

# Overloaded with Data?

## TELEMATICS AND THE IMPORTANCE OF A CLEAR TELEMATICS DATA MANAGEMENT POLICY (TDMP) IN THE TRUCKING INDUSTRY

By Heather C. Devine and Tenley R. Pearce, Alexander Holburn Beaudin + Lang LLP



Private Motor Carriers today face an everchanging and expensive demand: how to deal with all the data being generated by ELDs and ever more sophisticated telematics?

This 'data overload' has many implications from creating privacy issues for drivers and carriers to questions of data management and sharing that data with insurers and customers. Proper data management becomes particularly important if litigation arises: there is nothing like the hint of a nuclear verdict to motivate plaintiffs to find the one item that can persuade the jury or tip the settlement in their favour – and where do they look?

**Telematics:** the combination of telecommunications and informatics has given rise to devices that are able to send, receive, and store data. That data can be the source of a defence, or a reason to settle. In some cases, it can lead to catastrophe with damages being awarded in the U.S. that far exceed insurance coverage.

Consequently, we recommend that if you are 'overloaded with data,' you should implement a clear Telematics Data Management Policy or TDMP.

First, we will explain the sources of data that can be available and may require data management which is related to the 'Internet of Things.' Then, we explain the importance of a TDMP and review some of the beneficial inclusions.

### What is the Internet of Things (IoT)?

Our original title was, "When is a truck like a refrigerator?" but we kept getting the answer, "Both can contain beer!"

Instead, our point is that your fridge at home can be a source of data just like a tractor or a trailer – because all are connected to the Internet of Things.

The Internet of Things is a popular term for describing scenarios in which the connectivity of the internet and computing capability of modern devices extends to a variety of everyday items. Essentially, the IoT connects objects from the physical world to the Internet using sensors.<sup>1</sup>

Although the concept of the IoT is relatively new, the concept of combining computers and devices has been around for decades. In the 1970s, systems for monitoring meters on the electrical grid via telephone lines were already in commercial use. By the 1990s, machine-to-machine monitoring had already become widespread.<sup>2</sup> Once everyday devices were combined with internet networks, the possibilities grew exponentially. These days, telematics data is collected by countless personal devices, from your smart watch to your refrigerator.

### How are IoT and Telematics connected?

Nowadays, with the IoT, the applications are endless. They include home controllers and security systems, optimizing equipment use and inventory in factories, accessories such

as watches, and household appliances such as refrigerators and ovens. Using sensors, diagnostic systems, and communication with a network, these common devices can interact with the world around them and store data that is not human-entered.

One significant application of telematics and the IoT is commercial fleet tracking. These telematics devices in commercial vehicles vary from basic systems that meet regulatory electronic logging requirements to complex systems that collect, organize, and report almost infinite amounts of driver and vehicle information. We know that our readers are collecting this data every minute of every day.

### Telematics Data from Vehicles

Using telematics as a method of monitoring is becoming widespread in vehicles generally; however, it began and is still most used for fleet management in trucking companies. The use of telematics is only expected to grow with the newly implemented (June 12, 2021) electronic logging device mandate in Canada.<sup>3</sup>

There are several components used in a telematics device of a truck: on-board diagnostics (OBD), GPS receivers, engine interface, input/output interface, sim card, accelerometer, and a variety of other sensors.<sup>4</sup> Simply put, the sensors, receivers and interfaces retrieve data generated by the usage of the vehicle and send them to the cloud or originating database for storage.

Such data may include location, speed, idling time, harsh acceleration or braking, fuel consumption, hours-of-service, battery voltage, other engine data, and any other potential vehicle faults.<sup>5</sup> Even if a carrier is not actively seeking to collect this data, it is still generated and stored: the issue is how to manage data collection, storage, retention, sharing, and use.

### **The Importance of a Telematics Data Management Policy (TDMP)**

We recommend implementing a TDMP to govern how the significant amount of data collected by telematics devices is stored, protected, and used both within and outside the carrier. Data is only as useful as the carrier's use of it, and the volume of data coming in from an entire fleet can drown out the helpful data points and create areas of significant risk and vulnerability.

### **What Should a Telematics Data Management Policy (TDMP) Include?**

Your TDMP should address data collection, storage (including security), retention, sharing, and usage. A TDMP needs to be clear and specific enough so the drivers in the fleet are aware of and can consent to what personal data is being collected, how this data is stored and kept private, how this data is going to be used, and to whom this data may ultimately be disclosed.<sup>7</sup> The policy details may also be important for third parties such as brokers, shippers, and insurance carriers, as they navigate their own use of telematics data.

#### **1. Collection**

Early consideration and clarification of the type and amount of data collected has multiple benefits. First, it avoids some of the data overload problem by eliminating data that is not useful, to essentially "get rid of the noise."<sup>8</sup> Secondly, limiting your data collection avoids later complaints, if litigation arises and counsel makes a broad discovery request, that not all the data

was considered and/or acted upon prior to the event at issue. In short, only collect data you intend to use.

#### **2. Storage**

A TDMP must address where and how data is stored. Often data will be stored in the cloud via a cloud storage company, to take advantage of the specialized security software, monitoring and technological support these companies offer. It can also be cost effective and is easily scalable.<sup>9</sup> How data is stored depends on regulatory requirements in your operating jurisdiction, as well as the purpose for which you are collecting and storing the data. Regulation may require certain data points, such as hours of service, to be stored in a way that the data is identifiable by driver, while privacy implications (and privacy regulatory frameworks) may suggest other data should be aggregated upon collection and stored for purposes unrelated to individual drivers.<sup>10</sup>

#### **3. Retention**

How long data is stored will depend on the regulatory requirements in the jurisdictions you operate in, the type of data you are collecting, and the use for which you want to put it. It requires a balance between holding onto data too long, which can increase storage costs and potentially create problems with data discovery if litigation arises, and failing to keep data for the statutorily required time periods or data which could help in potential future litigation. Keeping data for five years after collection is a good starting point, but this policy should be tailored to your organization.

Another retention consideration is whether (and when) to delete potentially dangerous or harmful data, such as dangerous driver behaviour or equipment malfunctions. If there is the potential for, or already ongoing, litigation then the data must be retained, or an organization could risk an accusation of deleting data

for the purposes of avoiding disclosure. If there is no litigation potential then the data should be analyzed and used for safety improvements or driver training, and then it may be deleted – but this must be balanced with the considerations of losing potentially helpful safety data in doing so.

#### **4. Sharing Data: Share Reports Only, Not Primary Data**

Drivers and those who produce telematics data will want to know who the data is going to be shared with for privacy reasons, so this should be set out clearly in your TDMP. Regulation often dictates whether drivers must be able to access certain personal data points such as hours of service, so this will depend on your jurisdictional requirements. A general starting point is that drivers requesting non-personal data should only receive summaries.

Other third parties may request data, such as insurance carriers, brokers, and customers/shippers. The TDMP should dictate that these third parties can only receive reports, and typically only upon request. The policy should also detail how much personal information about drivers is available in these reports and seek to limit such disclosure. It is likely third parties will want to set clear limitations, as they similarly do not want to be overloaded with data (discussed further below). Data storage companies may offer options to control parameters third parties can access or set up separate databases to only be accessible by certain parties.

#### **5. Usage**

A TDMP must detail to what use the data is going to be put. This allows drivers to understand and be aware of what their information is being used for, as well as to help clarify any privacy concerns (such as concerns with driver-facing camera video footage). Specifying the use of data in your policy may also assist in litigation by eliminating claims of collected but un-analyzed data if the policy is correctly implemented.

### Availability of a Telematics Data Management Policy (TDMP)

There is no doubt that telematics data can provide valuable insight into productivity and safety in almost every area of freight management. However, collecting data from telematics devices without a plan or policy in place for how to use the data is risky – not only will you be unaware of the data you have collected but random storage without disposal leaves data to be harvested by plaintiff's who seek to establish patterns of unsafe behaviour, for example, to establish that a carrier had a knowing 'disregard' that its operations were unsafe.

Whenever telematics devices are implemented into operations, so should a policy about the data these devices will be gathering.

Since a TDMP will have impacts on drivers, carriers, brokers, insurers, and others, the policy should be designed to be disclosed and followed. It is particularly important to incorporate the TDMP into at least the Carrier Operations Manual and the Driver Manual (for employees and independent contractors) so those whose 'personal' data is generated, collected, and or stored can provide the proper informed consent.

The TDMP should be disclosed, and receipt acknowledged with a record of that acknowledgement stored in the driver's file.

### Data Management & Cybersecurity

The importance of proper data management policies and implementation is also relevant to cybersecurity: with increasingly sophisticated criminals seeking to gain access to data across all industries, it is important to incorporate third party security provisions into one's TDMP.

Cloud-based storage companies, for example, specialize in security and have all the latest software, so it may be wise for a company to transfer the onus for security onto a trusted storage company.<sup>11</sup>

Onboard security in the trucks themselves, such as encryptions and firewalls, is a starting point. However, whenever data is being pulled from the truck and transferred

elsewhere, there is a risk of a data breach. Fleets must protect implement formal third-party cybersecurity provisions, and ensure the security is provided to and by back-office applications which can access telematics data. Finally, carriers must ensure that the storage system and company holding the collected data have verified security in place.

### Use of Telematics Data in Litigation

The most well-known use of commercial vehicle telematics data is in litigation. Plaintiffs seek to mine Telematics Data to document's negligence, a pattern of unsafe operations, or even or a malfunction of the truck itself.

Plaintiffs seek to use telematics data to vilify trucking companies in the eyes of juries in the United States, prompting them to award so-called "nuclear verdicts" (verdicts of \$10M or more which do not correlate with actual losses).<sup>12</sup> This strategy appeals to the jury members' emotional response to alleged unsafe motor carrier safety practices, even if they are entirely unrelated to the subject accident.<sup>13</sup>


The risk of nuclear verdicts further underlies the importance of a TDMP: only collect what you are going to analyze, keep the data stored safely, only store it for as long as you need to, and use it to improve safety so the carrier can counter any negative data by showing a history of safe practices in the event of litigation. One benefit is that in some cases, telematics can provide the carrier with evidence to defend – perhaps to defend to trial or even to settle early where a finding of liability appears certain.

Third parties such as freight brokers should also be wary of overloading on data. Some cases have held brokers liable for the negligence of drivers following findings of an agency relationship where the broker was said to control the driver/carrier's operations in part through the broker's use of telematics data. Thus, third parties will want to avoid significantly relying on telematics to select, evaluate,

or engage with carriers; avoid collecting or holding data or evidence on the carrier's behalf; and clearly define, communicate, and limit what metrics they want to track and which metrics they want to use for carriers to avoid overly controlling, interfering, or monitoring them. This is particularly important for Canadian brokers who deal with cross-border carriers who may be subject to the nuclear verdict phenomenon in the United States.

### Last Word

In conclusion, a good TDMP will answer the following:

Know what to save, how to save it, where to save it, when to use it, how to protect it, to whom to disclose it, and get prior written consent from the driver. 

### Sources

1. Vivek Singhania, "The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World" (2015). *ACADEMIA*, online: [ISOC-IoT-Overview-20151221-en.pdf](https://www.isoc-internet.org/ISOC-IoT-Overview-20151221-en.pdf) ([internetsociety.org](http://internetsociety.org)).
2. *Ibid.*
3. Mitchell Scrimgeour-Brown, "Fuelling change: The next 'big thing' in transportation is telematics" (June 16, 2021), online: [www.insurancebusinessmag.com/ca/news/broker-leadership/fuelling-change-the-next-big-thing-in-transportation-is-telematics-258010.aspx](http://www.insurancebusinessmag.com/ca/news/broker-leadership/fuelling-change-the-next-big-thing-in-transportation-is-telematics-258010.aspx).
4. "What is telematics" (25 March 2021). Online: [www.geotab.com/blog/what-is-telematics](http://www.geotab.com/blog/what-is-telematics).
5. *Ibid.*; Ben Sharpe & Dave Schaller, "Telematics in the Canadian Trucking Industry (December 2019)." Online: [https://theicct.org/sites/default/files/publications/Telematics\\_Canadian\\_trucking\\_industry\\_20191210.pdf](https://theicct.org/sites/default/files/publications/Telematics_Canadian_trucking_industry_20191210.pdf).
6. Scrimgeour-Brown, *supra* note 5.
7. Helen M. Schweitz & Jonathan R. Todd, "Technology and Data Privacy Implications for Driver Relationships" (August 17, 2021). Online: [www.beneschlaw.com/resources/technology-and-data-privacy-implications-for-driver-relationships.html](http://www.beneschlaw.com/resources/technology-and-data-privacy-implications-for-driver-relationships.html).
8. "Pathways to Better Truck Data for Fleets" (April 19, 2018). Online: [www.truckinginfo.com/288128/pathways-to-better-truck-data-for-fleets](http://www.truckinginfo.com/288128/pathways-to-better-truck-data-for-fleets).
9. *Ibid.*
10. Schweitz & Todd, *supra* note 9.
11. "Pathways," *supra* note 10.
12. Eric L. Zalud, "Shutting Down the Texas Roadhouse Verdict Party (in part); the Texas Legislature Takes Aim at Nuclear Verdicts" (August 17, 2021). Online: [www.beneschlaw.com/resources/shutting-down-the-texas-roadhouse-verdict-party-in-part-the-texas-legislature-takes-aim-at-nuclear-verdicts.html](http://www.beneschlaw.com/resources/shutting-down-the-texas-roadhouse-verdict-party-in-part-the-texas-legislature-takes-aim-at-nuclear-verdicts.html).
13. *Ibid.*