MEALEY'S™
Data Privacy Law Report

Auto Insurance Telematics Data Privacy And Ownership

by
Frederick J. Pomerantz
Goldberg Segalla
New York, New York

and

Aaron J. Aisen
Goldberg Segalla
Buffalo, N.Y.

A commentary article reprinted from the May 2015 issue of Mealey's Data Privacy Law Report

LexisNexis®

Commentary

Auto Insurance Telematics Data Privacy And Ownership

By
Frederick J. Pomerantz
and
Aaron J. Aisen

[Editor's Note: Frederick J. Pomerantz is a partner in Goldberg Segalla's New York City office, where he focuses his practice on serving the corporate and commercial needs of highly regulated industries. With 30 years' experience representing insurance companies in transactional and related regulatory matters, he also handles the organization and licensure of insurers, reinsurers, and related entities, including producers, risk retention groups, and risk purchasing groups. He is a frequent author and speaker on insurance regulation and other topics, and has published articles in major insurance trade publications in the United States, South America, Asia, and Europe. Aaron J. Aisen is an associate in Goldberg Segalla's Buffalo, NY office. His practice is focused on regulatory matters, banking, global insurance and reinsurance matters, and cyber risk. He writes, contributes, and blogs on cyber risk and a variety of financial and other regulatory issues, and has co-authored papers on cyber risk and cyber insurance for the prestigious Federation of Defense and Corporate Counsel. Any commentary or opinions do not reflect the opinions of Goldberg Segalla or LexisNexis, Mealey's. Copyright © 2015 by Frederick J. Pomerantz and Aaron J. Aisen. Responses are welcome.]

Introduction

Data collection is the new normal in the 21st century. This extends from search engines to social media to consumer shopping habits. This also includes monitoring driving behavior and auto performance. Insurance companies can use vehicle driving data[1] gathered by telematics sensors attached to vehicles to rate automobile insurance policies, while auto dealers can use the same sensors to gather vehicle diagnostic data which is used by dealers for use in servicing customers in diagnosing problems with their vehicles and other related services.

This article analyzes two specific questions relating to the collection of this data through auto insurance telematics devices installed in vehicles sold by automobile manufacturers. First, what state and federal laws and regulations exist at present to protect the drivers' confidential information transmitted to the dealers and the service departments through the telematics devices or otherwise communicated to third parties by automobile manufacturers? Second, who owns the data gathered through auto insurance telematics devices installed in vehicles?

Statutory And Regulatory Environment

As a general rule, the legal environment surrounding the issue of data privacy and ownership is still relatively new and very fluid. For example, with respect to the ownership of data sent to dealers, the question is much easier to answer than the question regarding ownership of telematics data since there is a finite, but evolving (and still inadequate), body of state insurance and state privacy laws which define the categories of protected consumer information. In most instances, the categories of protected consumer information are defined by the statute. Few states define the categories of protected consumer information broadly, but in the context of auto telematics data, the current categories of protected consumer information are inadequate. There is, on the other hand, an evolving body of interpretations under federal law and regulation, including but not limited to the Federal Trade Commission (FTC), which suggest the existence of remedies by consumers where their information is sold to private parties for commercial purposes.

Contrast this to the legislative and regulatory regime regarding the use of telematics by insurance companies.

There is no definitive answer to this question. The law of telematics-data sharing is young and developing and has not kept pace with the realities of the rapidly changing market for automobiles and automobile insurance. Insurers need and want access to a growing database of telematics data to facilitate the setting of premiums for individual drivers and for vehicle diagnostic use; however, arrangements governing how that data is obtained, managed and accessed are likely to change quickly to adapt to new laws and regulations responding to the results of legislators' and regulators' scrutiny of the use of such data. The market for telematics data is growing and there is a strong possibility that in the future telematics data will become central to how insurers set drivers' premiums. Good drivers stand to benefit from the use of telematics data since their premiums will likely fall, even as those of poor drivers rise. However, it is unclear who owns the data gathered through auto insurance telematics devices, although there are hints in the available federal regulations pointing to the consumer as the owner of such information. However, the evidence is far from conclusive at this time and does not permit us to respond definitively to the issue of ownership of vehicle data.

Selected State Statutes Reviewed

In this article, due to space constraints, we focus our analysis primarily on the laws of six selected states: California, Kansas, Missouri, Nebraska, New York, and Texas. We also cite from time to time statutes of certain other states which are particularly relevant or shed light on the prevailing views of state legislators in a majority of states. We also discuss applicable federal laws or regulations where, for completeness of our discussion of the principal issues, those cannot be ignored. We do not, however, focus on the laws regulating the use of credit information in insurance underwriting.

Further, we have searched for U.S. case law on the subject of ownership of telematics data and, significantly, have found only seven decisions, none of which are relevant or responsive to the principal issues or helpful in the analysis.

We attempt to draw general responses to the two principal issues based solely on the laws of the six states selected and the federal legal framework, discussed below, which in any event is inadequate and does not prohibit the activity of automobile manufacturers outlined in the section on "Facts." Before drawing definitive conclusions on the two principal issues, we advise a comprehensive review of all 50 state laws and regulations.

The Origins Of A Legal Framework

Gramm-Leach-Bliley Act (GLB)

GLB requires financial regulators to establish standards for administrative, technical and physical safeguards for the security and confidentiality of customer records and information.[2] Safeguard standards under GLB for insurance providers are a matter of state insurance law, addressed by the applicable state insurance regulators.

National Association Of Insurance Commissioners Model Laws And Regulations

The National Association of Insurance Commissioners, in response to GLB, adopted in 2002 the Standards for Safeguarding Customer Information Model Regulation, 673-1 (NAIC Model), which states, in relevant part, as follows:

> Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities. 673-1, § 3
>
> A licensee's information security program shall be designed to:
>
> A. Ensure the security and confidentiality of customer information;
>
> B. Protect against any anticipated threats or hazards to the security or integrity of the information; and
>
> C. Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer. 673-1, § 4

Not all states have adopted the NAIC Model. Some states have adopted regulations, somewhat different in form and substance, but incorporate the principles stated in the NAIC Model.[3]

Other State Laws: Personally Identifiable Information (PII)

Virtually every state requires persons or organizations possessing PII of their residents to notify them if there is a breach of security regarding PII.[4] Security breach laws typically have provisions regarding who must comply with the laws (e.g., businesses, data/information brokers, government entities, etc.); definitions of "personal information" (e.g., names combined with Social Security numbers, driver's license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (encrypted or otherwise de-identified information).[5] In our review of selected state security breach laws, we have taken note of provisions in several other state statutes that were particularly noteworthy.[6]

Most states affirmatively require reasonable security procedures and practices to protect such PII, and either require a destruction policy or a secure means of disposal for such PII. These laws generally apply to PII in computerized form. However, at least nine states apply some or all of their safeguards and notification requirements to PII in both computerized and hard copy form. Effective encryption of electronic PII is generally a safe harbor for breach notification obligations.[7]

As discussed above, most states define PII as the combination of the resident's name with any information in additional categories, such as the resident's Social Security number, driver's license or state identification number, or financial account or card numbers with account access information, such as security or access codes or PINs.[8]

However, some U.S. jurisdictions add additional categories of combined information to PII, including, but not limited to, medical or health information (e.g., California[9], Missouri[10], and Texas[11]); unique biometric data or DNA profiles (e.g., Nebraska[12] and Texas[13]); birth dates (e.g., Texas[14]); mother's maiden name (e.g., Texas[15]), unique electronic identification numbers (e.g., Texas[16]) and even work-related evaluations (e.g., Puerto Rico[17]).

Missouri defines "medical information" to include "any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a healthcare professional."

Nebraska defines "unique biometric data" to include fingerprint, voice print, and retina or iris image, as well as "any other unique physical representation." This phrase may be interpreted to include at least some fitness- or health-related sensor data.

Texas' statute is triggered by any breach of "sensitive personal information," which includes "information that identifies an individual and relates to: (1) the physical or mental health or condition of the individual." This would protect at least fitness-related sensor data.

Thus, for the vast majority of states, a security breach that resulted in theft of records containing users' names and associated biometric or sensor data would not trigger state data-notification requirements. A breach that only stole sensor data without users' names would also not trigger such laws.

None of the states whose laws we reviewed protect as PII the type of vehicle data that automobile manufacturers gather from insurance telematics. Thus, at least some states do not apply any of their safeguards and notification requirements to vehicle data, which are not therefore considered to be PII for purposes of these states' data security and breach notification laws.[18]

Safe Harbor Under State Security Breach Laws: Encryption And/Or Redaction Of PII

Further, the security breach laws of 40 states and the District of Columbia have an encryption safe harbor. Excerpts from six state laws follow:

California

California's data breach laws are triggered for a person or business that conducts business in California and that owns, licenses, or maintains computerized data that includes personal information "following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[19]

Kansas

Kansas' security breach laws are triggered only by disclosure of unencrypted or unredacted computerized data (or PII) that compromises the security, confidentiality or integrity of such information and that causes, or that an individual has reason to reasonably believe, will cause identity theft to a consumer.

Missouri

Missouri's security breach laws are not triggered by disclosing PII that does not include personal information that is redacted, altered or truncated such that no more than five digits of a Social Security number or the last four digits of a driver's license number, state identification card number or account number is accessible as part of the PII.

Nebraska

Under Nebraska's security breach laws, notice is not required if the PII is encrypted or redacted.

New York

Under New York law, private information is personal information together with one of a number of data elements outlined in the statute that is either not encrypted or encrypted with an encryption key that has also been acquired.

Texas

Under Texas' security breach laws, "sensitive personal information" only applies to data items that are not encrypted.

Some states provide for some level of exemption of the data breach notification requirements if the entity is required to follow some other state and/or federal requirements. For example, some entities that deal with medical records are regulated by a federal law called the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[20] In California, entities governed by HIPAA will be deemed to have complied with applicable state notification requirements[21] if they completely comply with certain applicable provisions of the Health Information Technology for Economic and Clinical Health Act of 1996 (HITECH).[22] Such exceptions do not relieve an individual or a commercial entity from a duty to comply with other requirements of state or federal law regarding the protection and privacy of personal information.

State Laws Regarding Privacy Of Data From Event Data Recorders

Event Data Recorders (EDRs) also known as black boxes or sensing and diagnostic modules capture information such as the speed of a vehicle and the use of a safety belt, in the event of a collision, to help understand how a vehicle's systems performed. EDRs have become standard on most cars, SUVs and light trucks. In the last few years, the data recorded by EDRs has been found to be of tremendous value when analyzing a crash. The National Highway Traffic Safety Administration (NHTSA) ruled in 2012 that commencing with the release of model year 2011 vehicles, all manufacturers must release, by commercial license or other agreement, the hardware and software required to access EDR information from their vehicles if the vehicle is equipped with a recording capability.[23] The federal rule does not place any restrictions on who may access or use EDR data.

The NHTSA requires that EDRs store such information for 30 seconds following a triggering event, thus providing a composite picture of a car's status during any accident.[24] However, the NHTSA places no limits on the type of data that can be collected, nor does it specify who owns the data or whether data can be retained and used by third parties.

Section 563.11 of the NHTSA regulations states as follows:

§ 563.11 Information in owner's manual.

> (a) The owner's manual in each vehicle covered under this regulation must provide the following statement in English:
>
> This vehicle is equipped with an event data recorder (EDR). The main purpose of an EDR is to record, in certain crash or near crash-like situations, such as an air bag deployment or hitting a road obstacle, data that assist in understanding how a vehicle's systems performed. The EDR is designed to record data related to vehicle dynamics and safety systems for a short period of time, typically 30 seconds or less. The EDR in this vehicle is designed to record such data as:

> How various systems in your vehicle were operating;
>
> Whether or not the driver and passenger safety belts were buckled/fastened;
>
> How far (if at all) the driver was depressing the accelerator and/or brake pedal;
>
> and
>
> The speed at which the vehicle was traveling.[25]

These data help provide a better understanding of the circumstances in which crashes and injuries occur.[26] To read data recorded by an EDR, special equipment is required, and access to the vehicle or the EDR is needed. In addition to the vehicle manufacturer, other parties, such as law enforcement, that have the special equipment, can read the information if they have access to the vehicle or the EDR.

State Regulation Of Event Data Recorders

State legislatures have taken notice of EDRs. Driven by a number of concerns, including privacy rights, consumer rights and property rights, as of November 2014, 15 states have enacted laws specifically addressing gaining access to EDR data following a crash.

Of the 15 states that currently have EDR specific statutes, the Texas statute requires disclosure of EDRs in vehicles in the owner's manual of new vehicles sold or leased in the state and requires disclosure in agreements with subscription services. The Texas statute prohibits the download of data, except 1) with the owner's consent; 2) court order; 3) diagnosing, servicing or repairing the vehicle; or 4) vehicle safety research provided specific identifying information is redacted.[27]

The first EDR statute was enacted in 2003 by California. Currently, 15 states—Arkansas, California, Colorado, Connecticut, Delaware, Maine, Nevada, New Hampshire, New York, North Dakota, Oregon, Texas, Utah, Virginia and Washington—have enacted statutes relating to event data recorders and privacy. Among other provisions, these states provide that data collected from a motor vehicle event data recorder may only be downloaded with the consent of the vehicle owner or policyholder, with certain exceptions.[28]

In 2005, Arkansas passed its EDR statute, which is notably restrictive. The registered vehicle owner's written consent is required and if more than one person owns the vehicle then all owners must consent to the data retrieval in writing. The owner of the motor vehicle at the time the data is created retains exclusive ownership rights to the data and ownership of EDR data does not pass to an insurer because of succession in ownership (salvage). Additionally, the owner's written consent is required for an insurer to use the data for any reason. Consent to the retrieval or use of the data cannot be conditioned upon the settlement of a claim. Advance written permission to retrieve or use the data as a condition of an insurance policy is prohibited.

The Arkansas statute effectively prevents an insurer from gaining title to a vehicle that is a total loss due to a crash, assuming ownership of the EDR data record and then using it in litigation or claims processing without the consent of whoever owned the vehicle at the time of the crash. It also overrides any "cooperation clause" that may exist in an insurance policy. The Arkansas statute also declares EDR data as "private."

Apart from the specific declaration in the Arkansas statute that EDR data is "private," the Arkansas, North Dakota, New Hampshire, Virginia, and Oregon statutes all refer to EDR data as property with the same ownership rights as tangible property.

Computer Fraud And Abuse Act

There is also the federal Computer Fraud and Abuse Act,[29] but it is only applicable to what it narrowly defines as a "protected computer." This term refers primarily to computers owned by the federal government or those used for financial transactions and interstate communications.

EDR evidence cannot be obtained without special equipment. Providing the vehicle is properly secured, there is little chance for the data to be lost, corrupted or altered. A conclusive determination that EDR evidence even exists, allowing that a record may not be created in

a crash vehicle with an EDR for a variety of reasons, cannot be made until access is gained to the data file.

There have been a number of hearings in Texas associated with criminal trials involving EDR evidence. Basically, these hearings are used to determine whether scientific evidence produced by an expert witness is valid and admissible in court. In every instance, EDR evidence was found to be admissible.

Changes to existing state statutes, the enactment of new EDR statutes and relevant case law decisions are inevitable as EDRs become a more common tool for aiding in the analysis of traffic accidents. It is important that anyone retrieving EDR data be aware of the current applicable laws and court decisions.

State Data Disposal Laws

PII is frequently collected by businesses and government and is stored in various formats-digital and paper. As of January 21, 2015, at least 32 states have enacted laws that require entities to destroy, dispose of, or otherwise make personal information unreadable or undecipherable.[30] These states include California,[31] Kansas,[32] Missouri,[33] New York[34], and Texas.[35]

California

§ 1798.81. Disposal of records. A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

Kansas

§ 50-7a03. Destruction of consumer information; exception. Unless otherwise required by federal law or regulation, a person or business shall take reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the person or business by shredding, erasing or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

Missouri

Records of division—reproduction, destruction, copies.

§ 288.360. 1. The division may cause to be made such summaries, compilations, photographs, duplications or reproductions of any records, documents, instruments, proceedings, reports or transcripts thereof as it may deem advisable for the effective and economical preservation of the information contained therein, and such summaries, compilations, photographs, duplications or reproductions, duly authenticated or certified by the director or by an employee to whom such duty is delegated shall be admissible in any proceeding under this law or in any judicial proceeding, to the extent that the original record, document, instrument, proceeding, report or transcript thereof would have been admissible therein.

2. The division may provide by regulation for the destruction or disposition, after reasonable periods, of any records, documents, instruments, proceedings, reports or transcripts thereof or reproductions thereof or other papers in its custody, the preservation of which is no longer necessary for the establishment of the contribution liability or the benefit rights of any employing unit or individual or for any other purposes necessary for the proper administration of this law, whether or not such records, documents, instruments, proceedings, reports or transcripts thereof or other papers in its custody have been summarized, compiled, photographed, duplicated, reproduced or audited.

3. The division may prescribe by regulation the charges to be made for certified and uncertified copies of records, reports, decisions, transcripts or other papers or doc-uments. All sums received in payment of such charges shall be promptly transmitted to and deposited in the unemployment compensation administration fund.

New York

§ 399-h. Disposal of records containing personal identifying information.

. . .

2. Disposal of records containing personal identifying information. 1 No person, business, firm, partnership, association, or corporation 2, not including the state or its political subdivisions, shall dispose of a record containing personal identifying information unless the person, business, firm, partnership, association, or corporation, 3 or other person under contract with the business, firm, partnership, association, or corporation 4 does any of the following:

a. shreds the record before the disposal of the record; or

b. destroys the personal identifying information contained in the record; or

c. modifies the record to make the personal identifying information unreadable; or

d. takes actions consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record.

Provided, however, that an individual person shall not be required to comply with this subdivision unless he or she is conducting business for profit.

Texas

§ 521.052. BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION. (a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

(b) A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:

(1) shredding;

(2) erasing; or

(3) otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means.

(c) This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.

(d) As used in this section, "business" includes a nonprofit athletic or sports association.

§ 72.004. DISPOSAL OF BUSINESS RECORDS CONTAINING PERSONAL IDENTIFYING INFORMA-TION. (a) This section does not apply to:

(1) a financial institution as defined by 15 U.S.C. Section 6809; or

(2) a covered entity as defined by Section 601.001 or 602.001, Insurance Code.

(b) When a business disposes of a business record that contains personal identifying information of a customer of the business, the business shall modify, by shredding, erasing, or other means, the personal identifying information so as to make the information unreadable or undecipherable.

(c) A business is considered to comply with Subsection (b) if the business contracts with a person engaged in the business of disposing of records for the modification of personal identifying information on behalf of the business in accordance with that subsection.

(d) A business that disposes of a business record without complying with Subsection (b) is liable for a civil penalty in an amount not to exceed $500 for each business record. The attorney general may bring an action against the business to:

(1) recover the civil penalty;

(2) obtain any other remedy, including injunctive relief; and

(3) recover costs and reasonable attorney's fees incurred in bringing the action.

(e) A business that in good faith modifies a business record as required by Subsection (b) is not liable for a civil penalty under Subsection (d) if the business record is reconstructed, wholly or partly, through extraordinary means.

(f) Subsection (b) does not require a business to modify a business record if:

(1) the business is required to retain the business record under another law; or

(2) the business record is historically significant and:

(A) there is no potential for identity theft or fraud while the business retains custody of the business record; or

(B) the business record is transferred to a professionally managed historical repository.

Relevant Federal Law And Regulation

Federal Trade Commission (FTC) Act-Section 5 Protected Information

The FTC has enforcement authority under laws requiring security programs, including but not limited to GLB.[36] FTC orders in enforcement matters under the GLB security rule generally compel the respondent company to establish "a comprehensive information security program that is reasonably designed to protect the security, confidentiality and integrity of personal information" of consumers.[37] However, there is no general federal data security statute and the FTC's data security jurisprudence forms a rather detailed list of enforcement actions against inadequate security practices that violate consumer protection laws.[38]

Since there is no general federal data-security statute,[39] the FTC has used its general authority under the Federal Trade Commission Act (FTC Act) to penalize companies for security lapses.[40]

Section 5 of the FTC Act prohibits "unfair and deceptive acts or practices in or affecting commerce."[41]

Under Section 5 of the FTC Act, the FTC enforces information security under either of two theories: First, if a company makes representations, such as in its privacy policy, that it will maintain certain safeguards or provide a certain level of security for customer information, and fails to do so, the FTC may proceed under the "deceptiveness" prong of Section 5. On the other hand, without reference to any alleged misrepresentation reading information security, the FTC may instead proceed against a company under the "unfairness" prong of Section 5.[42] In an "unfairness" claim, the FTC must also allege and prove that "the act or practice cause or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by a countervailing benefit to consumers or to competition.[43]

In FTC enforcement actions under Article 5 of the FTC Act, not involving enforcement of GLB, the most common type of protected information is nonpublic personal information conducive to identity theft, including consumer names, physical and email addresses and telephone numbers, social security numbers, purchase card numbers, card expiration dates and security codes and driver's license numbers and other government-issued identification numbers. These categories are similar to the categories of information protected by state laws protecting PII. Other FTC actions under Section 5 have focused on safeguards for health-related information, credit report information, nonpublic consumer identification[44] and information from credit reporting agencies.

In enforcement actions by the FTC, companies have been pursued under a Section 5 "deception" theory, but with no companion claim under GLB, therefore with no underlying specific regulatory standards for prescribed safeguards. The representative FTC complaints we have seen were neither based upon specific security regulatory standards under GLB nor upon any alleged deceptive representations regarding security safeguards. In each, the FTC claimed that failure to provide "reasonable and appropriate security for protected consumer information" constituted an unfair act or practice

under Section 5. However, it is important to remember that information security is not a uniform endeavor. Different industries face different risks for information security and security threats are not static but evolve over time and may emerge or shift rapidly.[45]

Although the FTC held its first workshop on the Internet of Things[46] in November 2013, the FTC has yet to release guidelines or policy recommendations specifically relating to privacy policies on the Internet of Things.[47]

Of particular importance in addressing who owns vehicle data, the current federal law applicable to the insurance business does not provide any reason to believe that vehicle data is part of a protected class of information. This may change in the near future as telematics data becomes increasingly important in the automobile insurance industry.

FCRA And Consumer Credit Protection

The Fair Credit Reporting Act (FCRA)[48] is a federal law that regulates how consumer reporting agencies use consumer information. Enacted in 1970 and substantially amended in the late 1990s and again in 2003, the FCRA gives consumers the right to check and challenge the accuracy of information found in reports so that credit, insurance and employment determinations are fair. Among other things, the FCRA restricts who has access to sensitive credit information and how that information can be used.

Users of the information for credit, insurance, or employment purposes (including background checks) have the following responsibilities under the FCRA:

1. They must notify the consumer when an adverse action is taken on the basis of such reports.
2. Users must identify the company that provided the report, so that the accuracy and completeness of the report may be verified or contested by the consumer.

However, the FCRA applies to the underlying input data into a credit, insurance or employment determination, not the reasoning that a bank, insurer or employer then makes based on this data. Thus, the FCRA provides little remedy if such data is incorporated into credit-reporting processes.[49] Thus, and of great relevance to this analysis, vehicle data is not included among the types of information for which consumer protection is available under the FCRA.[50]

The Communications Act Of 1934 (Communications Act) And The Electronic Communications Privacy Act Of 1986 (ECPA)

The Communications Act imposes a duty on telecommunications carriers to secure information and imposes particular requirements for protecting information identified as customer proprietary network information (CPNI) including the location of customers when they make calls. The Communications Act does not cover location data collected by companies that provide in-car location-based services. The Communications Act also requires express authorization for access to, or sharing of, call location information concerning the user of commercial mobile services, subject to certain exceptions.

ECPA prohibits the federal government and providers of electronic communications from accessing and sharing the content of consumers' electronic communications, unless approved by a court or through consumer consent. ECPA also prohibits the providers from disclosing customer records to government entities, with certain exceptions, but companies may disclose such records to a person other than a governmental entity. ECPA does not specifically address whether location data are considered content or part of consumer-owned records. Some privacy groups have stated that ECPA should specifically address the protection of location data.

Select Recent Proposed Federal Legislation

The 113th and 114th Congresses saw an increase in legislative activity surrounding the question of data privacy. For example, legislation introduced in the current Congress requires the government to "establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission . . ."[51] In addition, the bill would also "amend the Children's Online Privacy Protection Act of 1998 to improve provisions relating to collection, use, and disclosure of personal information of children."[52] This bill is still in committee.

Ownership Of Vehicle Data

It is premature to answer with any certainty the question of who owns vehicle data.[53] The Government Accountability Office (GAO) issued a report that illustrates the difficulty with answering this question.

In December 2013, the GAO issued a report entitled *In Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, But Some Risks May Not Be Clear to Customers* (GAO Report).[54] The GAO identified privacy practices of 10 companies, including five of the largest automobile manufacturers, Chrysler, Ford, GM, Toyota and Nissan. All 10 companies reported they collect location data primarily to provide consumers with various requested location-based services, such as turn-by-turn directions, information on local fuel prices, stolen vehicle tracking and roadside assistance. The auto manufacturers told the GAO that their telematics systems also collect location data for other purposes relating to performance and diagnostics (e.g., when the "check engine light" is displayed, the company collects location data along with data to determine whether driving in certain locations, such as near power plants, affects a vehicle's overall performance).

Company representatives from all 10 selected companies revealed to the GAO that they share consumer location data with third parties to provide and improve services, with law enforcement, or with others for other purposes when data are de-identified.

Industry-recommended practices state that companies should protect the privacy of location data by providing (1) disclosure to consumers about data collection, use and sharing; (2) controls over location data; (3) data safeguards and explanations of retention practices; (4) accountability for protecting consumers' data. The recommended practices are not required, but rather provide a framework for understanding the extent to which these companies protect the privacy of consumers' location data. All ten companies have taken steps that are consistent with some, but not all, of the recommended practices, and the extent to which consumers' data could be at risk may not be clear to consumers.

The GAO learned that selected companies obtain consent and provide certain controls for collecting location data but consumers are not able to delete their collected data. Selected companies also disclosed to the GAO that they de-identify location data, but different methods and retention practices may lead to varying degrees of protection for consumers. All of the selected companies stated in their disclosures to the GAO that they use or share de-identified location data. . . . Representatives from some of the selected companies explained how they de-identify location data; the methods differed among the companies that responded.

Finally, selected companies revealed steps they have taken to be accountable for protecting location data, but the steps they take within their companies are generally not disclosed to consumers. The GAO report noted:

> Currently, no comprehensive federal privacy law governs the collection, use, and sale of personal information by private-sector companies; rather the privacy of consumers' data is addressed in various federal laws. Some of these federal laws are relevant to location data {quoting Section 5 of the FTC Act[55]}. The privacy of consumers' location and other data is also protected in accordance with companies' privacy practices. Federal law does not require companies to notify consumers of their privacy practices, but companies within the scope of our review have conveyed these practices through privacy policies and other documents. Additionally, the FTC has reported that because protecting privacy is important to consumers, companies that deal with consumer data, including location data, have placed emphasis and resources on maintaining reasonable security.[56]

This GAO report and other similar reports[57] highlight the fact that there remains no conclusive determination as to which party owns consumer data provided via auto insurance telematics devices installed in their vehicles. However, the concerns for privacy likely points to a future determination that the data belongs to the consumer providing same.[58]

Various state statutes that refer to EDR data as property with the same ownership rights as tangible property are a further indication that consumer data provided via auto insurance telematics devices installed in their vehicles are viewed in many quarters as proprietary to the consumer who owns the vehicle.

Conclusion

The area of data privacy is still very fluid and consumer protection law is essentially unprepared and out-of-date for today's internet-based society. Millions of health and fitness, automobile, home, employment, and

smartphone devices are currently in use, collecting and monitoring data on consumer behavior. However, manufacturers have little, if any, specific guidance from the FTC or other regulators about who owns the data they may collect and what constitutes adequate notice in relevant privacy policies. As the issues of data collection and data privacy become more prevalent, legislators and regulators are taking note and, while this area of law is still ambiguous, this will likely change in the near future and all parties need to pay close attention as these changes take place.

Endnotes

1. Vehicle Driving Data includes, but is not limited to, acceleration, braking, turning, cornering, time of day, night driven, etc.

2. 15 U.S.C. § 6801(b).

3. Mo: 20 CSR 100-6.110; Mo. DOI Bull. 00-03 (10/11/2000); Neb: 210 NAC Ch. 77 s 001.

4. See, e.g., Gina Stevens, Cong. Research Serv., R42475, Data Security Breach Notification Laws 4 (2012) (citations to laws omitted). In 2014, Kentucky became the latest state to enact a breach notification law, Ky. Rev. Stat. § 365.732.

5. National Conference of State Legislatures, Security Breach Notification Laws (last updated as of 1/1/2015).

6. We discovered them through a broad review of available secondary sources which shed light on the issues discussed in this article and led to additional valuable source materials uncovered through our research. In this regard, the authors wish to acknowledge the important contributions of Peter Sloan, Esq. of the law firm Husch Blackwell LLP of Kansas City, Mo., whose presentation paper, *Legal Ethics and the Reasonable Information Security Program* was part of the course materials utilized at a Continuing Legal Education ("CLE") Seminar during the Fall National Meeting of the National Association of Insurance Commissioners on November 15, 2014 in Washington, D.C. Further, the authors wish to acknowledge the important contributions of Scott R. Peppet, Professor of Law, University of Colorado School of Law, whose law review article entitled *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, November 2014 was also a most valuable source reference.

7. See, e.g., Va. Code Ann. § 18.2-186.6(A); Sloan, *supra* note 6, at 31.

8. See, e.g., *id.*

9. Cal Civ Code § 1798.82(h)(1).

10. Mo. Rev. stat. § 407.1500.1(9).

11. Tex. Bus. & Com. Code Ann. § 521.002(a)(2).

12. Neb. Rev. Stat. 87-802(5).

13. Tex. Bus. & Com. Code Ann. § 521.002(a)(1)(C).

14. *Id.* at § 521.002(a)(1)(A).

15. *Id.* at § 521.002(a)(1)(B).

16. *Id.* at § 521.002(a)(1)(D).

17. P.R. Laws Ann. Tit. 10, § 4051(a).

18. Peppet, *supra* note 6, at 136-140.

19. Cal Civ Code § 1798.82(a)-(b).

20. 42 U.S.C. § 1320d et seq.

21. Cal Civ Code § 1798.82(d).

22. Public Law 111-5.

23. 49 C.F.R. § 563. 2.

24. 49 C.F.R. § 563.6-7.

25. 49 C.F.R. § 563.11(a) discussing that some parties, such as law enforcement, may use EDR data, but making no mention of who owns such EDR data.

26. Note: EDR data are recorded by a vehicle only if a non-trivial crash situation occurs; no data are

recorded by the EDR under normal driving conditions and no personal data (e.g., name, gender, age, and crash location) are recorded. However, other parties, such as law enforcement, could combine the EDR data with the type of personally identifying data routinely acquired during a crash investigation. These regulations make no mention as to who owns such EDR data.

27. Tex. Trans. Code § 514.615.

28. National Conference of State Legislatures, *Privacy of Data from Event Data Recorders: State Statutes* (as of 11/12/2014); see also, Jim Harris, Harris Technical Services, *Event Data Recorders – State Statutes and Legal Considerations*, originally appearing in the Accident Reconstruction Journal, Vol. 18, No. 1, Jan/Feb 2008.

29. 18 U.S.C. § 1030.

30. National Conference of State Legislatures, Data Disposal Laws (last updated as of 01/21/2015) available at http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx (last accessed on April 9, 2015).

31. Cal. Civ. Code § 1798.81.

32. Kan. Stat. §§ 50-7a01 and 50-7a03.

33. Mo. Stat. § 288.360.

34. NY Gen Bus § 399-h.

35. Tex. Bus. and Com. Code § 72.004 and § 521.052.

36. 15 U.S.C. § 6805(a)(7); Sloan, *supra* note 6, at 9-14.

37. Consent Order *In re ACRAnet, Inc.*, FTC File No. 092-3088, No. C-4331 (F.T.C. Aug. 17, 2011) at 2-3; cited in Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia L. Rev. 583 (2014) at 652.

38. Solove and Hartzog, supra at 649-658.

39. Certain types of information, such as health and financial data, are subject to heightened data security requirements, but no statute sets forth general data security measures.

40. 15 U.S.C. § 45 (a)(2); Peppet, *supra* note 6, at 136-140; Sloan, *supra* note 6, at 9-14.

41. 15 U.S.C. § 45(a)(1).

42. Sloan, *supra* note 6, at 10-14.

43. 15 U.S.C. § 45(n).

44. *See*, *e.g. In the Matter of Dave & Buster's Inc., a corporation* (Docket No. C-4291) (May 20, 2010). The FTC's press release concerning the settlement is available at http://www.ftc.gov/opa/2010/03/davebusters.shtm.

45. Sloan, *supra* note 6, at 10-14.

46. "The term 'Internet of Things' is generally attributed to Kevin Ashton. Thomas Goetz, Harnessing the Power of Feedback Loops, Wired, June 19, 2011, http://www.wired.com/2011/06/ff_feedbackloop/, archived at http://perma.cc/H9D3-V6D3; *see also* Kevin Ashton, That 'Internet of Things' Thing, RFID J., June 22, 2009, http://www.rfidjournal.com/articles/pdf?4986, archived at http://perma.cc / B4CW-M29Z (claiming that the first use of the term "Internet of Things" was in a 1999 presentation by Ashton); *see generally* Neil Gershenfeld, When Things Start to Think (1999) (addressing the general concept of merging the digital world with the physical world); Melanie Swan, Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0, 1 J. Sensor & Actuator Networks 217 (2012) (exploring various ways of defining and characterizing the Internet of Things and assessing its features, limitations, and future)" cited in Peppet, *supra* note 6, at 89 fn. 13.

47. Peppet, *supra* note 6, at 146.

48. 15 U.S.C. § 1681.

49. Peppet, *supra* note 6, at 127-28.

50. *Id.* at 124-29.

51. S. 547, 114th Cong. (2015).

52. Id.

53. Peppet, *supra* note 6, at 91-92.

54. U.S. Government Accountability Office *In Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, But Some Risks May Not Be Clear to Customers* (Publication No. GAO-14-81) (December 2013).

55. At this juncture, the GAO Report also cites the Communications Act and ECPA. As mentioned, the Communications Act imposes a duty on telecommunications carriers to secure information and imposes particular requirements for protecting information identified as CPNI including the location of customers when they make calls. The Communications Act does not cover location data collected by companies that provide in-car location-based services. The GAO Report also cites here ECPA which prohibits the federal government and providers of electronic communications from accessing and sharing the content of consumers' electronic communications, unless approved by a court or through consumer consent. As discussed above, ECPA does not specifically address whether location data are considered content or part of consumer records.

56. GAO Report, *supra* note at 58 at 7.

57. *See*, *e.g.* U.S. Government Accountability Office *Consumers' Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent and Risks May Not Be Clear to Customers* (GAO-14-649T) (June 2014).

58. *Id.* ■

MEALEY'S DATA PRIVACY LAW REPORT
edited by Mark C. Rogers
The Report is produced by

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: http://www.lexisnexis.com/mealeys
ISSN 2378-6892