LORMAN®

Mobile Apps, Texts and More:
Obtaining Them and Getting Them Admitted

Prepared by:
Zachary B. Pyers
Reminger Co. LPA

Published on www.lorman.com - May 2019

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Mobile Apps, Texts, and More: Obtaining Them and Getting Them Admitted

I. Introduction

The first step in effectively conducting discovery in a matter that involves ridesharing is to construct a detailed discovery plan that includes the unique technologies and sources of information involved. This plan should take into account the information that is likely to be available, who has the information, and how that information can be effectively and efficiently obtained. Furthermore, given the new emphasis on proportionally restrictions related to the scope of discovery in the Federal Rules of Civil Procedure, it is also important to be able to explain why information is necessary to building your case.

This paper will address the many types of information that are created and stored through the use of modern technologies, how that information can be accessed—and used to strengthen your case. Conversely, this paper will also address ways of limiting the scope of discovery when opposing counsel seeks more data than they are entitled to. Additionally, the paper will address specific emerging sources of discoverable information and how it can be obtained. Finally, this paper will discuss how to authenticate and admit at trial the information you received from including modern technological sources of information in your discovery plan.

II. Beginning Discovery in a Ridesharing Accident Case

One of the most important aspects of conducting effective discovery in a ridesharing case is having a plan. An interregnal part of putting together a discovery plan and putting that plan into action is a strong understanding of the information available and what entities have access to that information. As with discovery in many other cases, ensuring the preservation of the data or documents you want to access is an important first step. One of the unique aspects of an accident involving a ridesharing driver is that relevant data is nearly always stored in the ridesharing application. Accessing the information from the relevant ridesharing app, as well as other information from

smartphones may prove essential to effective representation in a ridesharing accident case.

A. Using Preservation Letters Effectively

A first step in the litigation of a ridesharing case is to send preservation letters to the relevant parties including the ridesharing driver, or passenger, and the ridesharing coordinator. The practice of making sure that an anti-spoliation/preservation letter is sent as early as possible after a client is retained will increase the information available during discovery or make it easier to seek sanctions if the information is subsequently destroyed. This letter should also carefully consider the scope of what should be preserved, including what time period is relevant to the issues in the case. While much of the information that may be useful is likely stored remotely, there is still a significant likelihood that some data will be stored on the physical smartphone itself, which is why it is crucial to include in a spoliation letter to the driver a request that the smartphone owned at the time of the accident not be destroyed or sold.

When sending an anti-spoliation letter to a ridesharing company, it is important to broadly define the scope of information you are requesting the company retain. Doing this can be useful to rebut any assertion that the company was not on notice of a duty to preserve the information. However, a letter must have some limitations on scope to be meaningful—a letter that asks a company to preserve "everything" could create a basis to argue that the lack of specificity was permission to rely on their own limitations for the scope of the litigation hold.

Below is a sample anti-spoliation letter directed to a ridesharing company, which includes requests to retain the relevant types of information that the ridesharing company may have in its possession following a collision:

Lyber Ridesharing Co.
145 Technology Blvd.
10th Floor
San Francisco, CA 94103

RE: Lyber Driver: John D. Jones
Our Client: Sally P. Person
Date of Injury: April 5, 2018

To Whom It May Concern,

Please be advised our firm has been retained to represent Sally P. Person in relation to her injuries and legal claims arising from a motor vehicle collision that occurred while she was a Lyber passenger. The collision occurred on April 5, 2018 in Someplace, Texas. The police report for this collision is enclosed and it contains additional information about the collision.

Mrs. Person has informed us that your company was previously notified about the collision shortly after it occurred. Accordingly, it is likely that your company has already taken steps to preserve evidence related to this collision. However, in an effort to make certain that this information is being preserved, please accept this letter as formal request to preserve and retain all evidence and information related to this collision, the trip that was occurring prior to the collision, and all information you have regarding your driver, John D. Jones. This request includes all information that Lyber has, and any information or data in the possession of a related entity, such as the Lyber driver, John D. Jones, any subsidiary corporation, or related company that maintains records. If you have any company procedures regarding the time-based automatic destruction of information or data, those policies must be immediately suspended If it is necessary that you forward this letter to other persons or entities, please do so.

The information that this preservation request pertains to includes, but is not limited to:

- Electronic data related to the collision or preceding trip, including GPS data;
- email, messages, or other communications with the Lyber driver or any other party related to the collision or preceding trip;
- information sent to, or recorded by, the Lyber driver's phone or Lyber's system for dispatching and tracking vehicles;
- "black box," electronic data recorder, or similar information stored by a vehicle, smartphone, or other device;

- photographs, video recordings, or audio recordings related to the collision or preceding trip;

- information about the driver and his wireless communication carrier (e.g., Verizon, Sprint, etc.);

- training materials or instructions given to Lyber drivers (including John D. Jones) about what to do in the event of a collision; and

- Lyber's "file" –i.e., the information in Lyber's possession—regarding John D. Jones including all trips in the two weeks preceding the April 5, 2018 collision, all records of complaints or incident reports, and any information retained as a part of any background or driving record check that was performed.

Finally, while I do not anticipate that your company will fail to preserve this information, please be aware that failing to preserve this data and information could result in significant adverse legal consequences. (case from your jurisdiction awarding sanctions for spoliation).

Thank you,

Steve Q. Attorney

Additionally, given that many ridesharing drivers use more than one ridesharing platform, it may be useful to determine if there are any other ridesharing companies that the driver had recently worked for. The other companies could have valuable information related to the driver's recent trips and driving history. Furthermore, both major ridesharing companies, Uber and Lyft, place restrictions on how much a driver is permitted to drive in a given 24-hour period. A driver could potentially skirt the restrictions related to these rules by alternating between using Uber and Lyft. The only way to verify whether this is the case is to seek information from both major companies after a collision.

B. Appropriately Limiting the Scope of Formal Discovery

While smartphones record and store a tremendous amount of information, it is unlikely that the entirety of this information will be relevant to the issues at play in a given case. Recognizing this fact and incorporating it into the discovery plan for a case involving a ridesharing accident can lead to more effective discovery, in terms of both outcome and cost-effectiveness. Specifically, a broad request for "all information and app data" stored on a smartphone is likely to produce an unwinnable discovery dispute, particularly if the case is being litigated in federal court, where the Civil Rules now place a premium on specific and well-articulated requests.

Two cases from Florida show how different approaches to how information is requested can lead to significantly different results when it comes to the discovery of smartphone data. In *Holland v. Barfield*, a wrongful death case arising from an accident, the plaintiff requested production of "any and all computer hard drives" and "all cell phones."[1] The plaintiff claimed that the request was necessary to uncover conversation between the co-defendants, including text messages, Facebook, and myspace messages.[2] In her request for a protective order the defendant argued that such a broad request amounted to a "fishing expedition" and would be an invasion of privacy.[3] The Court agreed and found that there were less intrusive ways to obtain the requested information.[4] Furthermore, the Court took issue with the fact that the request asked for the hardware rather than "the specific information contained therein."[5]

A different outcome was reached in a very similar case, *Antico v. Sindt Trucking*.[6] *Antico* was also a wrongful death case involving a motor vehicle accident but, in this instance, there was a specific allegation that the defendant driver was distracted by her phone immediately before the collision. [7] Based on that allegation, and the fact that the plaintiff's request was limited in time to the day of the crash, the Court allowed the

---

[1] 35 So. 3d 953, 954 (Fla. 5th DCA 2010).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] 148 So. 3d 163, 164 (Fla. 1st DCA 2014).
[7] *Id.*

plaintiff's expert to inspect the defendant driver's phone to review essentially all use of the phone in the time leading up to the collision.[8]

The takeaway from these cases is that while it is easy to see a smartphone as treasure trove of discoverable information, attorneys should use a measured approach in discovery involving this technology and make sure their requests are tailored to information that is likely to be useful and relevant to the issues at hand. Being able to fully articulate why an inspection of an opposing party's smartphone is necessary will make prevailing in a potential discovery dispute far more likely. Finally, courts have shown there are more willing to grant requests that ask for specific information, rather than requests based on sources or locations of information. As an example of how directing requests at specific information is likely to work in practice, compare a request directed at a ridesharing driver that asks for "all data and information related to ridesharing applications" on the driver's smartphone, with a request that is limited to "all data related to trips or fares in the two weeks before the collision." The second versions of this request makes clear what specific information is being requested, which will make it easier to rebut an argument that the request is a mere "fishing expedition."

Conversely, as a party attempting to prevent broad discovery, employing some of the same principles can lead to positive outcomes. Not only will an objection stated with specificity be received more favorably by any court, setting out the specific grounds for an objection is now a requirement in federal court.[9] Additionally, when confronted with a request that is too broad, narrowing the scope of the request and responding to that narrowed request is another helpful tactic that can be used to effectively support an argument against a motion to compel, if one is filed.

III. Obtaining, Authenticating, and Admitting Data from Ridesharing Applications

The prevalence of smartphones and other smart devices has created new legal quandaries regarding how information from an app can be obtained and used. While this

[8] *Id*.
[9] See, FED. R. CIV. P. 34(b)(2)(C).

question had massive implications regarding privacy in the criminal law context, which the Supreme Court will continue addressing in the coming years. The plethora of information that is now available also presents issues in the civil context. Specifically, given how new these forms of information are, there is little precedent to guide how this information can or should be used in the litigation of a civil case. This portion of this paper will examine some of the available case law regarding the authentication of data that is created by the use of an app and which is then stored by the relevant tech company.

At the outset, those seeking to use evidence obtained from a ridesharing application should be mindful of the analysis that comes into play with respect to any piece of evidence. Attorney should ask themselves, is this relevant? Is it substantially more prejudicial than probative? Is there a hearsay issue, or exception that applies? And finally, is this evidence authentic?[10]

Generally, to authenticate data retrieved from an application you must be able to show who the account belongs to, and who created or authored the data you are seeking to authenticate. In the ridesharing context, this will likely involve showing who the driver account belongs to, and that the driver in question was using the app at the time of the crash. The ridesharing company, if they are not already subject to discovery by being a party in a suit, may be helpful in providing the proof necessary to establish who owns an account. While technology companies are generally very reluctant to provide underlying data created from the use of an application in response to a subpoena, on the basis that doing so would violate the Stored Communications Act, these tech companies will provide a certificate of ownership relative to the driver account at issue. The certificate of ownership is analogous to an auto title or property deed and provides a necessary link between the party and the account.

The prevailing standard that applies to admitting social media evidence, known as the Texas standard, is likely to be very similar to the authentication standard that will

[10] Fed. R. Evid. 401, 402, 403, 901, 902.

apply with respect to the authentication of data retrieved from a ridesharing application. Under the Texas standard, extrinsic evidence is needed to authenticate that data retrieved from an account is authentic, most frequently this will take the form of a certificate of ownership and some testimony that either the driver in question was using the app at the time, or even potentially that no other person was known to have access to the app.[11] Thus, the data you are seeking to authenticate must have been created by the person in question.[12] Once the evidence in question has been authenticate, it can be admitted, in a way that is similar to any other document.

IV. Uses of Data Obtained from Ridesharing Applications

As mentioned previously, smartphones, and the applications operating on them, can record and store a tremendous amount of information, some of which may be very useful in helping to establish your theory of how an accident occurred. For instance, by following the information above regarding how to ensure that data from an application is retained, produced, and authenticated, you may be able to present evidence that a driver was using her smartphone at the time an accident occurred. This type of evidence can be used to effectively argue that a crash was caused by the driver being distracted at the time of a collision. Furthermore, if the opposing side learns that you are going to be permitted to discover the information necessary to prove that a driver was distracted, they may be left with no choice but to admit to the distraction and cause of a crash, which could result in a quick and favorable settlement. Additionally, gaining access to a driver's trip history for the time prior to a collision can be useful to prove that the driver may have failed to exercise due care by speeding from one location to the next in order to be able to make more money by taking more fares. Alternatively, a driver's account history could be used to show that the driver had been on the road too long in a given span of time and that the drivers exhaustion played a role in causing a crash. Conversely, when defending a

---

[11] See, *Tienda v. State of Texas*, No. PD-0312-11 (Feb. 8, 2012) (discussing standard applicable to question of whether social media evidence may be presented to the jury).

[12] American Bar Association, *How to get social media evidence admitted to court*, (Nov. 2016), https://www.americanbar.org/publications/youraba/2016/november-2016/how-to-get-social-media-evidence-admitted-to-court.html.

ridesharing driver, this same information can be produced to rebut allegations of distraction or exhaustion, when the facts available support such an assertion.

V. Conclusion.

As with any case, effective use of discovery procedures in the context of a ridesharing matter can make or break a case. To ensure that you are using the tools available to you put your client in the best possible position for settlement talks or an eventual trial, it is necessary to fully consider how the rules of discovery can be best employed in your case. This analysis should include considering the available sources of information, how that information can be obtained, and how that information can ultimately be used to advance your position in a given dispute. Given the mountains of information that smartphones and applications can contain, it is critical that attorneys be able to explain what specific information they are seeking, and why this information is relevant to the issues in a given case. Keeping these requirements in mind will undercut any arguments from opposing counsel that the request to examine a smartphone of ridesharing account is a mere "fishing expedition." While the law surrounding ridesharing is currently developing, keeping these general principles in mind as you work through cases in this emerging field, and pairing the use of these principles with an understanding of the underlying technology will put you and your client in the best possible position.