Proceed With Caution: Data Collection and Connected Cars

Patrick D. Newman
Tal A. Bakke
Maria P. Brekke
Bassford Remele, P.A.
100 South Fifth Street, Suite 1500
Minneapolis, MN 55402
612.333.3000
www.bassford.com

Keep Right: Data Breaches Have Serious Consequences

Data privacy issues touch almost every facet of modern life, and these issues will only grow as technologies continue to progress.

The biggest data breaches generate huge amounts of negative press and can lead to regulatory headaches and severe monetary penalties. These breaches are not confined to the technology space—they can affect any industry that accesses, uses, or stores consumer data. For example, in 2017, personal data of approximately 147 million people was stolen from Equifax, one of the largest consumer credit reporting agencies in the United States. The breached data included names, addresses, phone numbers, dates of birth, social security numbers, and driver's license numbers. In the aftermath of the breach, Equifax spent over one billion dollars in its response, and the company reached a record-breaking settlement with the Federal Trade Commission (FTC).

Data breaches likewise have impacted the service industry. In 2018, Marriott, one of the largest hotel chains in the world, revealed that it had been the subject of a database breach that may have affected the information of approximately 500 million guests. A particularly troubling aspect of this breach is that the unauthorized access to the affected network had been occurring since 2014, undiscovered until 2018.

Data breaches can have drastic consequences not only for consumers and individuals whose data is stolen, but for the businesses that are subject to a breach as well. In 2019, American Medical Collection Agency (AMCA), a healthcare debt collection agency, filed for Chapter 11 bankruptcy protection following a data breach that affected its online payment page. The breach led to a severe and immediate drop in business—almost all of AMCA's largest clients terminated or substantially limited their involvement with AMCA.

In its 2020 *Cost of a Data Breach Report*, IBM Security stated that the average cost of a data breach in 2020, excluding "mega breaches" of one million records or more, was **$3.86 million**.

<u>Road Work Ahead</u>: Data Privacy Regulations (Existing and Potential) and the Recovery Industry

More and more, motor vehicles are equipped with technology that allows them to access the Internet and gather, store, and transmit data. These technologies provide numerous safety, comfort, and performance benefits, but they also raise privacy and data security concerns.

Some states have already passed laws that may impact the recovery industry. California, New York, and Virginia are three of those states.[1] While the laws of each of these states are unique, broad themes include requirements that businesses:

- destroy consumer records containing personal information when that information is no longer being used by the business;
- notify consumers and regulatory entities following data breaches; and
- implement reasonable safeguards to protect personally identifying information from unlawful use or unauthorized disclosure or access.

Some laws also specifically address the deletion and protection of biometric data and the requirement that businesses delete personally identifying information if a consumer requests that they do so.

Although the United States has not yet enacted a sweeping data privacy law, the European Union adopted the General Data Protection Regulation (GDPR) in 2016. The GDPR went into effect in 2018, and it had a major impact on businesses that collect data from individuals in European Union member states.

In the last two years, several data privacy bills have been introduced in the U.S. Congress, proposing various levels of federal regulation over the collection, use, and storage of data. These bills include the Information Transparency and Personal Data Control Act (ITPDCA), the Consumer Online Privacy Rights Act (COPRA), and the Data Protection Act (DPA), which would establish a new Data Protection Agency charged with protecting individual privacy.

---

[1] **California**: *see, e.g.*, Cal. Civ. Code §§ 1798.81, 1798.81.5, 1798.82, and 1798.81.5.; **New York**: *see, e.g.*, N.Y. Gen. Bus. Law §§ 399-H, 899-AA, 899-BB; *see also* proposed expansion to New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act, S.B. 567, 2021–2022 Reg. Sess. (N.Y. 2021).; **Virginia**: *see, e.g.*, Va. Code § 18.2-186.6; *see also* proposed Virginia Consumer Data Protection Act, S.B. No. 1392, 2021 Sess. (Va. 2021).

The FTC is paying attention to privacy and security concerns specific to technology in motor vehicles. In conjunction with the National Highway Traffic Safety Administration (NHTSA), the FTC held a workshop in 2017 to examine consumer privacy and security issues posed by automated and connected motor vehicles.

Following the workshop, the FTC published staff perspectives on those issues. The publication discusses the **benefits** of collecting this data, such as the collection of precise geolocation data to direct emergency personnel to crash scenes, the use of data to provide diagnostic information about a vehicle's state of health, and the ability of insurance companies to use information to give insurance discounts to consumers who identify good driving habits. The publication also discusses **potential dangers** of this form of data collection, such as the potential for insurance companies to use the information to increase rates without consumer's knowledge, or the undisclosed connection of occupants' real-time location and sale of such information to third parties.

The FTC publication concluded that because there are many different types of data involved, different approaches may be needed for the collection of some data than for other types—for instance, the collection of safety-critical data versus the collection of data generated when a consumer syncs their phone to the car's infotainment system.

In short, regulators across the globe—including those charged with overseeing consumer-facing businesses' compliance with federal law in the United States—are on high alert on the issue of consumer data privacy and security. The recovery industry should be, too.

Pay Attention to the Road Signs: Key Takeaways and Considerations

The past decade has shown rapid advancement in vehicle technology, and privacy and security laws are only now beginning to adapt to those technological changes. Although only time will tell how far future federal data privacy regulations will reach, it is not too soon to begin implementing practices and considering how to protect data. The impact of data breaches and misuse of consumer data can be severe, and these issues affect virtually every modern industry.

The recovery industry should be aware of and pay close attention to existing or potential laws and regulations that require a business to:

- destroy identifying information left on vehicles from previous customers or owners;
- provide notice of a breach if personally identifiable information is accessed by unauthorized third parties; and
- implement reasonable measures to prevent unauthorized access to the information of past drivers contained on vehicles.

The industry should likewise keep the following compliance considerations at top of mind ***now***, irrespective of the current state of the law (because, rest assured, the regulations are coming):

- who in the chain of custody and control should be responsible for deleting consumer information from vehicles;
- what contractual protections should be implemented to mitigate risk (e.g., hold harmless clauses);
- how to properly access and destroy the personally identifying information left on vehicles from previous owners;
- developing measures to prevent unauthorized access to personal information; and
- how to identify and respond to breaches when they do happen.

In sum, instituting proactive measures to stay ahead of the curve is a much more manageable, and less risky, approach to compliance than taking reactionary steps after a regulator or court becomes involved. The recovery industry should watch how current data privacy laws are being applied to other regulated industries to (1) determine what particular concerns the regulators and courts are raising regarding consumer data privacy; and (2) consider what steps can be taken now to address those concerns (before they become regulatory investigations or lawsuits), including any potential technological solutions that may exist.