorneys for the United States Department of Justice, and will argue that the search of Mr. Manmuna's emails did not violate his Fourth Amendment right against unreasonable searches and seizures, and thus his conviction should be upheld. Respondents will argue that the Stored Communications Act, 18 United States Code § 2701, does not violate the Fourth Amendment, because there is a lesser expectation of privacy by those using email which is stored by a "third party" such as Google, and thus a warrant is not necessary to search emails that are 180 days old or older.

Outline of Written and Oral Arguments

The following is a possible outline of NJ LEEP student debaters' arguments. There may be other iterations of strong argument outlines, but such logical flow should cover all the points mentioned below. (See page 23 of the NJ LEEP 2017-18 Debate manual for a legal argument flow chart.)

I. WERE MANMUNA'S FOURTH AMENDMENT RIGHTS VIOLATED?

- A. Was the search of Mr. Manmuna's emails incident to arrest reasonable without a warrant?
 - 1. Was the search necessary to preserve evidence?
 - 2. Was the search necessary to protect law enforcement safety?
- B. Does the search of Mr. Manmuna's emails fall under another exception to the warrant requirement?
- C. Did Manmuna have a privacy interest in his 180 day-old emails?
 - 1. Did he have an expectation of privacy?
 - 2. Was his expectation of privacy reasonable?
 - 3. Does the nature of cloud data effect his privacy interest?

(Note that this argument (I.C) can also be the first argument made above. Moreover, much of this line of reasoning may overlap with the public policy argument.)

II. IS THE STORED COMMUNICATIONS ACT CONSTITUTIONAL?

- A. Does a reasonable person have a privacy interest in which a warrant should be required in emails 180 days old or older?

1. How is the court order standard lower than the probable cause standard needed for a warrant?
 2. Apply 1., 2., and 3. of I.C above, to a general reasonable person in society.
- B. Public Policy (the public policy section can support the Manmuna individual right issue, and will definitely support the SCA issue).
1. What would the effect be on society in general if the SCA remains constitutional?
 2. What is the effect of the ubiquity of internet, cell phones, and cloud data on our lives? Should we expect privacy? Why or why not? What will be the effect of such expectation?

Cases and Materials For Debate Competition

There are four case excerpts included in the debate manual for this debate competition (pages 68-86). Students should compare and contrast cases, and included mention of all four cases in their written brief and oral argument. In addition, there is a law review article excerpt on page 45-47 that students may reference in their written and oral arguments if they desire. The following are summaries of the four case excerpts provided.

I. *Riley v. California*, 134 S.Ct. 2473 (2014) (see above for factual overview)

The court held that officers must generally secure a warrant before conducting a search of cell phone data.

Petitioners: Should pay attention to the reasoning of the Court’s argument as well as the holding. In addition to arguing that the facts of *Riley* and *Manmuna* are analogous, petitioners may want to use the Court’s reasoning to argue for broad Fourth Amendment protection of all cloud data.

Respondents: The Court opinion contains a great deal of language about the privacy concerns with cell phones. Respondents should pay close attention to the factual differences between this case and the *Manmuna* case. Respondents may want to argue to limit the holding of *Riley* to its facts and make a policy argument that all cloud data should not be protected by the Fourth Amendment?

II. *United States v. Graham*, 846 F. Supp. 2d 384, United States District Court for the District of Maryland (2012)

Federal authorities obtained a court order under the Stored Communications Act to retrieve cell tower (cell site) locations for suspects. The court held that “the Defendants in this case do not have a legitimate expectation of privacy in the historical cell site location records acquired by the government” and “that the Stored Communications Acts, as drafted, provides adequate privacy protections for historical cell site location data.”

Petitioners: This case re-affirms the “Third-Party Doctrine” which states there is no reasonable expectation of privacy in information voluntarily turned over to a third party. It also affirms the constitutionality of the Stored Communications Act. Petitioners may either argue that *Riley* overrules this case, or that the facts are distinguishable. What information does cell tower site location data reveal? Is there a difference between this information and the information police collected in the cloud emails in the *Manmunma* case?

Respondents: Can make an argument that *Riley* does not overrule this case. Respondents can potentially argue that the cell site location data from this case is similar to, or analogous to, the email information collected in the *Manmunma* case. Respondents will want to emphasize the continued constitutional validity of the Stored Communications Act, and the lower expectation of privacy for information voluntarily surrendered to a third party.

III. *United States v. Antoine Jones*, 132 S. Ct. 945 (2012)

The Court held that the installation of a GPS device on an automobile, and the use of that device to monitor vehicle movements, without a warrant, is an unconstitutional search under the Fourth Amendment.

Petitioners: Will try to find a way to show that the search in this case is analogous to and/or similar to the search in the *Manmunma* case to support their argument.

Respondents: Will pay attention to the specific holding of the case, and try to limit the holding to facts that are distinct from the facts in the *Manmunma* case.

IV. *Smith v. Maryland*, 442 U.S. 735 (1979)

The police installed a pen register without a warrant at the phone company to collect phone numbers called by a suspect. The court ruled as follows:

“We therefore conclude that petitioner in all probability entered no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not legitimate. The installation and use of a pen register, consequently, was not a search, and no warrant was required.”

Notes on Matter

I. Exceptions to the warrant requirement

In addition to the search incident to lawful arrest exception to the warrant requirement, respondents may make plausible arguments that the search of the email data in the *Manmunma* case falls under the plain view exception, or under the exigent circumstances exception. Of these arguments, the plain view is the stronger claim.

Plain View: Respondents may claim that law enforcement saw the Google Gmail accounts in plain view because Manmuna had his safari browser open. Unlike in *Riley*, law enforcement did not actively open anything on the phone. Petitioners may reply that the plain view exception does not apply because the actual email content seized was not in plain view.

Exigent Circumstances: Respondents may claim that law enforcement had to retrieve the emails without a warrant because of the threat of terrorist activity by Osiris. Petitioners may respond by arguing that the nexus between Manmuna and any immediate terrorist activity was not strong enough (as then known by any evidence) to warrant an exigent circumstances exception to the warrant requirement.

II. Third-Party Doctrine

Petitioners and respondents should both analyze whether the third-party doctrine should still be constitutionally valid. Consideration of the Third-Party Doctrine may be made as part of the public policy argument, as part of the level of privacy expectation balancing analysis, or both.

III. Use of Fact Pattern

Students should be encouraged to make creative arguments about the factual nuances of the case, but not to argue that any facts not in the materials exist. Thus, students can interpret factual vagaries, but not add facts. For example, students can make reasonable interpretations of exactly what happened to allow Manmuna's safari browser to remain on, and his phone to remain unlocked. They can say Manmuna "may have turned his autolock off, which can be done with an iphone." But students cannot argue, "the police probably just hit the safari app to open the emails, and then told the judge that it was already open."

Sample Questions : Petitioner

1. What case best supports your argument? Why?
2. How do you distinguish this case from *Smith v. Maryland*?
3. How is this case similar to *Riley v. California*?
4. Should the amount of information available on a cell phone come into our 4th Amendment analysis?
5. Mr. Manmuna appears to be a terrorist. Why should we consider his rights when he does not follow the law?
6. Why was Mr. Manmuna's expectation of privacy reasonable when he knew, or should have known, that he was disclosing all sorts of information to third party entities?
7. Is there a difference between information stored on the cloud and information stored on the phone? Why might this difference matter?
8. In *U.S. v. Graham* this court held that the defendant did not have an expectation of privacy in cell-site information. How is that different from the emails in this case?

Sample Questions : Respondent

1. What case best supports your argument? Why?
2. How do you distinguish this case from *Riley v. California*?
3. How is this case similar to *Smith v. Maryland*?
4. Should the amount of information available on a cell phone come into our 4th Amendment analysis?
5. Are you troubled by the actions of law enforcement in this case?
6. Why wasn't Mr. Manmuna's expectation of privacy reasonable? Are most people aware of the third-party doctrine? Doesn't the fact that people believe email to be private mean something?
7. Is there a difference between information stored on the cloud and information stored on the phone? Why might this difference matter?
8. In *U.S. v. Graham* this court held that the defendant did not have an expectation of privacy in cell-site information. How is this case similar?