O'MEARA LEER WAGNER KOHL

Attorneys at Law P.A.

LEGAL ISSUES INVOLVING THE POSSESSION OF TELEMATICS DATA

January 23, 2014

Shamus P. O'Meara
Mark R. Azman
M. Annie Santos
Lance D. Meyer

O'MEARA, LEER, WAGNER & KOHL, P.A.
Relationships ▪ Reliability ▪ Results

7401 Metro Boulevard | Suite 600 | Minneapolis | Minnesota | 55439-3034

LEGAL ISSUES INVOLVING THE POSSESSION OF TELEMATICS DATA

A Paper from
O'MEARA, LEER, WAGNER AND KOHL, P.A.
January 23, 2014

Shamus P. O'Meara
SPOMeara@olwklaw.com
d: 952.806.0438
f: 952.893.8338

Mark R. Azman
MRAzman@olwklaw.com
d: 952.806.0408
f: 952.893.8308

Lance Meyer
LDMeyer@olwklaw.com
d: 952.806.0409
f: 952.893.8309

M. Annie Santos
MASantos@olwklaw.com
d: 952.806.0440
f: 952.893.8340

O'MEARA, LEER, WAGNER & KOHL, P.A.

Legal Issues Involving the Possession of Telematics Data

January 23, 2014

TABLE OF CONTENTS

Section 1

INTRODUCTION

(Return to Table of Contents)

The use of the on-board data recording device is turning 40 this year. In 1974, General Motors installed the first 1000 event data recorders ("EDR") as part of a project conducted by the National Highway Traffic Safety Administration. ("NHTSA")[1] As of model year 2013, the NHTSA estimates that 96 percent of passenger cars and light-duty vehicles have EDR capability,[2] though the NHTSA has proposed a new rule mandating a passenger vehicles under 8500 pounds contain EDRs by September 1, 2014.[3] EDR devices are capable of recording a variety of information, including speed, brake usage just before impact, crash forces, engine throttle, air bag deployment and seat belt usage.[4] Interestingly, as of December 6, 2013, 14 states have enacted legislation providing that EDR data may only be downloaded with the consent of the vehicle owner.[5] Existing NHTSA policy treats EDR data as the property of the vehicle owner.[6]

1 Andrew Askland, Ph.D., *The Double Edged Sword That Is The Event Data Recorder*, 25 Temp.J.Sci.Tech & Envtl. L. 1 (2006).

2 NHTSA 46-10 (December 7, 2012)

3 *See* note 2.

4 *See* note 2; *see also* 49 C.F.R. §563.7 (listing recording guidelines for EDR data elements).

5 http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

6 *See* note 2.

Enter telematics. Telematics is the combination of telecommunications and informatics, and includes global positioning system capabilities. Telematic (or "black box") technologies are broader than EDRs, and include other on-board diagnostic tools, driver behavior devices and tracking devices. Telematics can monitor and collect data on vehicle performance, maintenance cycles, mechanical conditions, fleet management, freight management, driver behavior and performance, speed, miles traveled, vehicle navigation systems, traffic conditions, vehicle emergency systems, among other metrics, and can remotely control certain vehicle systems. Telematics data can be wirelessly transmitted between the vehicle and remote locations for processing and usage. Usage based insurance ("UBI") can be enhanced by the use of self-installed telematics devices to monitor certain data points (e.g., acceleration, miles driven, hard braking, time of day). Insurers use the data to set UBI premium rates based on driving behavior.

This paper discusses the legal implications of telematics data in the context of litigation and human resources, and also discusses several relevant regulations.

Section 2

LITIGATION ISSUES

(Return to Table of Contents)

2.1 Data Management and Preservation Protocols

There is no universal rule of law governing document retention.[7] Common law principles, however, impose obligations to preserve data upon notice of a pending claim.[8] Once a potential claim is known, a company must impose a "litigation hold" in order to preserve data potentially relevant to the claim.[9] Nevertheless, a company will be well served by adopting, following and rigorously enforcing a formal Document Retention Policy.

A Document Retention Policy covers not just paper documents, but also electronic documents and data. Electronic documents and data include emails, spreadsheets, word processing documents (e.g., Word or WordPerfect documents), PDF documents, IMs, text messages, photos, and information/files stored on smartphones. Having a policy, thus, can offer a number of strategic advantages:

7 *But see* 17 C.F.R. § 240.17a-4 (mandating SEC regulated companies retain emails for three years, the first two of which must be in an "easily accessible place.").

8 *See Willis v. Indiana Harbor Steamship Co., LLC*, 790 N.W.2d 177, 184 (Minn. Ct. App. 2010) ("disposal of evidence may be subject to a spoliation sanction when a party knows or should know that the evidence should be preserved for pending or future litigation.").

9 *See, e.g., 3M Innovative Properties Co. v. Tomar Electronics*, 2006 WL 2670038 (D. Minn. Sept. 18, 2006) (indicating a "litigation hold" should have been instigated upon notice of litigation for the purpose of retaining relevant information and materials).

- A business organization generates significant data every day. A good policy will enable the organization to manage information and records for business activities, regulatory, legal and continuity purposes.
- It provides a timetable for the destruction of data. In the absence of a policy, data may be retained that otherwise would be destroyed and that may be harmful to the company's position in future (and unknown) litigation. If a policy was in place, that data would no longer exist.
- Document retention can be expensive and laborious. Retention policies can reduce the expense and scope of the data that must be retained.
- Policies will contain information about the location of documents and data, and identify the positions responsible for data management, making finding data an easier process.
- In the event of litigation, a company's search for data will be limited by the time frame within which data has been retained. Data beyond that time frame will not be available, and thus need not be searched.
- Document retention plans impose uniform retention protocols upon which all employees may rely, and eliminates disparate practices on a company-wide basis. In the event of litigation, it is much better to avoid sanctions by explaining that data was destroyed pursuant to a formal company-adopted document retention policy, than to explain that data was indiscriminately destroyed on an ad-hoc basis. The failure to properly retain data can result in sanctions ranging from an award of attorneys' fees, to unfavorable evidentiary decisions, to adverse inferences, dismissal and default judgment.
- Court rules restrict discoverability to electronic information that is reasonably accessible considering cost and burden. A document retention policy can supply the basis of what is "reasonably accessible" in the event of litigation.
- The policy will include protocols in the implementation of "litigation hold" procedures, which will avoid the need to create such procedures in the midst of pending or threatened litigation.

In sum, the adoption and enforcement of a comprehensive Document Retention Policy promotes prudent corporate governance and can provide significant benefit in the event of litigation.

2.2 Discoverability and Use in Litigation

Before issues of discoverability can be addressed, the obligation to preserve must be

defined. One Court provided the following broad guidance:

> What is the scope of the duty to preserve? Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no'. Such a rule would cripple large corporations . . . that are almost always involved in litigation. As a general rule, then a party need not preserve all backup tapes even when it reasonably anticipates litigation.
>
> At the same time, anyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to the an adversary. While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.

Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (internal quotations and footnotes omitted).

To date, little doubt has been raised as to the admissibility of data from EDRs.[10] The courts have been nearly uniform as to the general acceptance of EDR data and their validity for recording information just prior to an accident.[11]

"Admissibility turns on evidence of authenticity and expert testimony to explain how the machine operates and to interpret" the data.[12] Authentication depends on two elements. First, a description of the system to produce a particular result, and second, evidence showing the system produces an accurate result.[13] The amount of information necessary regarding data input and processing to properly authenticate an output "will

10 *McCormack on Evidence*, §204(B).

11 *Com. v. Zimmerman*, 873 N.E.2d 1215, 1221 (Mass. Ct App. 2007) (cases collected therein).

12 *McCormack*, at §204(B).

13 *See, e.g.*, Minn. R.Evid. 901(b)(9).

depend on the nature and completeness of the data, the complexity of the manipulation, the routineness of the operation, and the verifiability of the result."[14] As to expert testimony, the proffered expert must satisfy three criteria: (1) The witness must qualify as an expert; (2) the expert's opinion must have foundational reliability; [and] (3) the expert testimony must be helpful to the trier of fact."[15] Additional foundation may be required if the computer is performing more complex computations.[16] The hearsay rule may impede admissibility, unless a hearsay exception applies,[17] though some would say that telematics does not fit the definition of hearsay because computer generated materials are not statements by persons.[18]

The use of telematics information in civil proceedings can be significant. The data can be used to support or refute a particular claim or defense. Data may be used to support or rebut air bag malfunctions or other alleged vehicle defects upon which bodily injury claims are premised. Data can be used in the development of accident reconstruction studies which render opinions regarding factors that contributed to the cause of an accident. In this context, opinions may be more objective and reliable because the studies are based on real data that can be corroborated by actual injuries and other data. It is not

14 *McCormack*, at § 227

15 *Doe v. Archdiocese of St. Paul*, 817 N.W.2d 150, 164 (Minn. 2012) (citing Minn. R.Evid. 702); *see also Malith v. Soller*, unpub., 2010 WL 2363621 (Minn. Ct. App. June 15, 2010) (noting trial court's exclusion of expert testimony based on even data recorder information because expert's opinion lacked foundational reliability).

16 *McCormack*, at § 227.

17 *See., e.g.*, Minn.R. Evid. 803(6)(business records).

18 *See, e.g.*, Minn.R. Evid. 801(c)(definition of hearsay).

uncommon for trial attorneys to routinely request EDR data as part of typical discovery demands.

2.3 Risks and Benefits of Possessing Telematics Data

From a litigation standpoint, telematics data can cut either way depending on the facts of the case; the data can support your position or it can refute your position. Collateral attacks may be available (e.g., as to reliability of the data or the context within which the data is applied), but if it exists, the data must nevertheless be dealt with. Outside of the litigation arena, telematics can be used for a variety of business purposes to increase fleet management efficiency and control costs, but there are drawbacks from an employee's perception of privacy and the "Big Brother" effect. These concerns will require a balancing of mutual objectives for driver and public safety, driver privacy, compliance with federal regulations, fleet efficiency and cost control, and litigation.

Overall, the usefulness of telematics data appears to outweigh the risks of possessing the data.

Section 3

HUMAN RESOURCES

(Return to Table of Contents)

3.1 Employer Use of Data

Employers' use of telematics continues to increase as an efficient means of tracking how company resources are used. In addition to using telematics to monitor and collect data on vehicle performance, maintenance cycles, mechanical conditions, fleet management, freight management, speed, miles traveled, vehicle navigation systems, traffic conditions, vehicle emergency systems, among other metrics, telematics can be used as a human resources tool, including as a means of measuring driver performance and improving the health of a business, among other things.

Telematics is about improving the health of a company. It is in the best interests of all employees when their employer is profitable. The healthier a company is financially, the more secure employees feel and the better position the employer is in to offer improved pay and other benefits. Telematics is about helping mobile employees work smarter, providing valuable insights into working more efficiently, and allocating resources more effectively.

Telematics can also be used to measure employees' performance and train employees. Employers can use telematics to create measurable goals and incentives for their employees. Offering bonuses for productivity or efficiency gains is easier when there

is an objective way to measure an employee's performance. On the other side, having objective data that may be used to support a disciplinary action against an employee for failing to meet required benchmarks or other conduct in violation of an employer's policy, helps in substantiating disciplinary decisions. Data gathered through the use of telematics can also be used to train employees in areas where there appears to be a general deficiency or for purposes of behavior-based safety training, which can reinforce good driving habits and draw attention to driving that puts the driver at risk of a collision. Employers can set impartial performance metrics and goals for improvement, emphasizing telematics behavior-based safety as a reward not a punishment.

3.2 Employee Privacy

The use of telematics is, by its very nature, often seen by employees as a technology that is highly intrusive, an infringement upon their right to privacy, and Big Brother-esque. This need not be the case, however. Introducing telematics that may include tracking of employee data should be a transparent process, involving dialogue between employer and employees. Telematics should be seen by both employer and employees as a positive step, which can help increase productivity, reduce costs, improve customer service, ensure driver safety, and ultimately be used to the benefit of the employer, employee, and customer.

Laws vary by state, and employers who consider using telematics devices to track their fleets should understand all regulations within their business coverage territories. When developing policies to track and monitor employees, fleet managers should consult local laws and regulations.

In using telematics data, employers should consider their employees' privacy rights as defined by the Minnesota Legislature, including the Minnesota Privacy of Communications Act, Minnesota Statutes § 626A.01 et seq., privacy implications in Minnesota's employment statutes, Minnesota Statutes § 181.01 et seq., the Minnesota Government Data Practices Act, Minnesota Statutes § 13.01 et seq., and Minnesota common law. Limitations imposed by federal statutes and regulations should also be considered, including the Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Parts 160 and 164.

The collection and use of telematics data has the potential to result in an invasion of an employee's privacy. In the context of Minnesota common law, "invasion of privacy" is a term for several tort claims based on violations of an individual's privacy rights, whether within the employment context or not. The Restatement (Second) of Torts identifies and outlines four separate causes of action that qualify as invasion of privacy: (1) intrusion upon seclusion; (2) appropriation; (3) publication of private facts; and (4) false light publicity. Minnesota law, however, only recognizes three of these four types of invasion of privacy claims: (1) intrusion upon seclusion; (2) appropriation; and (3) publication of private facts. *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998). Minnesota law does not recognize a claim for false light publicity.[19] *Id.* (rejected due to the concern that

19 "False light publicity occurs when one gives publicity to a matter concerning another that places the other before the public in a false light if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed." *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 233 (Minn. 1998).

claims under false light are similar to claims of defamation, and to the extent that false light is more expansive than defamation, tension between this tort and the First Amendment is increased.). The Minnesota Supreme Court recognized the other three invasion-of-privacy claims and described them as follows:

> 1. **Intrusion Upon Seclusion.** Intrusion upon seclusion occurs when one intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or upon his private affairs or concerns if the intrusion would be highly offensive to a reasonable person.
>
> 2. **Appropriation.** Appropriation protects an individual's identity and is committed when one appropriates to his own use or benefit the name or likeness of another.
>
> 3. **Publication of Private Facts.** Publication of private facts is an invasion of privacy when one gives publicity to a matter concerning the private life of another if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.

Id. at 233.

Invasion of privacy claims can arise in the employment context and have the potential to arise when collecting and using telematics. Familiarity with the three types of invasion of privacy claims recognized in Minnesota may help an employer avoid potential liability and manage risk.

Moreover, in order to help ensure a potential violation of privacy laws does not give rise to a cause of action, employers should review their internal procedures and posted policies to ensure that their personnel practices conform to all privacy laws and regulations. Employers should also consider alerting employees that the use of telematics may include or result in employee monitoring and expressly advise employees that they should not have an expectation of privacy while using company property with telematics

capabilities.20 A 2010 D.C. Circuit criminal case – *U.S. v. Maynard* – may herald an invasion of privacy claim based on an employer's use of telematics to track an employee's location 24 hours a day without the employee's knowledge. 615 F.3d 544, 563 (D.C. Cir. 2010), *aff'd in part sub nom. United States v. Jones*, 132 S. Ct. 945, 181 L. Ed. 2d 911 (U.S. 2012). In *Maynard*, the court held that the defendant's reasonable expectation of privacy was violated when the FBI tracked his movements with a GPS device that the FBI had installed on the defendant's vehicle without a warrant. Although not an employment law case, disgruntled employees may cite to it in order to establish their own invasion of privacy claims against employers who monitor employee movements without notice. Thus, if an employer intends to monitor employees while using company property, or the use of telematics results in the monitoring of employees, whether intended or not, then the employer should establish a comprehensive policy defining the circumstances under which monitoring may occur, ensure appropriate dissemination of the policy, and obtain signed acknowledgment/consent from affected employees. An employee's consent to be bound by an employer's policies should remove any expectation of privacy with respect to use of company property with telematics capabilities.

20 Some unions have also raised the issue of the use of telematics to monitor employees in contract negotiations. Generally, however, federal law allows employers to monitor work-related use of telephone, e-mail, and other communications.

Section 4

REGULATIONS

(Return to Table of Contents)

4.0 Introduction:

The commercial trucking industry is one of the most regulated industries in the United States. With federal and state regulations governing everything from driver qualifications and licensing to vehicle inspection, repair, and maintenance, there are certainly a number of regulations that impact the possession of telematics data. But, given the capabilities of fleet management systems and other telematics devices, the data collected by such devices may also aid commercial motor carriers and their drivers in complying with the plethora of regulations governing their every move. Along with the obvious benefits, however, comes a real risk of overregulation.

4.1 FMCSRs Impacting the Possession of Telematics Data:

Because the broad use of fleet management systems and other telematics devices is still relatively new to the interstate trucking industry, there are not yet specific regulations governing the possession of telematics data. But there are several FMCSRs that either directly impact or have the potential to impact the possession of telematics data. These FMCSRs include, but are not limited to, 49 C.F.R. §§ 392.80, .82, which prohibit commercial motor vehicle (CMV) drivers from texting and using hand-held mobile telephones while driving; 49 C.F.R. § 391, which requires motor carriers to maintain driver

qualification files; 49 C.F.R. § 396.3, which requires motor carriers to perform systematic inspections, repairs, and maintenance of its vehicles; and 49 C.F.R. § 395.15, which governs the use of automatic on-board recording devices (AOBRD) to record driver hours of service.

4.1.1 Prohibitions against the Use of Certain In-Cab Electronic Devices:

Since October 27, 2010, the FMCSRs have prohibited CMV drivers from texting while operating in interstate commerce and imposed sanctions for violation of the regulations. Specifically, section 392.80 provides that no driver shall engage in texting while driving and that no motor carrier shall allow or require its drivers to engage in texting while driving. Texting means "manually entering alphanumeric text into, or reading text from, an electronic device. 49. C.F.R. § 383.5. But texting does not include "[u]sing a device capable of performing multiple functions (e.g., fleet management systems, dispatching devices, smart phones, citizens band radios, music players, etc.) for a purpose that is not otherwise prohibited in this part." *Id.* Violation of the texting prohibition can result in fines and penalties for drivers and their employers and/or driver disqualification. *See* 49. C.F.R. §§ 383.51(c); 386, App. B (a)(3), (4); 391.15(e).

Similarly, as of January 3, 2012, the FMCSRs have prohibited CMV drivers from using hand-held mobile telephones while driving. Specifically, section 392.82 provides that no driver shall use a hand-held mobile telephone while driving a CMV and that no motor carrier shall allow or require its drivers to use a hand-held mobile telephone while driving a CMV. To "use a hand-held mobile telephone" means:

(1) Using at least one hand to hold a mobile telephone to conduct a voice

> communication;
>
> (2) Dialing or answering a mobile telephone by pressing more than a single button, or
>
> (3) Reaching for a mobile telephone in a manner that requires a driver to maneuver so that he or she is no longer in a seated driving position, restrained by a seat belt that is installed in accordance with 49 CFR 393.93 and adjusted in accordance with the vehicle manufacturer's instructions.

49 C.F.R. § 390.5. Once again, violation of section 393.82 can result in fines and penalties for drivers and their employers and driver disqualification. *See* 49. C.F.R. §§ 383.51(c); 386, App. B (a)(3), (4); 391.15(e).

Although these prohibitions against texting and using a hand-held mobile telephone while operating a CMV do not directly apply to telematics devices, they likely prohibit the use of such devices in a way "otherwise prohibited" by sections 392.80 and 392.82. Furthermore, such prohibitions are likely only the first step in the FMCSA's attempt to cut down on electronic distractions inside the cab. In comments published along with the final rule prohibiting the use of hand-held mobile telephones, the FMCSA indicated that it "is considering an advance notice of proposed rulemaking to seek public comment on the extent to which regulatory action is needed to address other in-cab electronic devices that may result in distracted driving." *See* Drivers of CMVs: Restricting the Use of Cellular Phones, 76 Fed. Reg. 75470, 75477 (Dec. 2, 2011). The FMCSA has not yet moved forward with this notice of proposed rulemaking, but there is a strong likelihood that the FMCSA will implement additional regulations addressing other electronic devices, including telematics devices, in the near future. It is therefore important for motor carriers to understand the prohibitions currently in place and to monitor changes to the FMCSRs to

ensure that their use of a fleet management system or other telematics device remains in compliance with federal regulations and does not increase the risk of distracted driving.

4.1.2 Maintenance of Driver Qualification Files:

The FMCSRs require a motor carrier to maintain a driver qualification file for each of its drivers that must include, in relevant part, "[a] note relating to the annual review of the driver's driving record as required by § 391.25(c)(2)." 49 C.F.R. § 391.51(b)(5). Section 391.25 requires a motor carrier once a year to "review the motor vehicle record of each driver it employs to determine whether that driver meets minimum requirements for safe driving or is disqualified to drive a commercial motor vehicle pursuant to § 391.15." In doing so, the motor carrier "must consider ***any evidence*** that the driver has violated any applicable [FMCSRs]." And section 391.25(c)(2) requires that a motor carrier maintain a note regarding the review in the driver's qualification file.

In the past, a driver's qualification file may have been limited to records obtained from government agencies and internal records created at the time of hiring, testing, review, and discipline. But now, with the continual collection of telematics data, the scope and extent of information that must be reviewed on an annual basis and noted in a driver's qualification file has expanded exponentially. Through the use of telematics devices, employers can now collect and analyze real-time data regarding speed, braking, acceleration and deceleration, evasive maneuvers, collisions, and other unsafe driving behavior. This data likely falls within the scope of "any evidence that the driver has violated any applicable [FMCSRs]," and therefore motor carriers must it annually and make notes in its drivers' qualification files.

With the increase in the amount of data available to motor carriers regarding the driving behavior of their employees, it also becomes more and more important that motor carriers take appropriate steps to investigate and remedy any issues they become aware of in order to avoid claims of negligent retention, supervision, or entrustment. In other words, motor carriers that use telematics devices to monitor driver conduct likely have an increased obligation to not only review and record information regarding the behavior of their drivers but also to take appropriate steps to address any issues as they arise to avoid liability.

4.1.3 Inspection, Repair, and Maintenance Records:

The FMCSRs also require motor carriers to systematically inspect, repair, and maintain their trucks and to keep records of such inspections, repairs, and maintenance for a period of time. *See* 49 C.F.R. § 396.3. Specifically, section 396.3(a) provides that a motor carrier "must systematically inspect, repair, and maintain, or cause to be systematically inspected, repaired, and maintained, all motor vehicles . . . subject to its control." And section 396.3(b) provides that a motor carrier must "maintain, or cause to be maintained, records for each motor vehicle they control for 30 consecutive days," including the date and nature of any inspection, repairs, and maintenance. As with driver qualification files, the FMCSRs mandating motor carriers to maintain inspection, repair, and maintenance records of likely obligate motor carriers to maintain records of any data collected by a telematics device regarding the inspection, repair, and maintenance of its fleet. And again, because of the increase in the amount of information available, motor carriers must act to address any issues as they arise to avoid liability.

4.1.4 Electronic Recording of Driver Hours of Service:

While the FMCSRs do not yet mandate the use of an electronic recording device to record driver hours of service, the FMCSRs permit the use of Automatic On-Board Recording Devices (AOBRDs) as long as they comply with the requirements of 49 C.F.R. § 395.15. According to section 395.15(a), "[a] motor carrier may require a driver to use an [AOBRD] to record the driver's hours of service." An AOBRD is

> an electric, electronic, electromechanical, or mechanical device capable of recording driver's duty status information accurately and automatically as required by § 395.15. The device must be integrally synchronized with specific operations of the commercial motor vehicle in which it is installed. At a minimum, the device must record engine use, road speed, miles driven, the date, and time of day.

49 C.F.R. § 395.2. But a motor carrier choosing to use an AOBRD to record its drivers' house of service must comply with the specific requirements of section 395.15, which mandate the information that such devices must record and provide guidelines for retention of the information required. Section 395.15 also includes device certification requirements and guidelines for recording driver hours of service in the event a device becomes nonoperational. Finally, section 395.15(j) gives the FMCSA authority to rescind a motor carrier or driver's authority to use an AOBRD to record driver hours of service and to comply with the traditional hours-of-service requirements contained in section 395.8 under certain circumstances.

In April 2010, the FMCSA published a final rule requiring that CMVs operated by motor carriers found by the FMCSA to have serious hours of service compliance issues be equipped with Electronic On-Board Recorders (EOBRs), which are more complex and

have more capabilities than AOBRDs. *See* Electronic On-Board Recorders for Hours-of-Service Compliance, 75 Fed. Reg. 17207, 17210-12 (April 5, 2010). Before it could be implemented, however, the 2010 rule was challenged in court based in part on concerns that motor carriers could use EOBRs to harass drivers. *See Owner-Operators Independent Drivers Association* v. *U.S. Department of Transportation,* 656 F.3d 580 (7th Cir. 2011). In August 2011, the 7th Circuit Court of Appeals vacated the April 2010 final rule based on the FMCSA's failure to address the issue of driver harassment.

In July 2012, Congress stepped in and mandated regulations requiring that all CMVs involved in interstate commerce and operated by drivers who are required to record their hours of service be equipped with "electronic logging devices." *See* Agency Information Collection Activities; Approval of a New Information Collection Request: Driver and Carrier Surveys Related to Electronic Onboard Recorders (EOBRs), and Potential Harassment Deriving From EOBR Use, 78 FR 32001, 32003 (May 28, 2013) (citing MAP-21, Pub. L. 112-141, § 32301(b), 126 Stat. 405, 786-788 [July 6, 2012], amending 49 U.S.C. 31137). As a result, it is inevitable that the majority of interstate motor carriers and their drivers will be required in the near future to use of AOBRDs or EOBRDs to record driver hours of service. And with the new mandate, there will likely be additional regulations regarding the use of such devices to record driver hours of service.

Assuming that the new rule ultimately passed by the FMCSA is substantially similar to the April 2010 final rule, the FMCSRs will most likely require all CMVs manufactured after a certain date, involved in interstate commerce, and operated by drivers

who are required to record their hours of service to be equipped with an EOBR that meets the requirements of the new regulations. Specifically, the EOBR will need to record driver, motor carrier, CMV, and shipping identification information, duty status, date and time, location, distance traveled, 24-hour period starting time, the multiday basis used, and hours in each duty status and total hours. *See* Electronic On-Board Recorders for Hours-of-Service Compliance, 75 Fed. Reg. 17207, 17246 (April 5, 2010). With respect to reporting, the April 2010 final rule required that an EOBR make it possible for officials to immediately check the status of a driver's hours of service, that an EOBR produce a driver's hours-of-service record upon demand, that a driver have in his or her possession records of duty status for the previous 7 consecutive days, and that a driver submit his or her record of duty status to the employing motor carrier within a specified number of days. *See id.* at 17246-47. Finally, the April 2010 final rule imposed certain requirements on motor carriers with respect driver training and supervision and the maintenance of electronic hours-of-service files. Motor carriers can likely expect similar, if not identical, requirements when the new rule is passed.

4.2 Aid of Telematics Data in Complying with FMCSRs:

Although there are several regulations that impact the possession of telematics data, the reality is that telematics devices and the data they collect can also significantly aid motor carriers in complying with key FMCSRs.

For instance, a telematics device that automatically records the required hours-of-service information can significantly aid a motor carrier and its drivers in complying with the FMCSRs and therefore avoiding fines and other significant liability.

According to the FMCSA, a "carrier is liable for violations of the hours of service regulations if it had or should have had the means by which to detect the violations. Liability under the [FMCSRs] does not depend upon actual knowledge of the violations." In other words, "[n]either intent to commit, nor actual knowledge of, a violation is a necessary element of that liability. Carriers 'permit' violations of the hours of service regulations by their employees if they fail to have in place management systems that effectively prevent such violations." As such, it is imperative that motor carriers have systems in place and take other appropriate steps to ensure compliance with hours-of-service regulations.

Telematics devices can also aid motor carriers in maintaining a low Comprehensive Safety Analysis (CSA) safety score. The CSA is a FMCSA program that was rolled out in December 2010 to improve large truck and bus safety and reduce accidents by measuring and evaluating motor carrier safety performance and providing officials the opportunity to intervene where necessary. Each motor carrier's safety performance is evaluated based on the following categories: unsafe driving, hours-of-service compliance, driver fitness, controlled substance and alcohol violations, vehicle maintenance, hazardous materials compliance, and crash information. A motor carrier is then given a safety score from 0 to 100 based on the number of violations or crashes, the severity of violations or crashes, and when the violations or crashes occurred. Given the above categories, a motor carrier could go a long way in controlling its safety score by collecting and evaluating the same information in the ordinary course of its business and intervene where necessary in order to cut down on the violations and crashes that lead to a high CSA safety score.

Although not necessarily a regulatory issue, the data collected by telematics devices can also aid motor carriers in avoiding liability for negligent supervision. By proactively taking steps to become aware of risky driving behavior, motor carriers can take appropriate actions in order to reduce the risk of accidents and thereby avoid liability. Similarly, telematics devices and the data they collect can aid a motor carrier in complying with vehicle inspection requirements by making it easier on both the motor carrier and its drivers to record and maintain inspection information. Along those same lines, telematics devices can assist motor carriers in complying with the FMCSRs regarding the preservation of records, contained in 49 C.F.R. § 379.

4.3 Risks of Over-Regulation:

Notwithstanding the numerous ways in which telematics devices can aid motor carriers in complying with the myriad amount of federal and state regulations, such devices create a potential environment for overregulation. With an ever-increasing amount of real-time data available to motor carriers employing fleet-management systems, there is a real risk that government inspectors will also be granted access to such data and be able to constantly monitor CMV drivers' compliance with CMV regulations. For example, if a telematics system is able to record and transmit real-time hours-of-service, maintenance, and driving behavior data from a CMV to the motor carrier, why can't the same data be transmitted to federal, state, and local enforcement offices at the same time. In sum, given the pushback over the past couple years regarding EOBRs and driver harassment, there is sure to be additional battles in the coming years as fleet management systems become more and more prevalent regarding who has access to telematics data and when.

Section 5

CONCLUSION

(Return to Table of Contents)

The possession of telematics data can involve a variety of issues. Telematics data can improve driver safety, vehicle maintenance and efficiency, and the protection of property. But it also can implicate issues of privacy, appropriate use of telematics data, and the preservation of data.

* * * *

Disclaimer

This paper is provided as a general informational memorandum. It is not legal advice or a solicitation, does not create an attorney-client relationship, and should not be used as a substitute for legal advice. Readers should consult with an attorney concerning specific circumstances.