



Liability of Transportation Entity for the Unintentional Release of Secure Data or the Intentional Release of Monitoring Data on Movements or Activities of the Public

DETAILS

56 pages | 8.5 x 11 | PAPERBACK
ISBN 978-0-309-37548-1 | DOI 10.17226/23586

AUTHORS

Larry W. Thomas and James B. McDaniel; National Cooperative Highway Research Program Legal Program; National Cooperative Highway Research Program; Transportation Research Board; National Academies of Sciences, Engineering, and Medicine

BUY THIS BOOK

FIND RELATED TITLES

Visit the National Academies Press at NAP.edu and login or register to get:

- Access to free PDF downloads of thousands of scientific reports
- 10% off the price of print titles
- Email or social media notifications of new titles related to your interests
- Special offers and discounts



Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. (Request Permission) Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences.

Legal Research Digest 71

LIABILITY OF TRANSPORTATION ENTITY FOR THE UNINTENTIONAL RELEASE OF SECURE DATA OR THE INTENTIONAL RELEASE OF MONITORING DATA ON MOVEMENTS OR ACTIVITIES OF THE PUBLIC

This report was prepared under NCHRP Project 20-06, Topic 21-04, “Legal Problems Arising Out of Highway Programs,” for which the Transportation Research Board is the agency coordinating the research. The report was prepared by Larry W. Thomas, The Thomas Law Firm, Washington, DC. James B. McDaniel, TRB Counsel for Legal Research Projects, was the principal investigator and content editor.

Background

State highway departments and transportation agencies have a continuing need to keep abreast of operating practices and legal elements of specific problems in highway law. The NCHRP Legal Research Digest series is intended to keep departments up-to-date on laws that will affect their operations.

Foreword

Transportation entities collect various amounts of data for transportation-related purposes. Without debating the legitimacy of the purpose for the specific data collected, what liability exists for the accidental release of data that was to be securely held by the entity for a transportation-related purpose? Similarly, what liability exists for the intentional release of data generated from the monitoring of the movements or activities of the public?

The Division of Motor Vehicles in each state collects secure data, also referred to as “sensitive” data, on vehicle ownership and drivers’ Social Security numbers, addresses, and medical information. The data are used by law enforcement agencies to locate a vehicle’s owner to enforce traffic violations recorded by roadside cameras. Data on individuals are protected by the Driver’s Privacy Protection Act of 1994 (DPPA) and may not be used for purposes prohibited by the DPPA.

Intelligent transportation systems, electronic tolling, and other technology may be used to reduce congestion, improve mobility, save lives, and optimize the use of existing infrastructure; however, there are privacy issues associated with the use of technology to collect, use, disclose, or maintain secure data or monitoring data on members of the public. Whether data are or should be secure depends on the purposes for which the data are being collected, with whom the data may be shared, the length of time the data are or may be retained, and on law enforcement agencies.

The main objective of this research is to review the statutes, regulations, and common law regarding the release of data collected for transportation purposes. Included in this research are questions concerning the application of public records laws and the application of any constitutional, statutory, or common law privacy rights. The digest also researches and identifies statutes and common law dealing with the collection of data on the activities of the public, includes a literature search of topics addressing these issues, and also includes a search of state and federal laws focusing on this and similar topics.

It should be useful to transportation officials, particularly those involved with recordkeeping; attorneys; freedom of information officials; those responsible for releasing such data; and the persons who are the subject of the collected information.

CONTENTS

Introduction, 3

I. Transportation Agencies' Use of Intelligent Transportation Systems and Other Methods to Collect Data, 5

- A. Intelligent Transportation Systems, 5
- B. Secure Data Collected and/or Retained by Transportation Agencies, 6
- C. Monitoring Data Collected and/or Retained by Transportation Agencies, 6

II. Transportation Agencies' Use of ITS to Collect Data, 7

- A. Legal Authority for ITS, 7
- B. Traffic Monitoring Systems, 8
- C. Electronic Toll Collection, 8

III. Whether Privacy Rights Under the United States Constitution Apply to Personal and Locational Data, 9

- A. Introduction, 9
- B. Evolution of Privacy Rights, 9
- C. The Fourth Amendment and a Constitutional Right to Privacy, 12
- D. Whether There Is an Implied Constitutional Claim for a Privacy Violation, 15
- E. Whether There Is a Section 1983 Claim for an Intentional or Unintentional Release of Data, 17

IV. Whether There Are Federal Statutes Applicable to Transportation Agencies' Collection or Disclosure of Data, 20

- A. Evolution of Federal Statutory Privacy Rights, 20
- B. Privacy Act of 1974, 20
- C. Driver's Privacy Protection Act, 22
- D. Other Federal Privacy Laws, 23
- E. Proposed Federal Privacy Legislation, 24
- F. Consumer Privacy Bill of Rights, 25

V. The Right to Privacy Under State Constitutions, 26

- A. State Constitutions Recognizing a Right to Privacy, 26
- B. States Recognizing an Implied Cause of Action for a Violation of a State Constitutional Provision, 27

VI. Right to Privacy Under State Statutes, 28

- A. Introduction, 28
- B. Specific State Privacy Statutes, 29
- C. Whether There Are Separate Claims Based on the Owner or Type of Data or on the Collection, Use, Disclosure, or Maintenance of Data, 30
- D. Privacy Policies Required by States, 32
- E. State Laws Banning or Restricting the Use of Certain Technology, 33
- F. State Legislative Trends and Proposed Legislation, 33

VII. Whether State Data Breach Notification Laws Apply to Transportation Agencies, 35

- A. Definition of a Data Breach, 35
- B. States Having Data Breach Notification Statutes, 35
- C. Applicability of the Statutes to Government Agencies, 36
- D. State Breach Notification Laws Authorizing Civil Penalties or Claims for Damages, 37

VIII. Remedies at Common Law for Invasion of Privacy, 40

- A. States that Recognize an Invasion of Privacy at Common Law, 40
- B. Invasion of Privacy, 41
- C. Applicability of a Common Law Right of Privacy to Transportation Agencies, 42

IX. Whether Transportation Agencies Are Potentially Liable for a Disclosure of Data, 43

- A. Whether a Claim for a Release of Data Is Barred by Sovereign Immunity or a State Tort Claims Act, 43
- B. Claims Against Transportation Agencies Arising Out of the Disclosure of Secure Data or Monitoring Data, 45
- C. Liability of Contractors for Data Disclosure, 48
- D. Causes of Action Alleged Against Private Companies for Privacy Violations, 48

X. Disclosures of Data Under the Federal or a State FOIA or State Public Records Disclosure Law, 49

- A. Introduction, 49
- B. The Federal FOIA and Release of Data, 49
- C. State FOIA or Public Records Disclosure Laws and a Release of Data, 49
- D. Agency Waiver of Privacy Exemption, 51
- E. Whether Both FOIA Requests and Discovery Requests May Be Used to Obtain a Transportation Agency's Data, 51

Conclusion, 52

Appendices, 54

LIABILITY OF TRANSPORTATION ENTITY FOR THE UNINTENTIONAL RELEASE OF SECURE DATA OR THE INTENTIONAL RELEASE OF MONITORING DATA ON MOVEMENTS OR ACTIVITIES OF THE PUBLIC

By Larry W. Thomas, The Thomas Law Firm, Washington, DC

INTRODUCTION

Transportation agencies are taking advantage of ever more rapid advances in Intelligent Transportation Systems (ITS) and other technology. However, collecting personal data on members of the public has privacy implications; moreover, individuals' data may be accessed by unauthorized persons or used for purposes unrelated to transportation agencies' reasons for collecting data.¹

The term ITS includes any technology used by transportation agencies to collect data.² ITS may be used to "[i]ntegrate vehicles and surface transportation infrastructure with information, communication, and sensory technologies to improve the safety, efficiency, security, service, accessibility, environmental responsibility, and reliability of the transportation system. The term ITS covers a broad range of transport-related activities...."³

Because transportation agencies collect, use, disclose, and/or maintain personal and locational data, the digest focuses on two issues: whether a state transportation agency may be liable for the

unintentional release of secure data (secure data) or for the intentional release of data collected by monitoring the movements and activities of the traveling public (monitoring data).⁴

Transportation agencies are not the only ones to find the collection of data to be useful. The collection and retention of data by the agencies and the associated privacy issues should be considered in the context of the ongoing, widespread collection and retention of personal data, including photographs, dates of birth, and other personally identifiable information (PII). For example, New York University's Center for Urban Science and Progress is developing the country's first "Quantified Community" that involves "[m]easuring, modeling, and predicting pedestrian flows through traffic and transit points, open spaces, and retail space."⁵ Personal data is being collected on individuals via the Internet or because of individuals' willingness to disclose personal information on social media.⁶ Facebook has been said to have more data than most government bodies.

Seventeen transportation agencies responded to a survey conducted for the digest regarding their

¹ James D. Phillips and Katharine E. Kohm, *Current and Emerging Transportation Technology: Final Nails in the Coffin of the Dying Right of Privacy*, 18 RICH. J.L. & TECH. 1, 2–3 (2011) [hereinafter Phillips and Kohm]; Teresa Scassa, Jennifer A. Chandler, and Elizabeth F. Judge, *Privacy by the Wayside: The New Information Superhighway, Data Privacy, and the Deployment of Intelligent Transportation Systems*, 74 SASK. L. REV. 117, 120 (2011) [hereinafter Scassa, Chandler, and Judge]. See also G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulations for a New Era*, 19 MICH. TELECOMM. TECH. L. REV. 163, 183–84 (2012).

² Thomas Garry, Frank Douma, and Stephen Simon, *Intelligent Transportation Systems: Personal Data Needs and Privacy Law*, 39 TRANSP. L. J. 97, 101 (2012), [hereinafter Garry, Douma, and Simon]. See also UNITED STATES DEPARTMENT OF TRANSPORTATION, RESEARCH AND INNOVATIVE TECHNOLOGY ADMINISTRATION [hereinafter RITA], *Frequently Asked Questions*, available at: <http://www.its.dot.gov/faqs.htm> (last accessed Oct. 12, 2015). See Frank Douma and Jordan Deckenbach, *The Challenge of ITS for the Law of Privacy*, 2009 U. ILL. J.L. TECH & POLY 295 (2009) [hereinafter Douma and Deckenbach].

³ Scassa, Chandler, and Judge, *supra* note 1, at 118 (footnote omitted).

⁴ See also Phillips and Kohm, *supra* note 1, at 2; Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 296 (2004) [hereinafter Glancy]; Jeremy Kahn, *High Technology in the Transportation Industry: Is the New Data We Gather Worth All the Costs?*, 28 TRANSP. L.J. 89, 91, 92, 103 (2000) [hereinafter Kahn]; Joshua D. Prok, *Intelligent Transportation Systems: From Hometown Solutions to World Leadership*, 35 TRANSP. L.J. 293, 294, 300, 302 (2008); Scassa, Chandler, and Judge, *supra* note 1, at 118–20.

⁵ Center for Urban Science + Progress, New York University, NYU CURP, *Related Companies and Oxford Properties Group Team Up to Create "First Qualified Community" in the United States at Hudson Yards*, available at <http://cusp.nyu.edu/press-release/nyu-cusp-related-companies-oxford-properties-group-team-create-first-quantified-community-united-states-hudson-yards/> (last accessed Oct. 12, 2015).

⁶ Lothar Determann, *Social Media Privacy: A Dozen Myths and Facts*, HARV. J.L. & TECH. 3 (2012) (stating that "it is rarely the social media company that invades your privacy. What haunts people is typically user-generated content, i.e., information that people themselves, their friends, and other social media users upload"); Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 556–58 (2008); and James P. Nehf, *Recognizing the Society Value in Information Privacy*, 78 WASH. L. REV. 1, 2–7 (2003).

collection of secure data and monitoring data. The survey was not intended for use as an empirical study, but rather as an aid to gather information from transportation agencies on their data practices and policies. The survey questions are included with the digest as Appendix A.⁷ The agencies' responses are discussed throughout the digest and summarized in Appendix B.⁸

Section I of the digest discusses transportation agencies' use of ITS and other technology to collect secure data and monitoring data; what is meant by the terms "secure data" and "monitoring data"; and the kinds of data that the agencies are collecting, using, disclosing, and/or retaining.

Section II reviews the legal authority for using ITS, the establishment of state traffic monitoring systems (TMS), and the collection of data by electronic tolling and other facilities.

Section III analyzes whether under the U.S. Constitution there is a right to privacy in personal and locational data, and whether there is an implied claim or a claim under 42 U.S.C. § 1983 for a violation of a constitutional right to privacy for the disclosure of secure data or monitoring data. However, as the digest explains, the U.S. Supreme Court has not recognized a constitutional right to privacy in personal data or locational data.

Section IV discusses relevant federal statutes that are applicable to personal and locational data, including the Privacy Act of 1974 and the Driver's Privacy Protection Act (DPPA). The digest also discusses proposed federal legislation that would restrict or prohibit the use of certain technology or restrict or prohibit the use of certain personal or locational data.

Section V analyzes the right to privacy under state constitutions that may apply to an agency's collection of secure data or monitoring data and whether in some states an implied cause of action is recognized for a violation of a state constitutional right to privacy. Nevertheless, no cases were located for the digest, and the transportation agencies did not report any cases arising under a state's constitution against an agency for a violation of privacy in connection with a disclosure of secure data or monitoring data.

Section VI analyzes state statutes that establish an individual's right to privacy and whether under any of the privacy statutes an individual has a right of action to claim damages against a

⁷ Although transportation agencies reported having other kinds of secure data, with some exceptions, the digest does not discuss health care or employment law.

⁸ See Appendix D for a list of the transportation agencies that responded.

transportation agency for a violation of the statute. No case, however, was located for the digest, nor did a transportation agency report a claim against an agency for violating a state privacy statute because of a disclosure of secure data or monitoring data. Also discussed are privacy policies that some states require state agencies to develop and to make available to the public. Section VI also reviews state laws banning or restricting the use of certain technology, as well as the status as of June 30, 2015, of proposed legislation in some states that would limit or prohibit the use of certain technology or limit or prohibit the collection or use of certain personal or locational data.

Section VII discusses data-breach notification laws that virtually all states have enacted, whether the statutes apply to government agencies, and whether the statutes that apply to government agencies authorize an assessment of civil penalties or allow a claim for damages for a breach of the applicable statute.

Section VIII discusses whether a claim may exist against a transportation agency for violating a privacy right under a state's common law for the unintentional disclosure of secure data or the intentional disclosure of monitoring data.

Section IX analyzes whether a privacy claim against a transportation agency would be barred by sovereign immunity or by a state tort claims act and discusses privacy claims that have been made against transportation agencies for disclosure of personal data. Although some privacy cases were located that are relevant to the digest, the transportation agencies responding to the survey reported that they had not had any claims against them for disclosing either secure data or monitoring data.

Section X examines whether secure data and monitoring data may be obtained through a request made pursuant to a Freedom of Information Act (FOIA) or other state public records disclosure law. Moreover, the digest discusses whether both FOIA and discovery requests and subpoenas may be used in a case against a transportation agency to obtain data from the agency.

As stated, Appendix B summarizes the transportation agencies' responses to the survey, in which they describe the kinds of secure data and monitoring data that they are collecting; their regulations, policies, and procedures for doing so; and contracts that they have with private entities to collect data. Appendix C provides copies of or links to the agencies' regulations, policies, procedures, and contracts concerning their collection of secure data or monitoring data.

I. TRANSPORTATION AGENCIES' USE OF INTELLIGENT TRANSPORTATION SYSTEMS AND OTHER METHODS TO COLLECT DATA

A. Intelligent Transportation Systems

ITS technology enables transportation agencies to collect a wide array of secure data and monitoring data, some of which have PII or could be used in combination with other means to obtain PII. Fourteen transportation agencies responding to the survey reported that they are using ITS technologies.⁹ Fourteen agencies reported that they collect or maintain secure data,¹⁰ whereas two agencies stated that they do not.¹¹ Thirteen transportation agencies reported that they are collecting or maintaining monitoring data,¹² whereas three agencies said that they are not doing so.¹³

ITS may involve the use of roadside systems to measure traffic volume, speed, and congestion; roadside and vehicle-mounted speed and red light cameras and license plate readers; and electronic toll collection. ITS may utilize infrared sensors, weight and motion sensors, vehicle safety systems, radar, transponders, smart cards, cell phones, the Internet, radio, closed-circuit television (CCTV), Global Positioning System (GPS) technology, onboard computers, variable message signs, black boxes, emergency response systems, and video surveillance.¹⁴

The data collected may be used for planning and monitoring purposes; improving the safety, efficiency, and performance of transportation systems; and enforcing traffic regulations.¹⁵ Vehicle data

may be used to provide traffic management centers with detailed, real-time information on traffic flow, speeds, and other conditions and to analyze driver behavior based on locational data, as well as for other purposes.¹⁶ Information collected by transportation agencies may be shared with members of the public to inform them about traffic flows and infrastructure,¹⁷ thereby assisting them in making better choices about their route of travel or alternate means of travel, such as walking, biking, or public transit.¹⁸

Vehicles may be tracked by electronic tolling and mass transit facilities. When a motorist obtains an electronic device such as an EZPass, the device typically has access to the owner's name, vehicle number, and credit card information. When the vehicle passes through a toll collection station, the place and time of the payment of the toll is recorded.¹⁹ An individual's movements are tracked in mass transit systems through the use of Smart Cards that operate in a manner similar to EZPass. The card contains PII and pairs it with specific financial, time, and locational data.²⁰

The divisions of motor vehicles (DMV) in each state collect secure data, also referred to as "sensitive" data, on vehicle ownership and drivers' Social Security numbers, addresses, and medical information.²¹ The data are used by law enforcement agencies to locate a vehicle's owner to enforce traffic violations recorded by roadside cameras.²² As discussed in Section IV.C, the DMV's data on individuals are protected by the DPPA²³ and may not be used for purposes prohibited by the DPPA.²⁴

⁹ Alabama DOT, Arizona DOT, District of Columbia DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, North Dakota DOT, Ohio DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Ohio DOT did not respond to the survey questions directly, but provided information regarding data practices for its department.

¹⁰ Alabama DOT, Arkansas DOT, Arizona DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT.

¹¹ District of Columbia DOT and Maine DOT.

¹² Alabama DOT, Arkansas DOT, Arizona DOT, District of Columbia DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, Ohio DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT.

¹³ Maine DOT, Montana DOT, and North Dakota DOT.

¹⁴ Scassa, Chandler, and Judge, *supra* note 1, at 118. GPS technology may be used to track a particular vehicle's movements.

¹⁵ Garry, Douma, and Simon, *supra* note 2, at 101; RITA, *supra* note 2; and Scassa, Chandler, and Judge, *supra* note 1, at 118.

¹⁶ See RITA, *supra* note 2, and http://www.its.dot.gov/factsheets/overview_factsheet.htm (last accessed Oct. 12, 2015). See also Garry, Douma, and Simon, *supra* note 2, at 132–33; Scassa, Chandler, and Judge, *supra* note 1, at 118; and Glancy, *supra* note 4, at 301.

¹⁷ Garry, Douma, and Simon, *supra* note 2, at 13; Glancy, *supra* note 4, at 313.

¹⁸ RITA.

¹⁹ FHWA, *Freeway Management and Operations Handbook, 15.2.7.1 Automatic Vehicle Identification*, available at http://ops.fhwa.dot.gov/freewaymgmt/publications/frwy_mgmt_handbook/chapter15_02.htm (last accessed Oct. 12, 2015).

²⁰ *Id.*

²¹ Garry, Douma, and Simon, *supra* note 2, at 134. See also Glancy, *supra* note 4, at 369.

²² Garry, Douma, and Simon, *supra* note 2, at 134–35.

²³ Pub. L. No. 103-322, tit. XXX, 108 Stat. 2099.

²⁴ Designated purposes include state-authorized release for public safety, prevention of car theft, prevention of fraud, claims investigations, and promotion of driver safety. See *Reno v. Condon*, 528 U.S. 141, 145 N. 1, 120 S. Ct. 666, 669 N. 1, 145 L. Ed. 2d 587, 592 N. 1 (2000) (citing 18 U.S.C. § 2721(b)(1)-(10)). See also Garry, Douma, and Simon, *supra* note 2, at 134; Glancy, *supra* note 4, at 369.

In sum, ITS, electronic tolling, and other technology may be used to reduce congestion, improve mobility, save lives, and optimize the use of existing infrastructure;²⁵ however, there are privacy issues associated with the use of technology to collect, use, disclose, or maintain secure data or monitoring data on members of the public.²⁶

B. Secure Data Collected and/or Retained by Transportation Agencies

Whether data are or should be secure depends on the purposes for which the data are being collected, with whom the data may be shared, the length of time the data are or may be retained, and whether and when the data are accessible by law enforcement agencies.²⁷

Secure data are data of a “sensitive” nature that should not be shared or otherwise disclosed except as authorized by law or with an individual’s consent.²⁸ The Consumer Privacy Bill of Rights, which was announced in February 2015 by the White House and is discussed in Section IV.F, defines “sensitive information as ‘personally identifiable information which, if lost, compromised, or disclosed without authorization either alone or with other information, carries a significant risk of economic or physical harm.’”²⁹ Secure data include PII, such as names, addresses, Social Security numbers, credit card numbers, pin numbers, passwords, security codes, and precise geographical locational data.³⁰ Secure data usually “require[s] heightened levels of data protection,”³¹ such as encryption and adequate security.³²

Although the transportation agencies’ responses to the survey identified the types of secure data they collect, the agencies specifically identified PII as

being secure data.³³ The Arizona Department of Transportation (DOT) defined PII to include drivers’ license numbers, Social Security numbers, credit card numbers, financial account data, federal tax information, and health information. The agencies also reported having other kinds of secure data, including accident or crash data;³⁴ data on bidders and contractors;³⁵ data relating to claims, litigation, and attorney work product;³⁶ data collected in connection with eminent domain and right-of-way acquisition (e.g., appraisals);³⁷ and data on employees, including information on disabilities, discrimination complaints, employee disciplinary matters, payroll, and Worker’s Compensation claims.³⁸ Although stating that the data are confidential and not subject to disclosure, the Florida DOT defined secure data to include the department’s data relating to bidding and contracting (e.g., official cost estimates, financial statements, the DOT’s Bid Analysis and Monitoring System, and sealed bids or proposals); investigations; and security planning pursuant to Florida’s Security of Data and Information Resources Act (e.g., plans, blueprints, and schematic drawings).

C. Monitoring Data Collected and/or Retained by Transportation Agencies

One method of data collection that seems to present a significant privacy concern is the use of technology that permits the location and positive identification of “individual drivers at a particular moment in time...”³⁹ Thus, data that are or that may be linked to a person and/or vehicle also are considered to be secure data.⁴⁰ However, monitoring data collected anonymously (i.e., not linked to an individual or used in a way to obtain PII) do not appear to come within the meaning of the term “secure data.”

²⁵ ITS SOCIETY, *Legislative Outreach Brochure*, available at http://www.itsa.wikispaces.net/file/view/ITSA+Govt+Affairs+Brochure_1.5.pdf/419564912/ITSA%20Govt%20Affairs%20Brochure_1.5.pdf (last accessed Oct. 12, 2015).

²⁶ Scassa, Chandler, and Judge, *supra* note 1, at 120 (e.g., “through traffic cameras, video, facial recognition, software, license plate identification, or other media and technologies”).

²⁷ Garry, Douma, and Simon, *supra* note 2, at 99.

²⁸ *Id.* at 114.

²⁹ Nancy J. King and V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 424 (2013) [hereinafter King and Raja].

³⁰ *Id.* at 431.

³¹ *Id.* at 456 and 464. See also Garry, Douma, and Simon, *supra* note 2, at 107.

³² King and Raja, *supra* note 29, at 427.

³³ Arizona DOT, Florida DOT (e.g., bank account and credit card numbers and data from electronic tolls); City of Minneapolis–Public Works Dept.; Montana DOT (e.g., banking records, date of birth, driver’s records, Social Security numbers); North Dakota DOT (e.g., driver’s license numbers and records and vehicle owner records); Oregon DOT; and Utah DOT (tolling data).

³⁴ Arkansas DOT, Florida DOT, MoDOT, Montana DOT (noting also property damage information), Oklahoma DOT, and Oregon DOT.

³⁵ Oklahoma DOT.

³⁶ Arkansas DOT, Florida DOT, and Oklahoma DOT.

³⁷ Arkansas DOT and Florida DOT.

³⁸ Alabama DOT, Florida DOT, Indiana DOT, Montana DOT (noting data concerning Americans with Disabilities Act), Oklahoma DOT, Oregon DOT, and Utah DOT.

³⁹ Garry, Douma, and Simon, *supra* note 2, at 117. See also Glancy, *supra* note 4, at 296–97.

⁴⁰ Garry, Douma, and Simon, *supra* note 2, at 106, 107.

As for the kinds of monitoring data transportation agencies are collecting and/or maintaining,⁴¹ they reported collecting data on accidents,⁴² driver behavior,⁴³ license plate numbers,⁴⁴ tolls and toll road data,⁴⁵ traffic counts,⁴⁶ traffic volume,⁴⁷ vehicle classification,⁴⁸ vehicle occupancy,⁴⁹ vehicle speed,⁵⁰ and Wi-Fi and Bluetooth media access control (MAC) addresses accessed along Interstate routes without, however, storing the data.⁵¹

The Missouri Highways and Transportation Department (MoDOT) stated that it “collects traffic count and turning movement information at intersections throughout the state. These counts can be collected manually by staff in the field or they may be captured using video that is later processed.” The department provided a copy of the contract that it has with one company

to receive a live traffic data feed for thousands of roadway miles in Missouri. This data is collected, processed, and distributed solely by [HERE North America, LLC (HERE)]. MoDOT is simply a recipient of the data feed. The data received by MoDOT include[] the average speed and travel time for pre-defined roadway segments at approximately 60-second intervals. This data feed has allowed MoDOT to monitor live traffic conditions on thousands of miles of roadways without the need for instrumentation such as is used in St. Louis and Kansas City.⁵²

The department stated that although MoDOT uses closed-circuit television cameras to monitor live traffic conditions, the images captured by the cameras are not recorded or stored.⁵³ Appendix B provides more details on the types of secure and monitoring data that the agencies reported that they are collecting.

II. TRANSPORTATION AGENCIES’ USE OF ITS TO COLLECT DATA

A. Legal Authority for ITS

Congress enacted the Intelligent Transportation Systems Act as part of the Transportation Equity

Act for the 21st Century (TEA-21) of 1998.⁵⁴ Congress decided that the investments authorized by the Intermodal Surface Transportation Efficiency Act of 1991⁵⁵ demonstrated that ITS “can mitigate surface transportation problems in a cost-effective manner.”⁵⁶ Congress also decided that continued investment in ITS was needed to accelerate the incorporation of ITS into the national surface transportation network to improve transportation safety and efficiency and reduce costs and “impacts on communities and the environment.”⁵⁷ Congress directed the Secretary of Transportation to “develop, implement, and maintain a national architecture and supporting standards and protocols to promote the widespread use and evaluation” of ITS technology in the surface transportation systems of the United States and to promote ITS to the “maximum extent practicable.”⁵⁸ Section 5208 of TEA-21 created the Intelligent Transportation System Integration Program.⁵⁹

ITS is codified in 23 U.S.C. § 501. Section 501(5) defines the term “ITS” as “electronics, photonics, communications, or information processing used singly or in combination to improve the efficiency or safety of a surface transportation system.”⁶⁰ Section 502 encourages the Secretary of Transportation to make decisions needed on the research, development, and technology for the implementation of intelligent transportation infrastructure.⁶¹ Section 501(4) defines intelligent transportation architecture as “fully integrated public sector intelligent transportation system components, as defined by the Secretary....”⁶² In implementing ITS programs, the secretary is obligated to cooperate with other governmental entities and private or educational entities.⁶³ Moreover, the secretary was directed to establish an Advisory Committee composed of relevant stakeholders to oversee the implementation of ITS programs.⁶⁴

⁵⁴ Pub. L. No. 105-178, §§ 5201–5207, 112 Stat. 457 (1998).

⁵⁵ Pub. L. No. 102-240, 105 Stat. 1914.

⁵⁶ Pub. L. No. 105-178, § 5202. *See* 23 U.S.C. § 514(a) (2015).

⁵⁷ *Id.*

⁵⁸ Pub. L. No. 105-178, § 5206(a), 112 Stat. 457 (1998).

⁵⁹ Pub. L. No. 105-178, § 5208, 112 Stat. 457 (1998).

⁶⁰ 23 U.S.C. § 501(5) (2015).

⁶¹ 23 U.S.C. § 502 (2015).

⁶² 23 U.S.C. § 501(4) (2015).

⁶³ 23 U.S.C. §§ 515(a)-(c) (2015).

⁶⁴ 23 U.S.C. § 515(h) (2015). The Advisory Committee must have no more than 20 members, balanced between metropolitan and rural interests, and include a representative of the agencies, disciplines, and groups identified in §§ 515(h)(2)(A)-(L).

⁴¹ *See* Appendix A.

⁴² Arizona DOT, District of Columbia DOT (crash information), and South Carolina DOT.

⁴³ Arkansas DOT.

⁴⁴ Arkansas DOT and Oregon DOT.

⁴⁵ Indiana DOT.

⁴⁶ Alabama DOT and MoDOT.

⁴⁷ Florida DOT and MoDOT.

⁴⁸ Arkansas DOT and MoDOT.

⁴⁹ Arkansas DOT.

⁵⁰ Alabama DOT, Arizona DOT, Florida DOT, and MoDOT.

⁵¹ Indiana DOT.

⁵² *See* Appendix B.

⁵³ The Utah DOT also reported that it uses real-time images from CCTV cameras without recording the images.

Section 503 outlines the objectives for research and technology that may be used, such as for active traffic and demand management, emergency operations, real-time transportation information, and impact of vehicle size and weight on congestion and on enhanced mode choice and intermodal connectivity.⁶⁵ Research is to be comprehensive and include “operational tests of intelligent vehicles, intelligent infrastructure systems, and other similar activities that are necessary to carry out this chapter.”⁶⁶

The secretary is expected to prioritize funding for projects that focus on improved traffic management, environmental impacts, and crash avoidance. The federal government may provide not more than 80 percent of a project’s funding when the project comes within one of the categories enumerated in 23 U.S.C. § 502(3).⁶⁷ ITS is to be implemented for passenger and freight transportation by all forms of surface transportation to meet the above goals.⁶⁸

B. Traffic Monitoring Systems

Federal regulations promulgated pursuant to 23 U.S.C. § 303 provide for the establishment in each state of a traffic monitoring system (TMS) for highways and public transportation facilities and equipment. The term “TMS” is defined as “a systematic process for the collection, analysis, summary, and retention of highway and transit related person and vehicular traffic data.”⁶⁹

A state is to use TMS data when providing data to the U.S. Department of Transportation (USDOT); when the data are used to support transportation management systems or studies or systems that are the USDOT’s responsibility; when the collection of data is supported by federal funding provided by USDOT programs; when the data are used in the apportionment or allocation of federal funds by the USDOT; when the data are used in the design or construction of a project funded by the Federal Highway Administration (FHWA); or when data are required as part of a federally mandated USDOT program.⁷⁰

C. Electronic Toll Collection

Electronic toll collection is defined as “the ability for vehicle operators to pay tolls automatically without slowing down from normal highway

speeds.”⁷¹ Unless FHWA grants an exception, any toll facility operating under the authority of Section 1604 of the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU) must use an electronic system to collect tolls.⁷²

Because of the breadth of the information collected by electronic tolling facilities, the regulations include a section on privacy:

A toll agency using electronic toll collection technology must develop, implement, and make publicly available privacy policies to safeguard the disclosure of any data that may be collected through such technology concerning any user of a toll facility operating pursuant to authority under a 1604 toll program, but is not required to submit such policies to FHWA for approval.⁷³

California law that governs electronic toll collection permits the collection of PII, including credit card numbers and billing addresses,⁷⁴ but requires that the transportation provider post its privacy policy clearly on its Web site.⁷⁵

Pennsylvania law governs the privacy of an account holder’s information for electronic toll collection. Under the statute, except for limited exceptions (e.g., criminal law enforcement actions or the enforcement of toll collection laws), toll collection

information shall not be deemed a public record under the Right-to-Know Law, nor shall it be discoverable by court order or otherwise or be offered in evidence in any action or proceeding which is not directly related to the discharge of duties under this section, the regulations of the commission or a violation of an account holder agreement.⁷⁶

New York, besides defining electronic toll collection and the methods used to obtain data, mandates that public data must be protected and that each department must have a privacy compliance officer.⁷⁷ The compliance officer is responsible for maintaining records of personal data that are collected and for assisting individuals in gaining access to information when it is requested.⁷⁸

Toll operators in Virginia may not sell or disclose “data to any entity other than for toll collection purposes.”⁷⁹

⁶⁵ 23 U.S.C. § 503 (2015) (terms not defined).

⁶⁶ 23 U.S.C. § 516(a) (2015).

⁶⁷ 23 U.S.C. § 516(c) (2015).

⁶⁸ 23 U.S.C. § 514(b) (2015).

⁶⁹ 23 C.F.R. § 500.202 (2015).

⁷⁰ 23 C.F.R. § 500.203 (2015).

⁷¹ 23 C.F.R. § 950.3 (2015).

⁷² 23 C.F.R. § 950.1 (2015).

⁷³ 23 C.F.R. § 950.5(c) (2015).

⁷⁴ CAL. STS. & HIGH. CODE § 31490 (2015).

⁷⁵ CAL. STS. & HIGH. CODE §§ 31490(b) and (c) (2015).

⁷⁶ 74 PA. CONS. STAT. § 8117(d)(1)(ii) (2015). *See also* 74 PA. CONS. STAT. § 8117(d)(2)(1) and (iii) (2015).

⁷⁷ N.Y. UNCONSOL. LAW §§ 6816-b (h)-(j) (2015).

⁷⁸ N.Y. COMP. CODES R. & REGS. tit. 17, §§ 2.3 (b)(2) and (4)(i) (2015).

⁷⁹ Phillips and Kohm, *supra* note 1, at P30.

III. WHETHER PRIVACY RIGHTS UNDER THE UNITED STATES CONSTITUTION APPLY TO PERSONAL AND LOCATIONAL DATA

A. Introduction

Privacy law in the United States is said to be a “disorganized body of law”⁸⁰ lacking a “comprehensive national regulatory structure.”⁸¹ Instead of a unified approach, privacy rights are created sporadically for a specific reason, often in response to changes in technology.⁸²

Privacy rights have been defined as the right to control the dissemination of one’s information⁸³ and to be free from government intrusion.⁸⁴ Although a “cluster of constitutional rights” protects citizens from various forms of government intrusion, decisions by the United States Supreme Court in recent years have narrowed an individual’s zone of privacy protected by the U.S. Constitution.⁸⁵

B. Evolution of Privacy Rights

In 1890, Samuel D. Warren and Louis D. Brandeis published an article entitled, “The Right to Privacy,”⁸⁶ in which they articulated the basis of a right to privacy in the United States.⁸⁷ The authors posited that an individual should have a legal remedy when the press “overstep[s] in every direction in the obvious bounds of propriety and of decency.”⁸⁸ Warren and Brandeis argued that the publishing of private facts “appeal[s] to the weak side of human nature” and “usurps the place of interest in brains capable of other things,” thus necessitating in their view the need to protect individuals’ privacy.⁸⁹ Although they recognized six limitations on the right to privacy,⁹⁰ they argued not only that society

should uphold an individual’s privacy rights, but also that a violation of privacy rights should be remediable either by compensation or, in rare cases, by an injunction.⁹¹ Following the Warren and Brandeis article, some courts held that privacy rights were fundamentally rooted in natural law,⁹² yet other courts rejected claims that a right to privacy existed.⁹³

A leading case on privacy rights is the United States Supreme Court’s 1965 decision in *Griswold v. Connecticut*,⁹⁴ which held that there is a right to privacy under the U.S. Constitution.⁹⁵ In *Griswold*, the petitioners were physicians who had provided their patients with contraceptives in violation of Connecticut law.⁹⁶ When the petitioners argued that the Connecticut statute violated the Fourteenth Amendment, the Court agreed that they had “standing to raise the constitutional rights of the married people with whom they had a professional relationship.”⁹⁷ However, the Court also held that there is a constitutional right to privacy, because the “specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy.”⁹⁸ Thus, the “right of association” is guaranteed by the First Amendment; the “right of the people to be secure in their persons, houses, papers, and effects[] against unreasonable searches and seizures” is secured by the Fourth Amendment; and a “zone of privacy which government may not force [a person] to surrender to his detriment” exists under the Fifth Amendment.⁹⁹

Because the constitutional guarantees created a zone of privacy, a “governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the

⁸⁰ Alain J. Lapter, *How the Other Half Lives (Revisited): Twenty Years Since Midler v. Ford, A Global Perspective on the Right of Publicity*, 15 TEX. INTELL. PROP. L.J. 239, 247 (2007) [hereinafter Lapter].

⁸¹ Douma and Deckenbach, *supra* note 2, at 300.

⁸² Garry, Douma, and Simon, *supra* note 2, at 102.

⁸³ J. Thomas McCarthy, *The Rights of Publicity and Privacy*, at § 1.6 (2013) (citing United States Department of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 761, 109 S. Ct. 1468, 1775-1776, 103 L. Ed. 2d 774, 788 (1989)) [hereinafter McCarthy].

⁸⁴ Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1361 (1992).

⁸⁵ McCarthy, *supra* note 83, at § 5.57.

⁸⁶ Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) [hereinafter Warren & Brandeis].

⁸⁷ McCarthy, *supra* note 83, at § 1.10.

⁸⁸ Warren & Brandeis, *supra* note 86, at 196.

⁸⁹ *Id.*

⁹⁰ *Id.* at 214–19.

⁹¹ *Id.* at 219–20.

⁹² McCarthy, *supra* note 83, at § 1.16 (citing *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902)).

⁹³ *Id.* § 1.17 (citing *Pavesich v. New England Life Ins. Co.*, 122 Ga. 190, 50 S.E. 68 (Ga.1905)).

⁹⁴ 381 U.S. 479, 85 S. Ct. 1678, 14 L. Ed. 2d 510 (1965).

⁹⁵ *Griswold*, 381 U.S. at 485–486, 85 S. Ct. at 1682, 14 L. Ed. 2d at 515–516.

⁹⁶ *Id.* at 480, 85 S. Ct. at 1679, 14 L. Ed. 2d at 512 (citing CONN. GEN. STAT. §§ 53-32, 54-196 (1958)).

⁹⁷ *Id.* at 484, 85 S. Ct. at 1681, 14 L. Ed. 2d at 514.

⁹⁸ *Id.* (citation omitted). There is a zone of privacy because of the constitutional “right of association” and the “right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures.” See *id.* (quoting U.S. CONST. amends. I and IV).

⁹⁹ *Id.* at 480–481, 85 S. Ct. at 1679, 14 L. Ed. 2d at 512.

area of protected freedoms.”¹⁰⁰ In a concurring opinion, Justice Goldberg stated that because personal liberties are grounded in “traditions and conscience,” people’s liberties are “not confined to the specific terms of the Bill of Rights.”¹⁰¹

After the *Griswold* decision, the Supreme Court and lower courts interpreted the scope of privacy rights to include a “seemingly disparate cluster of constitutional rights against government intrusion.”¹⁰² As privacy rights evolved after *Griswold*, they came to include protection against “government intrusion into a person’s mind and thought processes,”¹⁰³ “intrusion into a person’s zone of private seclusion,”¹⁰⁴ and “intrusion into a person’s right to make certain personal decisions, such as whether to use contraceptives or have an abortion.”¹⁰⁵

However, more recent jurisprudence has limited the zone of privacy established by the *Griswold* case and its progeny. Rather than expand the zone of privacy so that it would apply to an individual’s right to control the collection of personal data or its dissemination, the Supreme Court has narrowed the zone.¹⁰⁶ Thus, presently, there is neither a “specific constitutional right to privacy,” nor is there a constitutional right to privacy in one’s personal or locational information.¹⁰⁷

In 1977, in *Whalen v. Roe*,¹⁰⁸ the Supreme Court unanimously held “that New York State had the right to collect data about individuals and create a database if for the public good and with adequate security measures taken to protect the privacy and identification of individuals.”¹⁰⁹ In an opinion by Justice Stevens, the Court stated that it was not “unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files..., much of which is personal in character and potentially embarrassing or harmful if disclosed.”¹¹⁰

¹⁰⁰ *Id.* at 485, 85 S. Ct. at 1682, 14 L. Ed. 2d at 515–516 (internal citation omitted).

¹⁰¹ *Id.* at 486, 85 S. Ct. at 1683, 14 L. Ed. 2d at 516–517 (Goldberg, J., concurring).

¹⁰² McCarthy, *supra* note 83, at § 5.57.

¹⁰³ *Id.* (citing *Ramie v. City of Hedwig Village, Tex.*, 765 F.2d 490, 492 (5th Cir. 1985)).

¹⁰⁴ *Id.* (citing *Stanley v. Georgia*, 394 U.S. 557, 89 S. Ct. 1243, 22 L. Ed. 2d 542 (1969)).

¹⁰⁵ *Id.* See Paul v. Davis, 424 U.S. 693, 713, 96 S. Ct. 1155, 1166, 47 L. Ed. 2d 405, 421 (1976); *Bowers v. Hardwick*, 478 U.S. 186, 106 S. Ct. 2841, 92 L. Ed. 2d 140 (1986).

¹⁰⁶ Phillips and Kohm, *supra* note 1, at P6.

¹⁰⁷ *Id.* at P4.

¹⁰⁸ 429 U.S. 589, 97 S. Ct. 869, 51 L. Ed. 2d 64 (1977).

¹⁰⁹ Phillips and Kohm, *supra* note 1, at P6.

¹¹⁰ *Whalen*, 429 U.S. at 605, 97 S. Ct. at 879, 51 L. Ed. 2d at 77 (emphasis added).

Justice Stevens continued:

The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York’s statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual’s interest in privacy. *We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions.*¹¹¹

The *Whalen* Court held that the record did “not establish an invasion of any right or liberty protected by the Fourteenth Amendment.”¹¹²

In a 1981 Fifth Circuit case, *Fadjo v. Coon*,¹¹³ the plaintiff alleged that the State of Florida had conspired with others to divulge “the most private details” of the plaintiff’s life.¹¹⁴ The court recognized a privacy right in the plaintiff’s confidential information, but held that the right had to be balanced against any state interest in disclosure. Although the plaintiff had alleged the other elements required for a § 1983 action, discussed in Section III.E, the question for the Fifth Circuit was “whether Fadjo has alleged [the] deprivation of a constitutional right.”¹¹⁵ The Fifth Circuit stated that

[t]he privacy right has been held to protect decision making when the decision in question relates to matters such as “marriage, procreation, contraception, family relationships, and child rearing and education.” ...Matters falling outside the scope of the decision making branch of the privacy right may yet implicate the individual’s interest in nondisclosure or confidentiality.¹¹⁶

The court held that

Fadjo clearly states a claim under the confidentiality branch of the privacy right. He does not claim that the state lacked authority to obtain personal information from him while pursuing a criminal investigation. However, even if the information was properly obtained, the state may have invaded Fadjo’s privacy in revealing it to Julson and the insurance companies. Alternatively, although the state could compel Fadjo’s testimony it could delve into his privacy only in pursuit of aims recognized as legitimate and proper. *Implicit in both formulations of the complaint is the allegation that no legitimate state purpose existed sufficient to outweigh the invasion into Fadjo’s privacy.*¹¹⁷

The court reversed the district court’s dismissal of the complaint.¹¹⁸

¹¹¹ *Id.* at 605–606, 97 S. Ct. at 879, 51 L. Ed. 2d at 77.

¹¹² *Id.* at 606, 97 S. Ct. at 879–880, 51 L. Ed. 2d at 77.

¹¹³ 633 F.2d 1172 (5th Cir. 1981).

¹¹⁴ *Id.* at 1174.

¹¹⁵ *Id.* at 1175.

¹¹⁶ *Id.* (citations omitted).

¹¹⁷ *Id.* (emphasis added).

¹¹⁸ *Id.* at 1177.

In *Fadjo*, the court seems to be clear that when *confidentiality* is the privacy issue, “a balancing standard is appropriate as opposed to [a] compelling state interest analysis that is required when the *autonomy* of decision making is at issue.”¹¹⁹ The *Fadjo* court did not hold that when the confidentiality of personal information is at stake the governmental interest has to be compelling, but did indicate that “‘more than mere rationality must be demonstrated’ to justify a state intrusion.”¹²⁰

In 1987 in *Borucki v. Ryan*,¹²¹ the First Circuit agreed that since the *Griswold* decision, a “‘right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution.’”¹²² Nevertheless, the court held that the right to privacy does not emanate from the “penumbra of other fundamental rights” but is “founded” in the Fourteenth Amendment’s “concept of personal liberty.”¹²³ Although recognizing that the Third and Fifth Circuits had held “that there is an independent right of confidentiality applicable to personal information contained in medical, financial, and other personal records,”¹²⁴ the *Borucki* court held that “[t]he personal rights found in this guarantee of personal privacy must be limited to those which are ‘fundamental’ or ‘implicit within the concept of ordered liberty....’”¹²⁵ The court observed that “[m]ost of the courts finding a right of confidentiality had used a balancing test to assess violations of that right;”¹²⁶ however, the court held that the plaintiff’s complaint based on the prosecutor’s disclosure of information about the plaintiff’s competency to stand trial in another case failed to state a claim.¹²⁷

In its opinion in *Borucki*, the court was guided by the Supreme Court’s decision in 1976 in *Paul v. Davis*.¹²⁸ In *Paul*, although the plaintiff had been arrested but not convicted of shoplifting, the state police had distributed a flyer identifying the

plaintiff as an “active shoplifter.” The *Borucki* court stated:

Under *Paul*, an allegation that *government dissemination of information* or government defamation has caused damage to reputation, even with all attendant emotional anguish and social stigma, *does not in itself state a cause of action* for violation of a constitutional right; infringement of more “tangible interests” ... must be alleged as well.¹²⁹

In a similar analysis in *Kallstrom v. City of Columbus*,¹³⁰ the Sixth Circuit held that it is only when an individual’s privacy interest is one of “constitutional dimension” that the court will find it necessary to “balance an individual’s interest in nondisclosure of informational privacy against the public’s interest in and need for the invasion of privacy....”¹³¹ Moreover, as the same court would explain later in *Lambert v. Hartman*,¹³² the Supreme Court has identified only two types of interests that come within the substantive due process protection of the Fourteenth Amendment. The first interest has to do with “independence in making certain kinds of important decisions,” such as “matters relating to procreation, marriage, contraception, family relationships, and child rearing and education.”¹³³ The second privacy interest recognized by the Supreme Court is “in avoiding disclosure of personal matters.”¹³⁴

Nevertheless, in regard to the privacy interest in avoiding disclosure of personal data, the Sixth Circuit stated in *Lambert* that the court had “recognized an informational-privacy interest of constitutional dimension in only two instances: (1) where the release of personal information could lead to bodily harm ..., and (2) where the information released was of a sexual, personal, and humiliating nature....”¹³⁵

The *Lambert* court stated that the holdings in *Whalen*, and in *Nixon v. Administrator of General Services*,¹³⁶ had been “narrowly construed” so as “to extend the right to informational privacy only to interests that implicate a fundamental liberty

¹¹⁹ *Id.* at 1176 (citations omitted) (emphasis added).

¹²⁰ *Id.* (citations omitted).

¹²¹ 827 F.2d 836, 839 (1st Cir. 1987).

¹²² *Id.* at 839 (quoting *Roe v. Wade*, 410 U.S. 113, 152, 93 S. Ct. 705, 35 L. Ed. 2d 147 (1973)).

¹²³ *Id.* (citing *Roe v. Wade*, 410 U.S. 113, 153, 93 S. Ct. 705, 35 L. Ed. 2d 147 (1973) and *Whalen v. Roe*, 429 U.S. 589, 598–599 N 23, 97 S. Ct. 869, 51 L. Ed. 2d 64 (1977)).

¹²⁴ *Id.* at 845 (citing *United States v. Westinghouse Electric Corp.*, 638 F.2d 570 (3d Cir. 1980); *Plante v. Gonzalez*, 575 F.2d 1119, 1132 (5th Cir. 1978); *Duplantier v. United States*, 606 F.2d 654, 670 (5th Cir. 1979); *Fadjo v. Coon*, 633 F.2d 1172 (Fifth Cir. 1981)).

¹²⁵ *Borucki*, 827 F. 2d at 839 (quoting *Roe v. Wade*, 410 U.S. 113, 152, 93 S. Ct. 705, 35 L. Ed. 2d 147 (1973)).

¹²⁶ *Id.* at 848 (citations omitted) (emphasis added).

¹²⁷ *Id.* at 849.

¹²⁸ 424 U.S. 693, 96 S. Ct. 1155, 47 L. Ed. 2d 405 (1976).

¹²⁹ *Borucki*, 827 F.2d at 842-843 (citations omitted).

¹³⁰ 136 F.3d 1055, 1061 (6th Cir. 1998) (*overruled in part as stated in* *Frost v. Blom*, 2011 U.S. Dist. LEXIS 52571 (W.D. Mo. May 17, 2011) (stating that the Eighth Circuit has rejected the *Kallstrom* decision because the court “erroneously applied a negligence standard instead of the subjective deliberate indifference standard”) (citation omitted)).

¹³¹ *Id.* at 1061 (citation omitted).

¹³² 517 F.3d 433 (6th Cir. 2008), cert. denied, 2009 U.S. LEXIS 272 (U.S., Jan. 12, 2009).

¹³³ *Id.* at 440 (citations omitted) (internal quotation marks omitted).

¹³⁴ *Id.* (citations omitted) (internal quotation marks omitted).

¹³⁵ *Id.*

¹³⁶ 433 U.S. 425, 97 S. Ct. 2777, 53 L. Ed. 2d (1977).

interest.”¹³⁷ The *Lambert* court’s analysis appears to impose an additional requirement before a constitutional privacy interest would be implicated—the state’s action in disclosing personal data must have “created a special danger” that led to the plaintiff’s harm or humiliation.¹³⁸

The *Lambert* court was clear that the government’s disclosure, for example, of a person’s Social Security number does not rise to the level of a “fundamental right” or a right that is “‘deeply rooted in this Nation’s history and tradition’ or ‘implicit in the concept of ordered liberty.’”¹³⁹

It appears, therefore, that there is authority holding that when a privacy interest that comes within the confidentiality branch of privacy law has been violated, the government must show something more than “mere rationality” as justification for disseminating personal information. On the other hand, a privacy interest violated by government intrusion does not implicate a constitutional right unless the privacy interest at stake is a fundamental right or one that is implicit in the concept of ordered liberty. In the latter situation, the privacy interest must be balanced against a compelling governmental interest in disclosure.

Finally, at least one Supreme Court justice has suggested that state legislatures are better suited than the federal courts to decide whether privacy rights should be enlarged. In a concurring opinion in *Riley v. California*,¹⁴⁰ discussed *infra*, Justice Alito stated that

[i]n light of the growing privacy concerns of modern technology, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred.¹⁴¹

Justice Alito’s opinion is that the “Court is poorly positioned to understand and evaluate” sensitive privacy interests arising, for example, from the use of modern cell phones.¹⁴²

In sum, it does not appear that the disclosure by a transportation agency of secure data, including an individual’s PII, or of monitoring or locational data would violate a right to privacy under the U.S. Constitution.¹⁴³

¹³⁷ *Lambert*, 517 F.3d at 440 (citation omitted).

¹³⁸ *Id.* at 439 (citations omitted).

¹³⁹ *Id.* at 443 (citations omitted).

¹⁴⁰ 134 S. Ct. 2473, 2497, 189 L. Ed. 2d 430, 456 (2014) (Alito, J., concurring).

¹⁴¹ *Id.* at 2497, 189 L. Ed. 2d at 456.

¹⁴² *Id.* at 2497, 189 L. Ed. 2d at 455.

¹⁴³ See *Lambert*, 517 F.3d at 440; Phillips and Kohm, *supra* note 1, at P4.

C. The Fourth Amendment and a Constitutional Right to Privacy

Under the Fourth Amendment, “warrantless searches are permissible only when an individual has a substantially reduced expectation of privacy.”¹⁴⁴ Although the collection or disclosure of data by transportation agencies may raise privacy issues, the courts have held that a person’s reasonable expectation of privacy is reduced with respect to automobile searches, searches incident to an arrest, and seizures of items in plain view that are believed to be contraband.¹⁴⁵

In *Katz v. United States*,¹⁴⁶ the Supreme Court held that because the Federal Bureau of Investigation (FBI) failed to obtain a warrant prior to listening to and recording the petitioner’s conversations, the petitioner’s conviction had to be reversed.¹⁴⁷ Relevant to the issue of data collection, however, is that the *Katz* Court stated that “the Fourth Amendment cannot be translated into a general constitutional ‘right to privacy.’”¹⁴⁸ Furthermore, “what a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection.”¹⁴⁹

Although the Supreme Court precedents since *Katz* fail to show a “clear pattern” on what the “acceptable limits of government action” are under the Fourth Amendment,¹⁵⁰ the Supreme Court “has not found information about an individual’s activities in public to be protected.”¹⁵¹ For example, in a 1983 decision in *United States v. Knotts*,¹⁵² Minnesota law enforcement officers had placed a beeper in a drum containing chloroform purchased by the respondent’s codefendants to track them from Minnesota to a cabin in Wisconsin.¹⁵³ The law enforcement agents obtained a search warrant for the cabin, discovered a drug lab on the premises, and charged the respondent with conspiracy to manufacture controlled

¹⁴⁴ *Bourgeois v. Peters*, 387 F.3d 1303, 1314 (11th Cir. 2004).

¹⁴⁵ *Id.* at 1314–1315 (citations omitted).

¹⁴⁶ 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967). Some courts regard the *Katz* decision as having been abrogated or superseded. See, e.g., *State v. Earls*, 214 N.J. 564, 70 A.3d 630 (2013) (stating abrogated) and *United States v. Koyomejian*, 946 F.2d 1450 (9th Cir. Cal. 1991) (stating superseded).

¹⁴⁷ *Katz*, 389 U.S. at 358–359, 88 S. Ct. at 514–515, 19 L. Ed. 2d at 586.

¹⁴⁸ *Id.* at 350, 88 S. Ct. at 510, 19 L. Ed. 2d at 581 (footnotes omitted).

¹⁴⁹ *Id.* at 351, 88 S. Ct. at 511, 19 L. Ed. 2d at 58 (citation omitted).

¹⁵⁰ Phillips and Kohm, *supra* note 1, at P35.

¹⁵¹ Douma and Deckenbach, *supra* note 2, at 305.

¹⁵² 460 U.S. 276, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983).

¹⁵³ *Knotts*, 460 U.S. at 277, 103 S. Ct. at 1083, 75 L. Ed. 2d at 59.

substances.¹⁵⁴ The respondent argued that his conviction had to be reversed because the use of the beeper to track his movements violated his right to privacy under the Fourth Amendment.¹⁵⁵

The *Knotts* Court held that there is “no reasonable expectation of privacy” for “a person traveling in an automobile on public thoroughfares.”¹⁵⁶ Thus, law enforcement could place a beeper in a container and monitor the movements of the car in which the container was placed.¹⁵⁷ The only issue in *Knotts* was whether the monitoring of the car, not the installation of the beeper in the container, was a violation of the Fourth Amendment. The Court held that the government’s action in monitoring the beeper signals was neither a “search” nor a “seizure” within the meaning of the Fourth Amendment; therefore, a warrant was not required.¹⁵⁸ The Court reversed the appellate court’s reversal of the appellant’s conviction.¹⁵⁹

In 1999, in *Wyoming v. Houghton*,¹⁶⁰ the Supreme Court held that a police officer’s search of a passenger’s purse during a traffic stop was a legitimate exception to the warrant requirement of the Fourth Amendment. The Court, in an opinion by Justice Scalia, held that although the search intruded on the passenger’s privacy, “the governmental interests at stake [were] substantial.”¹⁶¹ Furthermore, because a passenger’s privacy interests are “considerably diminished” when the passenger is traveling on a public thoroughfare, the weighing of the passenger’s and the government’s interests “militate in favor of the needs of law enforcement.”¹⁶²

Being on a public highway does not obviate completely, of course, a person’s right to a reasonable expectation of privacy protected by the Fourth Amendment. In 2009, in *Arizona v. Gant*,¹⁶³ the Supreme Court held that a search was not lawful when the arrestee had been “handcuffed[] and locked in the back of the patrol car” on charges of driving with a suspended license.¹⁶⁴ The Court held that the police are authorized to search a vehicle

¹⁵⁴ *Id.* at 277–279, 103 S. Ct. at 1084, 75 L. Ed. 2d at 59–60.

¹⁵⁵ *Id.* at 279, 103 S. Ct. at 1084, 75 L. Ed. 2d at 60.

¹⁵⁶ *Id.* at 281, 103 S. Ct. at 1085, 75 L. Ed. 2d at 62.

¹⁵⁷ *Id.* at 277–280, 103 S. Ct. at 1083–1084, 75 L. Ed. 2d at 59–60.

¹⁵⁸ *Id.* at 284–285, 103 S. Ct. at 1087, 75 L. Ed. 2d at 64 (quoting *United States v. Knotts*, 662 F.2d 515, 518 (8th Cir. 1981) (internal citation omitted)).

¹⁵⁹ *Id.* at 285, 103 S. Ct. at 1087, 75 L. Ed. 2d at 64.

¹⁶⁰ 526 U.S. 295, 119 S. Ct. 1297, 143 L. Ed. 2d 408 (1999).

¹⁶¹ *Id.* at 304, 119 S. Ct. at 1302, 143 L. Ed. 2d at 417.

¹⁶² *Id.* at 303, 306, 119 S. Ct. at 1302–1303, 143 L. Ed. 2d at 417.

¹⁶³ 556 U.S. 332, 129 S. Ct. 1710, 173 L. Ed. 2d 485 (2009).

¹⁶⁴ *Id.* at 335, 129 S. Ct. at 1714, 173 L. Ed. 2d at 491.

incident to an arrest only when the person under arrest was unsecured and within reaching distance of the passenger compartment at the time of the search.¹⁶⁵ The Court stated that “[a]lthough we have recognized that a motorist’s privacy interest in his vehicle is less substantial than in his home...the former interest is nevertheless important and deserving of constitutional protection.”¹⁶⁶

In 2010, Justice Kennedy stated in his opinion for the Court in *City of Ontario v. Quon*¹⁶⁷ that “[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”¹⁶⁸ Justice Kennedy stated that the Court would refrain from issuing a broad ruling that may fail to consider the evolution of technology and society’s response to developments; thus, it was “preferable to dispose of this case on narrower grounds.”¹⁶⁹

In 2012, in *United States v. Jones*,¹⁷⁰ the Court held that the government’s warrantless installation of a GPS device on a vehicle to monitor it was a search under the Fourth Amendment.¹⁷¹ Jones, the owner and operator of a night club in Washington, DC, became the target of an investigation by a joint FBI and Metropolitan Police task force on suspicion of trafficking in narcotics. Based on the results of prior surveillance, the government sought and obtained a warrant from a federal court in the District of Columbia authorizing the use of an electronic tracking device to be installed on a Jeep vehicle registered in the name of Jones’s wife. However, the GPS tracking device was installed in Maryland. The government conceded that it had failed to comply with the warrant, but argued that a warrant was not needed.¹⁷²

Over a 4-week period, the device relayed over 2,000 pages of data. The government ultimately obtained a multiple count indictment for conspiracy and the possession of cocaine with the intent to distribute it. The U.S. District Court for the District of Columbia granted in part and denied in part a motion to suppress the data obtained from the GPS. The court suppressed the admission of data obtained while the Jeep was parked in a garage adjacent to the Jones’s residence, but allowed the admission of

¹⁶⁵ *Id.* at 343, 129 S. Ct. at 1719, 173 L. Ed. 2d at 496 (citing *New York v. Belton*, 453 U.S. 454, 101 S. Ct. 2860, 69 L. Ed. 2d 768 (1981)).

¹⁶⁶ *Id.* at 345, 129 S. Ct. at 1720, 173 L. Ed. 2d at 497 (citation omitted).

¹⁶⁷ 560 U.S. 746, 130 S. Ct. 2619, 177 L. Ed. 2d 216 (2010).

¹⁶⁸ *Id.* at 759, 130 S. Ct. at 2629, 177 L. Ed. 2d at 227.

¹⁶⁹ *Id.* at 760, 130 S. Ct. at 2630, 177 L. Ed. 2d at 227.

¹⁷⁰ 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012).

¹⁷¹ *Id.* at 948–949, 181 L. Ed. 2d at 917.

¹⁷² *Id.* at 948 and N 1, 181 L. Ed. 2d at 917 and N 1.

the remaining data on the basis that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”¹⁷³ The U.S. Circuit Court for the District of Columbia reversed the conviction because of the admission of evidence obtained by a “warrantless use of the GPS device....”¹⁷⁴

In an opinion by Justice Scalia, the Supreme Court unanimously affirmed the circuit court’s decision. In the opinion, Justice Scalia explained that the Court was not abandoning prior precedent holding that the Fourth Amendment “protects people, not places,”¹⁷⁵ and that a violation of the Fourth Amendment occurs when government officers violate a person’s “reasonable expectation of privacy....”¹⁷⁶ After noting that the Court has deviated from its prior “property-based approach,” Justice Scalia explained that the Court’s decision in *Jones* was entirely consistent with its prior decisions because “the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.”¹⁷⁷ In other cases when the government installed a beeper, it did so in property that belonged to a third party and before the property came into the possession of the defendant, with the consent of the original owner of the property; thus, there was no violation of the Fourth Amendment.¹⁷⁸

In this case, *Jones* possessed the Jeep before “the Government trespassorily inserted the information-gathering device,” a detail that put the *Jones* case “on a much different footing.”¹⁷⁹ Thus, the “physical intrusion” that occurred in the *Jones* case “would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.”¹⁸⁰

The methods of data collection discussed in the digest do not involve a warrantless physical trespass and search as occurred in the *Jones* case. A violation of the Fourth Amendment occurs when the government violates a person’s reasonable expectation of privacy without a warrant.¹⁸¹ Justice Scalia’s opinion in *Jones* stated that “[s]ituations involving merely the transmission of electronic

signals without trespass would remain subject to *Katz* analysis.”¹⁸² The Court stated that it “has to date not deviated from the understanding that mere visual observation does not constitute a search.”¹⁸³ The Court reiterated that “[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”¹⁸⁴ The Court did not decide whether the collection of the same information electronically without trespassing, which is available already by visual observation, would be an unconstitutional invasion of privacy. The Court opined that attempting to answer the question in the *Jones* case would “lead[] us needlessly in additional thorny problems.”¹⁸⁵

The Court’s opinions in *Gant*, *Jones*, and *Quon* illustrate the Supreme Court’s appreciation of the privacy issues presented by the use of technology to collect and retain data on individuals. In a concurring opinion in *Jones*, Justice Sotomayor observed that the use of electronic surveillance may “alter the relationship between a citizen and government in a way that is inimical to democratic society.”¹⁸⁶

Thereafter, in 2014 in *Riley v. California*,¹⁸⁷ the Court held that absent a warrant, the police might not search digital information on a cell phone seized from an individual who has been arrested.¹⁸⁸ The Court’s reasoning was that, because cell phones contain “vast quantities of personal information,” searches of cell phones are distinguishable from other physical searches.¹⁸⁹ Searches of cell phones “implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.”¹⁹⁰ Finally, the Court observed that the “fact that technology now allows an individual to carry such [private] information in his hand does not make the information any less worthy of the protection for which the Founders fought.”¹⁹¹

In sum, the Court has held that individuals using public highways have a diminished expectation of

¹⁷³ *Id.* at 948, 181 L. Ed. 2d at 917 (citation omitted).

¹⁷⁴ *Id.* at 949, 181 L. Ed. 2d at 917 (citation omitted).

¹⁷⁵ *Id.* at 950, 181 L. Ed. 2d at 918 (citation omitted).

¹⁷⁶ *Id.* at 950, 181 L. Ed. 2d at 916–919 (citations omitted).

¹⁷⁷ *Id.* at 952, 181 L. Ed. 2d at 921 (emphasis added).

¹⁷⁸ *Id.* (discussing and distinguishing cases).

¹⁷⁹ *Id.*

¹⁸⁰ *Id.* at 949, 181 L. Ed. 2d at 918.

¹⁸¹ *Id.* at 949, 181 L. Ed. 2d at 919 (citing *Katz v. United States*, 389 U.S. 347, 360, 88 S. Ct. 507, 196 L. Ed. 2d 576 (1967)).

¹⁸² *Id.* at 953, 181 L. Ed. 2d at 922.

¹⁸³ *Id.* at 953, 181 L. Ed. 2d at 922 (citing *Kyllo*, 533 U.S. at 31–32, 121 S. Ct. 2038, 150 L. Ed. 2d 941).

¹⁸⁴ *Id.* at 953, 181 L. Ed. 2d at 923 (citation omitted).

¹⁸⁵ *Id.* at 954, 181 L. Ed. 2d at 923.

¹⁸⁶ *Id.* at 956, 181 L. Ed. 2d at 925 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011)).

¹⁸⁷ 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014).

¹⁸⁸ *Id.* at 2485, 2495, 189 L. Ed. 2d at 442, 452.

¹⁸⁹ *Id.* at 2485, 189 L. Ed. 2d at 442.

¹⁹⁰ *Id.* at 2488, 189 L. Ed. 2d at 446.

¹⁹¹ *Id.* at 2495, 189 L. Ed. 2d at 452.

privacy.¹⁹² It appears that using technology to enhance and record the visual observation of motorists on public highways is not a violation of a constitutional right to privacy. On the other hand, the government's attachment of a GPS device to a vehicle owned or used by one suspected of a crime without a warrant, or the government's seizure of a cell phone in a vehicle without a warrant, are entirely different matters and distinguishable from the routine collection of secure data or monitoring data by transportation agencies.

D. Whether There Is an Implied Constitutional Claim for a Privacy Violation

In 1971, in *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*,¹⁹³ the United States Supreme Court held that an implied cause of action exists for a violation of an individual's rights under the Fourth Amendment.¹⁹⁴ More recently, in *Ashcroft*, the Court explained that “[i]n the limited settings where *Bivens* does apply[] the implied cause of action is the ‘federal analog to suits brought against state officials under... § 1983.’”¹⁹⁵

In *Bivens*, without a warrant for a search or for an arrest, Federal Bureau of Narcotics agents entered the petitioner's apartment, arrested him in front of his family, and searched his apartment for narcotics.¹⁹⁶ The Supreme Court held that

the Fourth Amendment operates as a limitation upon the exercise of federal power regardless of whether the State in whose jurisdiction that power is exercised would prohibit or penalize the identical act if engaged in by a private citizen. It guarantees to citizens of the United States the absolute right to be free from unreasonable searches and seizures

¹⁹² *Knotts*, 460 U.S. at 281, 103 S. Ct. at 1085, 75 L. Ed. 2d at 62. See also *California v. Carney*, 471 U.S. 386, 390–394, 105 S. Ct. 2066, 2068–2071, 85 L. Ed. 2d 406, 412–415 (1956); *United States v. Moreno*, 1994 U.S. App. LEXIS 31365, at *1 (9th Cir. 1994); *South Dakota v. Opperman*, 428 U.S. 364, 368, 96 S. Ct. 3092, 3096, 49 L. Ed. 2d 1000, 1004–1005 (1976); *Cardwell v. Lewis*, 417 U.S. 583, 590–591, 94 S. Ct. 2464, 2469–2470, 41 L. Ed. 2d 325, 334–336 (1974); *Commonwealth v. Gary*, 625 Pa. 183, 196, 91 A.3d 102, 110–112 (Pa. 2013). See also *People v. Case*, 220 Mich. 379, 388–989, 190 N.W. 289, 292 (Mich. 1922).

¹⁹³ 403 U.S. 388, 91 S. Ct. 1999, 29 L. Ed. 2d 619 (1971) (holding that the plaintiff was entitled to redress for his injuries caused by the federal agents' violation of his Fourth Amendment rights), *on remand*, 456 F.2d 1339 (2d Cir. N.Y. 1972) (holding that the federal agents were not immune from damages suits based upon allegations of constitutional violations, but the defenses of good faith and reasonable belief were available).

¹⁹⁴ *Bivens*, 403 U.S. at 389, 91 S. Ct. at 2001, 29 L. Ed. 2d at 622.

¹⁹⁵ *Ashcroft*, 556 U.S. at 675, 129 S. Ct. at 1948, 173 L. Ed. 2d at 882 (citations omitted).

¹⁹⁶ *Bivens*, 403 U.S. at 389, 91 S. Ct. at 2001, 29 L. Ed. 2d at 622.

carried out by virtue of federal authority. And “where federally protected rights have been invaded, it has been the rule from the beginning that courts will be alert to adjust their remedies so as to grant the necessary relief.”¹⁹⁷

The *Bivens* Court held that an implied cause of action exists under the Fourth Amendment when a petitioner “can demonstrate an injury consequent upon the violation by federal agents of his Fourth Amendment rights” and that the petitioner may “redress his injury...in the federal courts.”¹⁹⁸

The jurisprudence since *Bivens* on whether particular conduct supports a specific constitutional claim for which there is an implied right of action has been inconsistent with the courts recognizing some claims while dismissing others.¹⁹⁹ A decision on whether to recognize a *Bivens* claim has depended in part on an evaluation of the particular constitutional claim and on whether there were “available alternative remedies.”²⁰⁰

Legislation in 1974 and 1988 has affected *Bivens* claims. The Federal Tort Claims Act (FTCA) precludes claims for certain intentional torts against the United States under 28 U.S.C. § 1346(a)(2). In 1974, however, Congress amended the FTCA to allow claims for assault, battery, false imprisonment, false arrest, abuse of process, or malicious prosecution caused by acts or omissions of United States investigative or law enforcement officers. The amendment together with 28 U.S.C. § 2679(b)(2)(A) “specifically preserves and ratifies the *Bivens* remedy.”²⁰¹ However, the amendment to the FTCA does not appear to be relevant to the subject matter of this digest.

On the other hand, the Federal Employees Liability Reform and Tort Compensation Act of 1988

¹⁹⁷ *Id.* at 392, 91 S. Ct. at 2002, 29 L. Ed. 2d at 624 (citation omitted).

¹⁹⁸ *Id.* at 397, 91 S. Ct. at 2004, 29 L. Ed. 2d at 627. See *Yorinsk v. Imbert*, 39 F. Supp. 3d 218–220 (D.D.C. 2014) (holding that constitutional tort claims brought pursuant to *Bivens* do not authorize injunctive relief) and *Dorwart v. Caraway*, 2002 MT 240, P44, 312 Mont. 1, 15, 58 P.3d 128, 136 (Mont. 2002) (holding that “the *Bivens* line of authority buttressed by § 874A of the *Restatement (Second) of Torts* are sound reasons for applying a cause of action for money damages for violations of those self-executing provisions of the Montana Constitution”). See also *Wood v. Moss*, 134 S. Ct. 2056, 2066, 188 L. Ed. 2d 1039, 1050–1051 (2014) (holding that the “implied right of action for damages against federal officers” extends to First Amendment claims).

¹⁹⁹ James E. Pfander and David Baltmanis, *Rethinking Bivens: Legitimacy and Constitutional Adjudication*, 98 GEO. L. J. 117, 118 (2009) [hereinafter Pfander and Baltmanis].

²⁰⁰ *Id.* at 121, 126.

²⁰¹ *Id.* at 131.

(Westfall Act) may have some relevance to the digest.²⁰² In the Westfall Act, Congress “virtually” immunized federal government officials from liability under state common law by “substituting the government as a defendant under the FTCA for these claims,” while “preserving the right of individuals to pursue *Bivens* actions for a ‘violation of the Constitution of the United States.’”²⁰³ Under 28 U.S.C. § 2679(d)(1), if the Attorney General certifies that a

defendant employee was acting within the scope of his office or employment at the time of the incident out of which the claim arose, any civil action or proceeding commenced upon such claim in a United States district court shall be deemed an action against the United States under the provisions of this title and all references thereto, and the United States shall be substituted as the party defendant.

Nevertheless, a “plaintiff must still allege and prove an actionable constitutional violation and overcome any qualified immunity defense.”²⁰⁴ In addition, the availability of alternative federal remedies could preclude a *Bivens* claim.²⁰⁵

The prevailing view on the viability of *Bivens* claims is that, first, “the Westfall Act changed the nature of the *Bivens* question” by immunizing federal employees from private lawsuits based on acts performed within the scope of their employment and converting them into FTCA suits against the United States.²⁰⁶ Second, the “the Westfall Act...explicitly

²⁰² Federal Employees Liability Reform and Tort Compensation Act of 1988 (Westfall Act), Pub. L. No. 100-694, 102 Stat. 4563.

²⁰³ Pfander and Baltmanis, *supra* note 199, at 131. See also HENRY COHEN AND VIVIAN S. CHU, CONG. RESEARCH SERV., FEDERAL TORT CLAIMS ACT 16 (April 27, 2009) [hereinafter Cohen and Chu] (stating that the Westfall Act immunizes a federal employee from liability under state law but that a federal employee may be sued for violating the Constitution or violating a federal statute that authorizes suit against an individual).

²⁰⁴ Pfander and Baltmanis, *supra* note 199, at 132.

²⁰⁵ *Id.*

²⁰⁶ Carlos M. Vazquez and Stephen I. Vladeck, *State Law, the Westfall Act, and the Nature of the Bivens Question*, 161 U. PA. L. REV. 509, 517 (2013) (citing 28 U.S.C. § 2679(b)) [hereinafter Vazquez and Vladeck]. 28 U.S.C. § 2679(b) (2015) states:

(1) The remedy against the United States provided by sections 1346(b) and 2672 of this title for injury or loss of property, or personal injury or death arising or resulting from the negligent or wrongful act or omission of any employee of the Government while acting within the scope of his office or employment is exclusive of any other civil action or proceeding for money damages by reason of the same subject matter against the employee whose act or omission gave rise to the claim or against the estate of such employee. Any other civil action or proceeding for money damages arising out of or relating to the same subject matter against the

preserves actions “brought for a violation of the Constitution of the United States.”²⁰⁷ Writers have argued that in 2012 the Supreme Court in *Minneci v. Pollard*²⁰⁸ “endorsed the prevailing reading of the Westfall Act as preempting state law remedies against federal officials, even for conduct that violates the Constitution.”²⁰⁹ Thus, “[a] federal official who commits a constitutional tort is not subject to liability under state law (because of the Westfall Act), and no statute similar to § 1983 makes federal officials liable under federal law for violating another person’s constitutional rights.”²¹⁰ Thus, the Westfall Act “leaves the federal *Bivens* action as the sole remedy against [a federal] official,”²¹¹ but “the Court has essentially abandoned the practice of recognizing implied rights of action to enforce federal statutory rights.”²¹²

Another scholar writing on privacy law and post-*Bivens* cases argues that the Supreme Court is unlikely to create new *Bivens* claims for violations of privacy and highlights several obstacles to a *Bivens* claim against a federal official.²¹³ First, as discussed in the article, in 2009 in *Ashcroft v. Iqbal*,²¹⁴ Justice Kennedy stated that the Court in *Bivens* “recognized for the first time an implied private action for damages against federal officers alleged to have violated a citizen’s constitutional rights.”²¹⁵ However, Justice

employee or the employee’s estate is precluded without regard to when the act or omission occurred.

(2) Paragraph (1) does not extend or apply to a civil action against an employee of the Government—

(A) which is brought for a violation of the Constitution of the United States, or

(B) which is brought for a violation of a statute of the United States under which such action against an individual is otherwise authorized.

(Emphasis added).

²⁰⁷ Vazquez and Vladeck, *supra* note 206, at 517 (quoting 28 U.S.C. § 2679(b)(2)(A) (quoted in the preceding footnote)).

²⁰⁸ 132 S. Ct. 617, 181 L. Ed. 2d 606 (2012).

²⁰⁹ Vazquez and Vladeck, *supra* note 206, at 517 (citing 132 S. Ct. 617, 623, 181 L. Ed. 2d 606 (2012)).

²¹⁰ Cohen and Chu, *supra* note 203, at 18.

²¹¹ Vazquez and Vladeck, *supra* note 206, at 517. See also Pfander and Baltmanis, *supra* note 199, at 123 (stating that “[t]oday, *Bivens* provides the only generally available basis on which individuals can seek an award of damages for federal violations of constitutional rights”).

²¹² Pfander and Baltmanis, *supra* note 199, at 126 (citing *Wilkie v. Robbins*, 551 U.S. 537 (2007)).

²¹³ A. Michael Froomkin, *Symposium: Security Breach Notification Six Years Later: Government Data Breaches*, 24 BERKELEY TECH. L.J. 1019, 1055 (2009) [hereinafter Froomkin].

²¹⁴ 556 U.S. 662, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009).

²¹⁵ *Id.* at 675, 129 S. Ct. at 1947, 173 L. Ed. 2d at 882 (citation omitted).

Kennedy also wrote that “[b]ecause implied causes of action are disfavored, the Court has been reluctant to extend *Bivens* liability ‘to any new context or new category of defendants.’”²¹⁶ Even when *Bivens* claims have been allowed, a 2009 Government Accountability Office (GAO) report concluded that the likelihood of an eventual monetary recovery in a *Bivens* case is quite rare.²¹⁷

A second obstacle to *Bivens* claims is that “[g]overnment officials may not be held liable for the unconstitutional conduct of their subordinates under a theory of *respondeat superior*.”²¹⁸ Because vicarious liability does not apply in a *Bivens* case (or in § 1983 actions), each government official who is a defendant in a *Bivens* case must be shown to have violated the Constitution; otherwise, a plaintiff does not have a cognizable claim against that defendant.²¹⁹

Third, a particularly difficult obstacle to a *Bivens* claim is the defense of qualified immunity, discussed in the next subsection.²²⁰

Finally, a threshold, and likely dispositive issue that would preclude a *Bivens* claim, as well as a § 1983 claim, is that there is no case holding that the collection or dissemination of one’s personal or locational data violates a right to privacy under the U.S. Constitution.

²¹⁶ *Id.* at 675, 129 S. Ct. at 1947, 173 L. Ed. 2d at 882 (citations omitted).

²¹⁷ Cohen and Chu, *supra* note 203, at 21.

²¹⁸ *Ashcroft*, 556 U.S. at 676, 129 S. Ct. at 1948, 173 L. Ed. 2d at 882 (citing *Monell v. Dep’t of Soc. Servs.*, 436 U.S. 658, 691, 98 S. Ct. 2018, 56 L. Ed. 2d 611 (1978) (finding no vicarious liability for a municipal “person” under 42 U.S.C. § 1983)); *Dunlop v. Munroe*, 11 U.S. 242, 7 Cranch 242, 269, 3 L. Ed. 329 (1812) (A federal official’s liability “will only result from his own neglect in not properly superintending the discharge” of his subordinates’ duties.); *Robertson v. Sichel*, 127 U.S. 507, 515–516, 8 S. Ct. 1286, 1290, 32 L. Ed. 203, 206 (1888) (“A public officer or agent is not responsible for the misfeasances or positive wrongs, or for the nonfeasances, or negligences, or omissions of duty, of the sub-agents or servants or other persons properly employed by or under him, in the discharge of his official duties.”).

²¹⁹ *Ashcroft*, 556 U.S. at 676, 129 S. Ct. at 1948, 173 L. Ed. 2d at 882. The Court further stated that:

Absent vicarious liability, each Government official, his or her title notwithstanding, is only liable for his or her own misconduct. In the context of determining whether there is a violation of a clearly established right to overcome qualified immunity, purpose rather than knowledge is required to impose *Bivens* liability on the subordinate for unconstitutional discrimination; the same holds true for an official charged with violations arising from his or her superintendent responsibilities.

Id. at 677, 129 S. Ct. at 1949, 173 L. Ed. 2d at 883 (emphasis added).

²²⁰ Cohen and Chu, *supra* note 203, at 21.

E. Whether There Is a Section 1983 Claim for an Intentional or Unintentional Release of Data

As discussed, a *Bivens* claim against federal officials is the “federal analog” to 42 U.S.C. § 1983 claims against state officials.²²¹ However, it does not appear that a complaint against transportation agency officers or employees for a violation of an individual’s right to privacy based on a disclosure of secure data or monitoring data would state a claim under § 1983.

Section 1983 states in part that “[e]very person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured....”²²²

As explained in *Toomer v. Garrett*,²²³ a state and state officials acting in their official capacities are not “persons” within the meaning of § 1983 actions for money damages,²²⁴ but they are considered persons for § 1983 purposes when they are sued for injunctive relief.²²⁵ When state officials are sued under § 1983 in their *individual* capacities, they may be held liable for damages.²²⁶ However, when state officials are sued in their individual capacities, the defense of qualified immunity will shield them from personal liability, unless it is shown that they have caused an injury by violating a known, clearly established constitutional or statutory right.²²⁷

Thus, the qualified immunity doctrine may shield completely an official’s conduct even though the conduct violated the Constitution.²²⁸ As one scholar explains the defense, if a reasonable official could have believed that his or her actions were lawful, then the doctrine operates to excuse some “reasonable ignorance” of the law.²²⁹ The rationale for the doctrine is that it permits officials to be decisive and exercise their judgment for the public good but

²²¹ *Ashcroft*, 556 U.S. at 675, 129 S. Ct. at 1948, 173 L. Ed. 2d at 882.

²²² 42 U.S.C. § 1983 (2015).

²²³ 155 N.C. App. 462, 574 S.E.2d 76 (2002).

²²⁴ *Id.* at 472, 574 S.E.2d at 86 (citation omitted).

²²⁵ *Id.*

²²⁶ *Id.* at 473, 574 S.E.2d at 86.

²²⁷ *Id.*, citing *Andrews v. Crump*, 144 N.C. App. 68, 75–76, 547 S.E.2d 117, 122, *disc. review denied*, 354 N.C. 215, 553 S.E.2d 907 (2001) (quoting *Harlow v. Fitzgerald*, 457 U.S. 800, 818, 102 S. Ct. 272, 773 L. Ed. 2d 396, 410 (1982)).

²²⁸ Barbara E. Armacost, *Qualified Immunity: Ignorance Excused*, 51 VAND. L. REV. 581, 584 (1998) [hereinafter *Armacost*].

²²⁹ *Id.*

provides them with a “margin of error” when they “make reasonable mistakes about the exact boundaries of constitutional law....”²³⁰ Or, stated differently, “qualified immunity protects from liability all but the ‘plainly incompetent’ or the official who could not reasonably have believed that [his or her] actions were lawful.”²³¹

In *Harlow v. Fitzgerald*,²³² a § 1983 action, the Supreme Court held that government officials who are acting within their discretionary authority but who are sued in their individual capacities have qualified immunity as long as “their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.”²³³ For government officials to have acted within the scope of their discretionary authority means that their “actions were (1) undertaken pursuant to the performance of [their official] duties and (2) within the scope of [their] authority.”²³⁴

In *Borucki v. Ryan*,²³⁵ the First Circuit relied on *Harlow* in holding that the defendant was entitled to qualified immunity, because the “alleged right of privacy was not clearly established as of the date” of the alleged violation of a right to privacy.²³⁶ The *Borucki* court appears to attach an additional requirement, one that goes beyond determining whether a constitutional or statutory right has been clearly established: “when the law requires a balancing of competing interests, it may be unfair to charge an official with knowledge of the law in the absence of a previously decided case with *clearly analogous facts*.”²³⁷

In *Toomer*, a former state government employee alleged that the Secretary of the North Carolina DOT disclosed the plaintiff’s personnel file to the news media. The plaintiff alleged that the file contained his Social Security number and other PII, as well as the history and details of a settlement of a personnel claim between the plaintiff and the DOT.²³⁸

²³⁰ *Id.* at 586.

²³¹ *Id.* at 600 (citing *Malley v. Briggs*, 475 U.S. 335, 341 (1986) and quoting *Anderson v. Creighton*, 483 U.S. 635, 638 (1987) (stating that qualified immunity obtains “as long as [the officials’] actions could reasonably have been thought consistent with the rights they were alleged to have violated”).

²³² 457 U.S. 800, 814, 102 S. Ct. 2727, 73 L. Ed. 2d 396 (1982).

²³³ *Id.* at 818, 102 S. Ct. 2727, 73 L. Ed. 2d 396 (citation omitted).

²³⁴ *Lenz v. Winburn*, 51 F.3d 1540, 1545 (11th Cir. 1995) (citations omitted) (internal quotation marks omitted).

²³⁵ 827 F.2d 836, 837 (1st Cir. 1987) (citations omitted).

²³⁶ *Id.*

²³⁷ *Id.* at 848 (footnote omitted) (citations omitted) (emphasis added).

²³⁸ *Toomer*, 155 N.C. App. at 467, 574 S.E.2d at 83.

In response to the plaintiff’s substantive due process claim, the court held that “one’s privacy interest in the information contained in personnel files does not fall under the recognized fundamental right to privacy” that exists for personal and family decisionmaking.²³⁹

However, the plaintiff’s allegations were sufficient to state a claim for a violation of the Fourth Amendment’s protection “against arbitrary government action that is so egregious that it ‘shocks the conscience’ or offends a ‘sense of justice.’”²⁴⁰ In *Toomer*, the defendants allegedly “acted with a high level of culpability, including deliberate indifference, malice, willfulness, and retaliation. While intentional conduct is that ‘most likely’ to meet the test, that alone will not suffice; the conduct must be ‘intended to injure in some way unjustifiable by any government interest.’”²⁴¹ Thus, “[a]rbitrary acts that have an abusive purpose and lack legitimate justification violate due process.”²⁴² The court held that the North Carolina DOT’s Secretary’s action in disclosing Toomer’s personnel file was “outside the scope of authority, [done] maliciously, in bad faith, and for retaliatory reasons.”²⁴³

Another privacy case against state officials is *Collier v. Dickinson*,²⁴⁴ in which the plaintiffs sued executive-level officials with the Florida Department of Highway Safety and Motor Vehicles for selling the plaintiffs’ personal information to mass marketers in violation of the DPPA.²⁴⁵ In addition to a claim under the DPAA, the plaintiffs filed a § 1983 claim. Stating that the court’s decision was consistent with prior precedent in the Eleventh Circuit, the *Collier* court held there was no constitutional right to privacy that had been violated.²⁴⁶ There was, however, a statutory violation of privacy, because the “DPPA clearly, unambiguously, and expressly creates a statutory right which may be enforced” by the plaintiffs.²⁴⁷ Although the defendants argued that the DPAA’s “comprehensive enforcement scheme” was incompatible with enforcement under § 1983,²⁴⁸ the

²³⁹ *Id.* at 469, 574 S.E.2d at 84 (citing *Kallstrom, supra*).

²⁴⁰ *Id.* at 470, 574 S.E.2d at 84 (citing *United States v. Salerno*, 481 U.S. 739, 746, 107 S. Ct. 2095, 95 L. Ed. 2d 697, 708 (1987), *County of Sacramento v. Lewis*, 523 U.S. 833, 118 S. Ct. 1708, 140 L. Ed. 2d 1043 (1998), *State v. Guice*, 141 N.C. App. 177, 541 S.E.2d 474 (2000)).

²⁴¹ *Id.* (citation omitted) (some internal quotation marks omitted).

²⁴² *Id.* at 474, 574 S.E.2d at 84. Under the circumstances of the *Toomer* case, the intentional disclosure also stated a § 1983 claim for a violation of the Equal Protection Clause of the United States Constitution. *Id.* at 477, 574 S.E.2d at 89.

²⁴³ *Id.* at 481, 574 S.E.2d at 91.

²⁴⁴ 477 F.3d 1306 (11th Cir. 2007).

²⁴⁵ *Id.* at 1307.

²⁴⁶ *Id.* at 1308.

²⁴⁷ *Id.* at 1308–1309.

²⁴⁸ *Id.* at 1311.

court disagreed, holding that the DPAA and § 1983 enforcement mechanisms are “complementary.”²⁴⁹ Because the statutory language gave the defendants “clear notice...that releasing the information...violated federal law,” the defendants were not entitled to qualified immunity.²⁵⁰

In *Kiminski v. Hunt*,²⁵¹ in which a federal court in Minnesota dismissed claims brought under the DPPA, the court likewise dismissed the plaintiffs’ § 1983 claim. The complaint alleged that defendant John Hunt (Hunt), a former employee of the Minnesota Department of Natural Resources (DNR), accessed the motor vehicle record data of the plaintiffs, as well as the data of 5,000 other individuals.²⁵² The complaint sought to hold various state defendants, namely employees of the Minnesota Department of Public Safety and DNR and the agencies’ commissioners in their official capacities, liable under the DPPA and § 1983.²⁵³

The court granted the state defendants’ motion (which did not include Hunt) to dismiss the § 1983 action for failure to state a claim.²⁵⁴ The court held that in a § 1983 action, the “plaintiff must allege deprivation of a right secured by the Constitution and laws of the United States and must show that the deprivation was committed by a person acting under color of state law.”²⁵⁵ As held by the court in *Borucki*, it is not enough that a general right exists, “otherwise ‘plaintiffs would be able to convert the rule of qualified immunity...into a rule of virtually unqualified liability simply by alleging violation of extremely abstract rights.’”²⁵⁶

In *Kiminski*, the court dismissed the plaintiffs’ § 1983 claim because there was “no constitutional right to privacy in the information protected by the DPPA.”²⁵⁷ The court observed that the Eighth Circuit has held that even for medical information, there is “no blanket constitutional privacy protection....”²⁵⁸ Unlike the Eleventh Circuit’s decision in *Collier*, the court in *Kiminski* also held that a § 1983 claim for a violation of the DPPA was precluded “because the DPPA explicitly provides for a

comparatively restrictive private cause of action” that is “inconsistent” with a § 1983 claim.²⁵⁹

In *Kraege v. Busalacchi*,²⁶⁰ the plaintiff likewise alleged that state employees had released their personal information in violation of the DPPA.²⁶¹ Wisconsin’s policy was to permit Wisconsin driver information to be released to purchasers who agree to use it for permissible purposes, a policy that the defendant employees followed.²⁶² The court held that the defendants did not misread or misjudge the state policies but simply had followed the policy; the crux of the plaintiff’s complaint had to do with the policy, not with the defendants’ choices.²⁶³ Therefore, the claims were “substantially against the State of Wisconsin” and thus were barred by the doctrine of sovereign immunity.²⁶⁴

Finally, a disclosure, of course, could be made by contractors charged with the responsibility to collect and safeguard data. Section 1983 requires that a violator act under color of law, but “does not require that the accused be an officer of the State. It is enough that he is a willful participant in joint activity with the State or its agents....”²⁶⁵ Although it appears that a contractor could be subject to § 1983, it would have to be shown that a transportation agency’s agent violated a known, established constitutional right to privacy.

In sum, unless the Supreme Court recognizes a constitutional right to privacy in secure or monitoring data, it appears that a complaint against transportation agency officers or agents for a disclosure of such data would fail to state a claim under § 1983. It has been held that there is no constitutional right to privacy even in the PII of the type protected by the DPPA or in an employee’s personnel file.²⁶⁶ A violation of a statute (e.g., the DPPA) may be the basis of a § 1983 claim in courts permitting a claim both under the statute and under § 1983. (More recent authority holds that there is a claim only under the DPAA.) Unlike the DPAA, discussed in Section IV.C, there is presently no federal statute that protects personal and locational data of the type found in secure data or monitoring data collected by transportation agencies.

Moreover, in the absence of a clearly established constitutional or statutory right to privacy of which a

²⁴⁹ *Id.*

²⁵⁰ *Id.* at 1312.

²⁵¹ 2013 U.S. Dist. LEXIS 157829, at *1 (D. Minn. 2013).

²⁵² *Id.* at *2.

²⁵³ *Id.* at *1.

²⁵⁴ *Id.* at *2, 43.

²⁵⁵ *Id.* at *25 (citing *West v. Atkins*, 487 U.S. 42, 48, 108 S. Ct. 2250, 101 L. Ed. 2d 40 (1988)).

²⁵⁶ *Borucki*, 827 F.2d at 838 (citations omitted).

²⁵⁷ *Kiminski*, 2013 U.S. Dist. LEXIS 157829, at *40 (citation omitted).

²⁵⁸ *Id.* at *42 (citing *Cooksey v. Boyer*, 289 F.3d 513, 517 (8th Cir. 2002)).

²⁵⁹ *Id.* at *31, 35.

²⁶⁰ 687 F. Supp. 2d 834 (W.D. Wis. 2009).

²⁶¹ 18 U.S.C. §§ 27211–27225.

²⁶² *Kraege*, 687 F. Supp. 2d at 839.

²⁶³ *Id.* at 836.

²⁶⁴ *Id.* at 835.

²⁶⁵ *Fadjo*, 633 F.2d 1172, 1175 (5th Cir. 1981) (citations omitted).

²⁶⁶ *Kiminski*, 2013 U.S. Dist. LEXIS 157829, at *40 (citation omitted).

reasonable person would have known, state officials or employees sued in their individual capacities would have qualified immunity for a disclosure of secure data or monitoring data.²⁶⁷ A § 1983 claim could arise if an official commits an egregious, intentional, arbitrary, and malicious act that in and of itself violates the Fourth Amendment as alleged in the *Toomer* case. However, a claim based on “mere negligence” for a disclosure of personal data ordinarily would be insufficient because “under section 1983 there must be an intentional or deliberate deprivation of life, liberty, or property, or at least ‘deliberate indifference.’”²⁶⁸

IV. WHETHER THERE ARE FEDERAL STATUTES APPLICABLE TO TRANSPORTATION AGENCIES’ COLLECTION OR DISCLOSURE OF DATA

A. Evolution of Federal Statutory Privacy Rights

With respect to federal statutes protecting individuals’ right to privacy, the laws historically have been derived from general tort law, but government recordkeeping on its citizens has resulted in “a distinct subspecies of statutory law.”²⁶⁹ Some federal laws, such as the Privacy Act and the FOIA, broadly control the “use and disclosure of federal government records about its citizens,”²⁷⁰ whereas other laws such as the DPPA or the Gramm-Leach-Bliley Act of 1999²⁷¹ govern narrow, specific issues that affect individuals.²⁷² Although several federal laws address the privacy rights of individuals, the subject of the right to privacy has been left largely to the states.²⁷³

Scholars point out that with respect to data collection in public transportation, other than the DPPA, there are no federal statutes that protect an individual’s personal data and none that protect an individual’s locational data.²⁷⁴ Thus, with the exception of the DPPA that applies to the state DMVs’ collection of secure data including PII, there appear to be no federal statutes protecting privacy rights that are implicated by transportation agencies’ collection of secure or monitoring data.²⁷⁵

²⁶⁷ *Harlow v. Fitzgerald*, 457 U.S. 800, 818, 102 S. Ct. 2727, 73 L. Ed. 2d 396 (1982) (citation omitted).

²⁶⁸ *Froomkin*, *supra* note 213, at 1053.

²⁶⁹ *McCarthy*, *supra* note 83, at § 5.83.

²⁷⁰ *Id.* § 6.135.

²⁷¹ Gramm-Leach-Bliley Act of 1999, § 501, Pub. L. No. 106-103, 113 Stat. 1338, codified at 15 U.S.C. § 6801 (2015).

²⁷² Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, codified at 5 U.S.C. §§ 551(1) and 552a(b) (2015).

²⁷³ *Katz*, 389 U.S. at 350–351, 88 S. Ct. at 511, 19 L. Ed. 2d at 581 (footnote omitted).

²⁷⁴ Garry, Douma, and Simon, *supra* note 2, at 97.

²⁷⁵ *Id.* at 103.

B. Privacy Act of 1974

The Privacy Act of 1974²⁷⁶ protects the privacy of records maintained by federal agencies on individuals²⁷⁷ and regulates the agencies’ release of privacy information.²⁷⁸ The Act is a “reaction to the perceived threat to personal privacy presented by computerized government records about its citizens” and addresses problems “largely beyond the reach of traditional tort law.”²⁷⁹

The Act requires each government agency to make certain information available to the public but provides further that

[t]o the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, staff manual, instruction, or copies of records referred to in subparagraph (D)....²⁸⁰

The USDOT explains that the Privacy Act sets forth “how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII).”²⁸¹ The USDOT also observes that Section 208 of the E-Government Act of 2002 “establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections.”²⁸²

The Privacy Act governs government or government-controlled corporations, but not private entities.²⁸³ However, the Privacy Act applies to “certain federal contractors who operate Privacy Act systems of records on behalf of federal agencies.”²⁸⁴ When disclosing records, no federal agency or its contractors may disclose PII without the affected individual’s written consent.²⁸⁵ If the Privacy Act and privacy regulations provide different standards, a federal

²⁷⁶ See Pub. L. No. 93-579, 88 Stat. 1896, codified at 5 U.S.C. § 552a (2015).

²⁷⁷ 5 U.S.C. § 552a(b) (2015). See also 5 U.S.C. § 552(d) (1) (2015); Douma and Deckenbach, *supra* note 2, at 306.

²⁷⁸ 5 U.S.C. §§ 552(a) and (b) (2015).

²⁷⁹ *McCarthy*, *supra* note 83, at § 5.85.

²⁸⁰ 5 U.S.C. § 522(a)(2)(E) (2015).

²⁸¹ U.S. DEPT. OF TRANSPORTATION, Privacy Impact Assessment (Update) National Registry of Certified Medical Examiners (National Registry) (Aug. 20, 2012), available at: http://www.dot.gov/sites/dot.dev/files/docs/FMCSA_PIA_National_Registry_082012.pdf (last accessed Oct. 12, 2015).

²⁸² *Id.*

²⁸³ John M. Eden, *When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID*, 2005 DUKE L. & TECH. REV. 20, P4 (2005) (citing 5 U.S.C. § 522(a) and (a)(1)) [hereinafter Eden].

²⁸⁴ 65 Fed. Reg. 82,462, 82,482 (Dec. 28, 2000).

²⁸⁵ *Id.*

agency must abide by whichever provision allows for the least disclosure.²⁸⁶

Section 552g(1) of the Privacy Act states:

Whenever any agency...fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness...or fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, *the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction* in the matters under the provisions of this subsection.²⁸⁷

Although an individual may bring a civil action when private information allegedly was wrongfully disclosed, a plaintiff has the burden of showing that the agency willfully or intentionally disclosed the information.²⁸⁸ Apparently, the Privacy Act has not been applied to data breaches resulting from unauthorized access.²⁸⁹

There are four essential elements that must be established when a plaintiff makes a claim under the Privacy Act:

(1) the information is covered by the Act as a “record” contained in a “system of records;” (2) the agency “disclosed” the information; (3) the disclosure had an “adverse effect” on the plaintiff (an element which separates itself into two components: (a) an adverse effect standing requirement and (b) a causal nexus between the disclosure and the adverse effect); and (4) *the disclosure was “willful or intentional.”*²⁹⁰

In *Stephens v. Tennessee Valley Authority*,²⁹¹ a former Tennessee Valley Authority (TVA) employee sued the TVA under the Privacy Act for violating his federal civil rights when it publicly circulated a memorandum accusing the plaintiff of accepting kickbacks and violating several laws.²⁹² After the document was released to the media, the TVA recalled and replaced it with a sanitized document that did not personally identify the plaintiff; however, one copy of the original document was released publicly.²⁹³ The court held that the plaintiff could not recover for a violation of the Privacy Act even though there was a wrongful disclosure because the agency had not acted willfully or intentionally.²⁹⁴ By recalling and sanitizing the document,

²⁸⁶ *Id.*

²⁸⁷ 5 U.S.C. §§ 552a(g)(1)(A)–(D) (2015) (emphasis added).

²⁸⁸ 5 U.S.C. § 552a(g)(4) (2015).

²⁸⁹ Froomkin, *supra* note 213, at 1034.

²⁹⁰ Quinn v. Stone, 978 F.2d 126, 131 (3d Cir. 1992).

²⁹¹ 754 F. Supp. 579, 584 (E.D. Tenn. 1990).

²⁹² *Id.* at 580.

²⁹³ *Id.* at 581.

²⁹⁴ *Id.* at 582.

the TVA demonstrated a concern for the plaintiff’s privacy interests.²⁹⁵

However, in a 2008 case brought under the Privacy Act, *American Federation of Government Employees v. Hawley*,²⁹⁶ the plaintiffs alleged that the defendants violated the Aviation and Transportation Security Act (ATSA)²⁹⁷ and the Privacy Act²⁹⁸ by failing to establish appropriate safeguards to insure the security and confidentiality of personnel records.

A federal court in the District of Columbia explained what is meant by the Privacy Act’s requirement that a violation be intentional or willful:

An agency acts in an intentional or willful manner “either by committing the act without grounds for believing it to be lawful[] or by flagrantly disregarding others’ rights under the Act.” ...To rise to this level, “[t]he violation must be so patently egregious and unlawful that anyone undertaking the conduct should have known it [to be] unlawful.”²⁹⁹

The plaintiffs alleged that the defendants were informed repeatedly of “recurring, systemic, and fundamental deficiencies in [their] information security,” but that the defendants “demonstrated reckless disregard for privacy rights when [they] failed to effectively secure the external hard drive that maintained the personal information of [their] personnel workforce.”³⁰⁰ The court held, *inter alia*, that the plaintiffs’ allegations that the agency had *negligently* lost control of their personal data by failing to establish safeguards to prevent the loss of hard drives stated a claim.³⁰¹

In subsequent proceedings, however, the court granted the defendants’ motion for summary judgment because the undisputed facts showed that neither had there been a violation of the Privacy Act nor had the plaintiffs sustained any actual damages.

In 2014 in *Kelley v. FBI*,³⁰² a federal court in the District of Columbia held that the plaintiffs pled sufficient facts to state a claim against the FBI under the Privacy Act.³⁰³ In *Kelley*, after the

²⁹⁵ *Id.* at 583. See also *Wisdom v. Dep’t of Housing and Urban Development*, 713 F.2d 422, 424–425 (8th Cir. 1983) (holding that the Department of Housing and Urban Development had not acted intentionally or willfully in disclosing information to the IRS pertaining to an individual’s default on a home loan).

²⁹⁶ 543 F. Supp. 2d 44 (D.D.C. 2008).

²⁹⁷ *Id.* at 45 (citing 49 U.S.C. §§ 44901 and 44935).

²⁹⁸ *Id.* (citing 5 U.S.C. § 552a).

²⁹⁹ *Id.* at 51 (citations omitted) (some internal quotation marks omitted).

³⁰⁰ *Id.* at 52 (citations omitted) (some internal quotation marks omitted).

³⁰¹ *Id.* at 51–53.

³⁰² 67 F. Supp. 3d 340 (D.D.C. 2014).

³⁰³ *Id.* at 264.

plaintiffs received a number of harassing emails, they notified the FBI of the cyber stalking.³⁰⁴ During the investigation, the plaintiffs consented to giving the passwords to their email accounts to the FBI to enable it to track the IP address of the stalker.³⁰⁵ The FBI promised not to release the plaintiffs' names, but their names were released when the media received some of the harassing emails that the plaintiffs had received.³⁰⁶ The plaintiffs alleged that their information and report to the FBI were maintained in a system of records that identified them by name or identification number, that the FBI shared this information with the Department of Defense, and that both agencies disclosed the information to the media.³⁰⁷ As of October 12, 2015, there were no further reported proceedings in the *Kelley* case.

Finally, the Privacy Act provides that a person shall be entitled to recover no less than \$1,000.³⁰⁸ In 2004, in *Doe v. Chao*,³⁰⁹ the Supreme Court held that in the absence of proof of actual damages, the petitioner could not recover for a violation of the Privacy Act even though the government repeatedly disclosed the claimant's Social Security number.³¹⁰ It was not sufficient to show that the government intentionally or willfully violated the Act; the claimant also had to show an adverse effect, i.e., actual damages.³¹¹

C. Driver's Privacy Protection Act

The Driver's Privacy Protection Act of 1994³¹² protects personal information collected by a state DMV. The DPPA provides that a DMV officer, employee, or contractor must not knowingly disclose or otherwise make available to any person or entity:

(1) personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b)...; or

(2) highly restricted personal information, as defined in 18 U.S.C. 2725(4), about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9)...³¹³

³⁰⁴ *Id.* at 248.

³⁰⁵ *Id.* at 248–49.

³⁰⁶ *Id.*

³⁰⁷ *Id.* at 265. The court dismissed all other claims for either lack of jurisdiction or failure to state a claim. *Id.* at 256.

³⁰⁸ Froomkin, *supra* note 213, at 1034 (citing 5 U.S.C. § 552(q)(4)).

³⁰⁹ 540 U.S. 614, 124 S. Ct. 1204, 157 L. Ed. 2d 1122 (2004).

³¹⁰ *Id.* at 616, 124 S. Ct. at 1206, 157 L. Ed. 2d at 1129.

³¹¹ *Id.* at 627, 124 S. Ct. at 1212, 157 L. Ed. 2d at 1134.

³¹² 18 U.S.C. §§ 2721–2725 (2015).

³¹³ 18 U.S.C. §§ 2721(a)(1) and (2) (2015).

The term “personal information” is defined as information that identifies an individual, such as by name, address (but not the 5-digit zip code), telephone number, Social Security number, driver identification number, photograph, or medical or disability information, but not information on vehicular accidents, driving violations, and a driver's status.³¹⁴ The term “highly restricted personal information” means an individual's Social Security number, photograph or image, or medical or disability information.³¹⁵ The term “express consent” means that a person must consent in writing, but consent may be evidenced by a signature sent electronically.³¹⁶

Although there are various exceptions in the DPPA that allow for the dissemination of personal information, an important one is that personal information may be disclosed “[f]or use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.”³¹⁷

The DPPA provides for a private right of action that may be brought in a United States district court against a person who knowingly violates the DPPA.³¹⁸ The DPPA provides that “[a] person who knowingly obtains, discloses, or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains...”³¹⁹ In the event of liability, a court may award actual damages but not less than liquidated damages in the amount of \$2,500, punitive damages if there is proof of a willful or reckless disregard of the law, and attorneys' fees and other litigation costs that are reasonably incurred, as well as preliminary and equitable relief when appropriate.³²⁰

Several state and local governments unsuccessfully challenged the constitutionality of the DPAA on the basis that the law exceeds Congress's authority under the Commerce Clause. In *Travis v. Reno*,³²¹ the State of Wisconsin argued that the law required the state to “make costly changes in the way it handles requests for access to its records,” as well as prevented the State from generating revenue by selling personal information to third parties for mailing lists. However, the Seventh Circuit, stating that “driving is an interstate business,”³²² held that

³¹⁴ 18 U.S.C. § 2725(3) (2015).

³¹⁵ 18 U.S.C. § 2725(4) (2015).

³¹⁶ 18 U.S.C. § 2725(5) (2015).

³¹⁷ 18 U.S.C. § 2721(b)(1) (2015).

³¹⁸ 18 U.S.C. § 2724(a) (2015).

³¹⁹ 18 U.S.C. § 2724(a) (2015).

³²⁰ 18 U.S.C. § 2724(b) (2015).

³²¹ 163 F.3d 1000, 1002 (7th Cir. 1998).

³²² *Id.*

“nothing in the [DPPA] interferes with the state’s ability to license drivers and remove dangerous ones from the road; it regulates external rather than internal uses of the information.”³²³

Thus, with respect to statutes such as the DPPA, it appears that federal privacy laws are likely to be upheld when they regulate interstate commerce and govern the external uses of information without interfering with a state or local government’s performance of its regulatory responsibilities.

D. Other Federal Privacy Laws

Some federal laws are broad in scope and allow a government agency to enforce privacy law even in the absence of explicit rules. For example, the Federal Trade Commission Act of 1914 (FTC Act)³²⁴ is used to regulate companies’ privacy notices to consumers concerning how they collect and use consumer data, including locational data.³²⁵ However, the FTC Act only states that the FTC is “empowered and directed to prevent persons, partnerships, or corporations...from using unfair methods of competition...and unfair or deceptive acts or practices in or affecting commerce.”³²⁶

In 2014, in *FTC v. Wyndham Worldwide Corporation*,³²⁷ a federal district court in New Jersey stated that rapidly evolving digital and privacy issues are in an “ongoing struggle” over a “variety of thorny legal issues that Congress and the courts will continue to grapple with...”³²⁸ Nevertheless, the court held that even in the absence of more formal notice via rulemaking, the FTC could bring an action against the defendant under the FTC Act when “an agency...is given an option to proceed by rulemaking or by individual adjudication the choice is one that lies in the informed discretion of the administrative agency.”³²⁹ The court recognized that the FTC has broad authority to regulate the security of data even if explicit language is not included in the statute. The court reasoned that “the FTC’s unfairness authority over data security” would not “lead to a

result that is incompatible with more recent legislation” or “plainly *contradict* congressional policy.”³³⁰

Because Section 5 of the FTC Act “codifies a three-part test that proscribes whether an act is ‘unfair,’” the court was not convinced by the defendant’s argument that regulations are the only way to provide fair notice.³³¹ Therefore, prior to bringing a suit for a violation of the Act, the FTC was not required to promulgate regulations explaining what data security practices were forbidden or required by the FTC Act. The court stated that a ruling for the defendant would mean that “the FTC would have to cease bringing *all* unfairness actions without first proscribing particularized prohibitions—a result that is in direct contradiction with the flexibility necessarily inherent in Section 5 of the FTC Act.”³³²

As for other federal privacy legislation, there are federal laws that require regulated entities to have privacy policies, but the laws do not create a private right of action for violations of the policies. For example, the Gramm-Leach-Bliley Act of 1999³³³ requires financial institutions to have privacy policies but does not provide for a private right of action.³³⁴

A 2014 *Legal Research Digest* (LRD) published by TRB discusses³³⁵ USDOT privacy regulations, as well as the Health Insurance Portability and Accountability Act (HIPAA),³³⁶ the Patient Protection and Affordable Care Act,³³⁷ the Public Health Service Act³³⁸ and Records of Substance Abuse, the

³³⁰ *Id.* at 612 (citation omitted) (internal quotation marks omitted).

³³¹ *Id.* at 619 (citation omitted).

³³² *Id.* at 621.

³³³ Pub. L. No. 106-102, 113 Stat. 1338, codified at 15 U.S.C. § 6801 (2015).

³³⁴ *Lowe v. Viewpoint Bank*, 972 F. Supp. 2d 947, 954, 961 (N.D. Tex. 2013). *See also* *Dunmire v. Morgan Stanley*, 475 F.3d 956 (8th Cir. 2007); *Borninski v. Williamson*, 2004 U.S. Dist. LEXIS 29407, at *1 (N.D. Tex. 2004); and *Downs v. Regions Bank*, 2010 U.S. Dist. LEXIS 6231, at *1 (M.D. Ala. 2010).

³³⁵ LARRY W. THOMAS, HOW THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) AND OTHER PRIVACY LAWS AFFECT PUBLIC TRANSPORTATION OPERATIONS (Legal Research Digest No. 46, Transportation Research Board of the National Academies of Sciences, Engineering, and Medicine, 2014). (Digest also referencing the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511(1)(a)-(b), Telecommunications Act, 47 U.S.C. §§ 222(a)-(c), Cable Communications Act, 47 U.S.C. § 551, Child Online Protection Act, 15 U.S.C. §§ 6501(4) and (8), Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801(a)-(b), Sarbanes-Oxley Act, 15 U.S.C. § 7262, and Fair Credit Reporting Act, 15 U.S.C. § 1681), available at http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_lrd_46.pdf (last accessed Oct. 12, 2015).

³³⁶ Pub. L. No. 104-191, 110 Stat. 1936 (1996).

³³⁷ Pub. L. No. 111-148, 124 Stat. 119-1025 (2010).

³³⁸ Pub. L. No. 78-410, ch. 373, 58 Stat. 682 (1944).

³²³ *Id.* at 1003. *See also* *Reno v. Condon*, 528 U.S. 141, 148, 151, 120 S. Ct. 666, 671, 672, 145 L. Ed. 2d 587 (2000) (holding that the sale or release of motorists’ information in interstate commerce was “sufficient to support congressional regulation” and that the DPPA does not require the states to enact any laws or regulations) and *Zittel v. City of Gainesville*, 2013 U.S. Dist. LEXIS 128209, at *1 (N.D. Fla. 2013) (upholding the DPPA’s constitutionality).

³²⁴ Pub. L. No. 63-203, 38 Stat. 717, as amended and codified at 15 U.S.C. §§ 41-58 (2015).

³²⁵ *See* 15 U.S.C. § 45(a) (2015).

³²⁶ 15 U.S.C. § 45(a)(2) (2015).

³²⁷ 10 F. Supp. 3d 602 (D. N.J. 2014).

³²⁸ *Id.* at 610.

³²⁹ *Id.* at 617, 619 (citation omitted).

Employee Retirement Income Security Act of 1974,³³⁹ the Family Educational Rights and Privacy Act,³⁴⁰ Medicare and Medicaid, and the Genetic Information Nondiscrimination Act.³⁴¹

E. Proposed Federal Privacy Legislation

1. Geolocational Privacy and Surveillance Act

Introduced in the House on January 22, 2015, the Geolocational Privacy and Surveillance Act³⁴² would amend the federal criminal code to require a search warrant to acquire geolocational information.³⁴³ Although there are exemptions (e.g., consent, emergency circumstances), the bill also would prohibit any person providing covered services from intentionally divulging geolocational information pertaining to another person and would prevent the use of such information as evidence. The bill has been assigned to the House Committee on the Judiciary, the Select Committee on Intelligence, and the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. In January 2015, a bill with the same title that was introduced in the Senate was referred to the Committee on the Judiciary.³⁴⁴

2. Online Communication and Geolocation Protection Act

Introduced in the House on February 2, 2015, the Online Communication and Geolocation Protection Act (OCGPA) would prohibit “an officer, employee, or agency of the United States in the normal course of the official duty of the officer, employee, or agent to conduct electronic surveillance” without the consent of the individual under surveillance or pursuant to a warrant.³⁴⁵ The OCGPA also would prohibit communications-related service providers from disclosing

³³⁹ Pub. L. No. 93-406, 88 Stat. 829 (1974).

³⁴⁰ Pub. L. No. 93-380, 88 Stat. 484 (1974).

³⁴¹ Pub. L. No. 110-233, 122 Stat. 881 (2008).

³⁴² Geolocational Privacy & Surveillance Act, H.R. 491, 114th Cong. (2015).

³⁴³ An older version of the bill was previously introduced in the House in 2013 under the same title. *See* Geolocational Privacy & Surveillance Act, H.R. 1312, 113th Cong. (2013). It may be noted that the Location Privacy Protection Act of 2014 (LPPA), S. 2171, 113th Cong. (2014) would have made it presumptively illegal for nongovernment entities to collect an individual’s locational information absent consent. On March 27, 2014, the LPPA was referred to the Committee on the Judiciary. 113 Bill Tracking S. 2171, 113th Cong. (2014). On June 4, 2014, the Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law held hearings on the proposed legislation. *Id.* The bill has not been introduced in the current session of Congress.

³⁴⁴ Geolocational Privacy and Surveillance Act, S. 237, 114th Cong. (2015).

³⁴⁵ Online Communications and Geolocation Protection Act, H.R. 656, 114th Cong. (2015).

geolocational information to governmental entities.³⁴⁶ The bill includes exceptions for electronic surveillance authorized by the Foreign Intelligence Surveillance Act of 1978³⁴⁷ and for emergency responders or police officers acting in situations presenting an immediate danger of death or serious injury.³⁴⁸ On March 17, 2015, the bill was referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.³⁴⁹

3. Driver Privacy Act

The proposed Driver Privacy Act (DPA), introduced in the Senate on March 17, 2015, would protect data recorded in a passenger vehicle’s event data recorder (EDR), regardless of when the vehicle was manufactured, by ascribing ownership of the data to the owner or lessee of the vehicle.³⁵⁰ Under the DPA, EDR data would not be accessible by anyone other than the owner or lessee unless: 1) the data is required by court order; 2) the owner or lessee grants consent; 3) the data is obtained pursuant to an investigation by the National Transportation Safety Board or the USDOT; 4) the data is obtained “for the purpose of determining the need for, or facilitating, emergency medical response in response to a motor vehicle crash”; or 5) the data is obtained for traffic safety research and the owner’s or lessee’s identification is not disclosed.³⁵¹

After referral to the Committee on Commerce, Science, and Transportation, the Committee on March 25, 2015, sent the DPA to the Senate for its consideration.³⁵²

4. Biometric Information Privacy Act

Under the proposed Biometric Information Privacy Act (BIPA), although biometric information on an individual would have been available pursuant to a court order, it would have been a crime whenever a business entity, government entity, or individual fraudulently obtained or disclosed an individual’s biometric information.³⁵³ Referred to the Subcommittee

³⁴⁶ *Id.*

³⁴⁷ Pub. L. No. 95-511, 92 Stat. 1783.

³⁴⁸ CRS Bill Summary, H.R. 656, 114th Cong. (2015), available at Congress.gov (last accessed Oct. 12, 2015). On March 6, 2013, the bill was referred to the House Committee on the Judiciary and to the Committee on Intelligence. 113 Bill Tracking H.R. 983, 113th Cong. (2013).

³⁴⁹ Online Communications and Geolocation Protection Act, H.R. 656 (114th Cong. (2015)).

³⁵⁰ Driver Privacy Act of 2015, S.766, 114th Cong. (2015).

³⁵¹ *Id.* The DPA was first introduced in 2014. On September 15, 2014, the Committee on Commerce, Science and Transportation amended the DPA and placed the DPA on the Senate Legislative Calendar. 113 Bill Tracking S. 1925, 113th Cong. (2014).

³⁵² *Id.*

³⁵³ Biometric Information Privacy Act, H.R. 4381 (2014).

on Crime, Terrorism, Homeland Security, and Investigations in April 2014, the bill has not been reintroduced in the current session of Congress.³⁵⁴

5. *Transportation, Housing and Urban Development, and Related Agencies Appropriations Act*

In 2014, an amendment to the Transportation, Housing and Urban Development, and Related Agencies Appropriations Act would have prohibited the use of funds to mandate GPS tracking or EDRs in personal motor vehicles. The Senate version of the bill did not include a provision on GPS tracking.³⁵⁵ The final version of the bill, enacted as Public Law No. 113-235, prohibited the use of funds that would be made available under the Act to require GPS tracking in private passenger motor vehicles without providing “full and appropriate consideration of federal privacy concerns.”³⁵⁶

6. *Commercial Privacy Bill of Rights Act*

Introduced in the House on February 25, 2015, HR 1053 proposes to establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission.³⁵⁷ The bill would amend the Children’s Online Privacy Protection Act of 1998 to “improve provisions relating to collection, use, and disclosure of personal information of children.”³⁵⁸ On February 24, 2015, the bill was referred to the House Committee on Energy and Commerce and thereafter on February 27, 2015, to the Subcommittee on Commerce, Manufacturing, and Trade. On February 24, 2015, an identical bill in the Senate was referred to the Senate Committee on Commerce, Science, and Transportation.³⁵⁹

7. *Black Box Privacy Protection Act*

The Black Box Privacy Protection Act would amend the Automobile Information Disclosure Act of 1958³⁶⁰ by requiring automobile manufacturers to disclose to consumers the installation of EDRs on new automobiles. Manufacturers would have to provide every consumer with an option to enable or disable the device prior to purchasing a vehicle. The bill

³⁵⁴ Biometric Information Privacy Act, 2013 Legis. Bill Hist. U.S. H.B. 4381, 113th Cong. (2013).

³⁵⁵ Transportation, Housing and Urban Development, and Related Agencies Appropriations Act of 2015, 2013 Legis. Bill Hist. U.S. H.B. 4745, 113th Cong. (2013).

³⁵⁶ Pub. L. No. 113-235, § 416 (2013–2014).

³⁵⁷ H.R. 1053, 114th Congress (2015). Short titles for portions of the bill include *Commercial Privacy Bill of Rights Act of 2015* and *Do Not Track Kids Act of 2015*.

³⁵⁸ *Id.*

³⁵⁹ S. 547, 114th Congress (2015).

³⁶⁰ 15 U.S.C. §§ 1231–1233 (2015).

also would prohibit the importation into the United States of an automobile manufactured after 2015 that is equipped with an EDR unless the consumer is given control over the recording capabilities.³⁶¹ In May 2015, the bill was referred to the Subcommittee on Commerce, Manufacturing, and Trade.

8. *Secure Data Act*

The Secure Data Act of 2015 would prohibit a federal agency from requiring or requesting a manufacturer, seller, or developer of computer hardware, software, or an electronic device made available to the general public to design the security functions of their products in a way that would allow the surveillance of any user.³⁶² The bill also would prohibit a requested or mandated physical search by a federal agency of such a product. The bill excludes acts of surveillance by law enforcement agencies authorized by the Communications Assistance for Law Enforcement Act.³⁶³ On March 16, 2015, the bill was referred to the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.

F. Consumer Privacy Bill of Rights

In February 2012, the Obama Administration released a Consumer Privacy Bill of Rights (CPBR) that is directed at how companies handle and protect consumers’ data.³⁶⁴ The CPBR applies comprehensive, globally recognized Fair Information Practice Principles,³⁶⁵ stating, *inter alia*, that consumers have a right to exercise control over the kinds of personal data that companies collect on them and how they use it.³⁶⁶ The CPBR applies to the commercial uses of personal data, meaning

any data, including aggregations of data, [that are] linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device. For example, an identifier on a smart phone or family computer that is used to build a usage profile is personal data. This definition provides the flexibility that is necessary to capture the many kinds of data about consumers that commercial entities collect, use, and disclose.³⁶⁷

³⁶¹ Black Box Privacy Protection, H.R. 2526, 114th Cong. (2015).

³⁶² Secure Data Act of 2015, H.R. 726, 114th Cong. (2015).

³⁶³ Pub. L. No. 103-414, 108 Stat. 42 79, codified at 47 U.S.C. 1001–1010 (1994).

³⁶⁴ THE WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb.), available at: <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf> (last accessed on Oct. 12, 2015).

³⁶⁵ See *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

³⁶⁶ *Id.* at 1.

³⁶⁷ *Id.* at 10.

The CPBR sets forth aspirational goals for the protection of consumers, but is not equivalent to a federal law or regulations.

V. THE RIGHT TO PRIVACY UNDER STATE CONSTITUTIONS

A. State Constitutions Recognizing a Right to Privacy

Although the Supreme Court has held that there is a narrow zone of privacy protected by the U.S. Constitution, at least 10 state constitutions include protection of an individual's right to privacy,³⁶⁸ such as those of Alaska,³⁶⁹ Arizona,³⁷⁰ Florida,³⁷¹ Montana,³⁷² and Washington.³⁷³ Alaska's constitution states that "[t]he right of the people to privacy is recognized and shall not be infringed."³⁷⁴ Arizona's constitution states that "[n]o person shall be disturbed in his private affairs...without authority of law."³⁷⁵ California's constitution secures individuals' "inalienable rights,"³⁷⁶ including their pursuit of "safety, happiness, and privacy."³⁷⁷ Florida's constitution states that "[t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated."³⁷⁸ Iowa's constitution states "All men and

women are, by nature, free and equal, and have certain inalienable rights—among which are those of enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety and happiness."³⁷⁹

Other state constitutional provisions mirror the U.S. Constitution's Fourth Amendment's protection against unreasonable searches and seizures.³⁸⁰

Some state constitutions provide, or some courts have held, that an individual's right to privacy must be balanced against a compelling state interest in disclosure. In *Cutter v. Brownbridge*,³⁸¹ the court held that, even though a patient has a constitutionally protected interest in his or her medical file, a "disclosure may be appropriate in narrowly limited circumstances to serve a compelling interest."³⁸² However, when there has been a deliberate disclosure of one's personal information, the disclosure "leaves no room for the careful balancing that must take place prior to possible infringement of a constitutional right."³⁸³

Hawaii's constitution provides that "[t]he right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest."³⁸⁴ Montana's constitution similarly provides that "[t]he right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."³⁸⁵

In some states the courts have recognized a constitutional right to privacy. In 2002, the Supreme Court of Arkansas held that "Arkansas has a rich and compelling tradition of protecting individual privacy" and that a "fundamental right to privacy [is] guaranteed to the citizens of Arkansas."³⁸⁶

Georgia's Supreme Court has held that there is an implicit right to privacy in Georgia's constitution, stating "that Georgia citizens have a liberty of privacy guaranteed by the Georgia constitutional provision which declares that no person shall be deprived of liberty except by due process of law."³⁸⁷

³⁶⁸ Douma and Deckenbach, *supra* note 2, at 307. See also NATIONAL CONFERENCE OF STATE LEGISLATURES, *Privacy Protections in State Constitutions* (citing ALASKA CONST. art. 1, § 22; ARIZ. CONST. art. 2, § 8; CAL. CONST. art. 1, § 1; FLA. CONST. art. 1, § 12; HAW. CONST. art. I, § 6; ILL. CONST. art. I, § 6; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; and WASH. CONST. art. I, § 7), available at <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx> (last accessed Oct. 12, 2015).

³⁶⁹ ALASKA CONST. art. 1, § 22 (2015).

³⁷⁰ ARIZ. CONST. art. 2, § 8 (2015) ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.").

³⁷¹ FLA. CONST. art. 1, § 23 (2015) ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life....").

³⁷² MONT. CONST. art. 2, § 10 (2015) ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.").

³⁷³ WASH. CONST. art. 1, § 7 (2015) ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.").

³⁷⁴ ALASKA CONST. art. 1, § 22 (2015).

³⁷⁵ ARIZ. CONST. art. 2, § 8.

³⁷⁶ CAL. CONST. art. 1, § 1 (2015).

³⁷⁷ *Id.*

³⁷⁸ FLA. CONST. art. 1, § 12.

³⁷⁹ IOWA CONST. art. 1, § 1 (Lexis 2012).

³⁸⁰ See FLA. CONST. art. 1, § 12 (2015); HAW. CONST. art. 1, § 7; ILL. CONST. art. 1, § 6; LA. CONST. art. 1, § 5; S.C. CONST. art. 1, § 10.

³⁸¹ 183 Cal. App. 3d 836, 228 Cal. Rptr. 545 (Cal. App. 1986).

³⁸² *Id.* at 842, 228 Cal. Rptr. at 549.

³⁸³ *Id.*, 183 Cal. App. 3d at 847, 228 Cal. Rptr. at 553 (citations omitted).

³⁸⁴ HAW. CONST. art. 1, § 6.

³⁸⁵ MONT. CONST. art. 2, § 10.

³⁸⁶ *Jegley v. Picado*, 349 Ark. 600, 632, 80 S.W.3d 332, 349–350 (2002).

³⁸⁷ *Powell v. State*, 270 Ga. 327, 329, 510 S.E.2d 18, 21 (1998) (citing *Pavesich v. New England Life Ins. Co.*, 122 Ga. 190, 197, 50 S.E. 68, 71 (Ga. 1905) (internal citation omitted)).

The Kentucky Supreme Court likewise has stated that “[t]he right of privacy has been recognized as an integral part of the guarantee of liberty in our 1891 Kentucky Constitution since its inception.”³⁸⁸

B. States Recognizing an Implied Cause of Action for a Violation of a State Constitutional Provision

In *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*,³⁸⁹ the United States Supreme Court held that there is an implied right of action for a violation of the U.S. Constitution’s prohibition on unreasonable searches and seizures. Since *Bivens*, although some state courts have held that an “an individual may bring a cause of action for monetary damages for violations of state constitutional provisions,” other states’ high courts have not done so.³⁹⁰ Some state courts that have recognized an implied cause of action under their state constitution did not rely solely on the Supreme Court’s reasoning in *Bivens*,³⁹¹ but relied also on the common law³⁹²

³⁸⁸ Commonwealth v. Wasson, 842 S.W.2d 487, 495 (Ky. 1993).

³⁸⁹ 403 U.S. 388, 91 S. Ct. 1999, 29 L. Ed. 2d 619 (1971) (holding that the plaintiff was entitled to redress for his injuries caused by federal agents’ violation of his Fourth Amendment rights), *on remand*, 456 F.2d 1339 (2d Cir. N.Y. 1972) (holding that the federal agents were not immune from actions for damages based on allegations of constitutional violations but that the defenses of good faith and reasonable belief were available).

³⁹⁰ Sharon N. Humble, Annotation, *Implied Cause of Action for Damages for Violation of Provisions of State Constitutions*, 75 A.L.R. 5th 619, at [2a] (2000) [hereinafter Humble] (*citing* Porten v. University of San Francisco, 64 Cal. App. 3d 825, 134 Cal. Rptr. 839 (1st Dist. 1976) (recognizing an implied cause of action for violations of the right to privacy); Fenton v. Groveland Community Services Dist., 135 Cal. App. 3d 797, 185 Cal. Rptr. 758 (Cal. App. 1982) (recognizing an implied cause of action for a violation of the right to vote); Phillips v. Youth Development Program, Inc., 390 Mass. 652, 459 N.E.2d 452 (1983) (recognizing an implied cause of action for violation of the right to due process); Johnson v. Wayne Co., 213 Mich. App. 143, 540 N.W.2d 66 (1995) (recognizing an implied cause of action for violations of the rights of equal protection and due process and right to be free from cruel and unusual punishment); and Woodruff v. Board of Trustees of Cabell Huntington Hosp., 173 W. Va. 604, 319 S.E.2d 372 (1984) (recognizing an implied right of action for an alleged violation of the right to free speech)).

³⁹¹ Humble, *supra* note 390, at [3b] (*citing* Porten v. University of San Francisco, 64 Cal. App. 3d 825, 134 Cal. Rptr. 839 (1976); Lamartiniere v. Allstate Ins. Co., 597 So. 2d 1158 (La. App. 1992); and Bott v. DeLand, 922 P.2d 732 (Utah 1996)).

³⁹² *Id.* at [3c] (*citing* Moody v. Hicks, 956 S.W.2d 398 (Mo. Ct. App. E.D. 1997); DiPino v. Davis, 354 Md. 18, 720 A.2d 354 (1999); and Brown v. Consolidated Rail Corp., 223 N.J. Super. 467, 538 A.2d 1310 (App. Dis. 1988)).

or Section 874A of the *Restatement (Second) of Torts*.³⁹³

When a legislative provision protects a class of persons by proscribing or requiring certain conduct but does not provide a civil remedy for the violation, the court may, if it determines that the remedy is appropriate in furtherance of the purpose of the legislation and needed to assure the effectiveness of the provision, accord to an injured member of the class a right of action, using a suitable existing tort action or a new cause of action analogous to an existing tort action.³⁹⁴

In 1986, in *Cutter v. Brownbridge*, a psychotherapist revealed information about his patient to the patient’s wife while they were in the midst of a divorce, which resulted in the plaintiff’s loss of his visitation rights.³⁹⁵ A California appellate court held that the privacy provision in the California Constitution “is self-executing[] and needs no legislation to create ‘a legal and enforceable right of privacy for every Californian.’”³⁹⁶ Violation of a privacy right is permissible only “when the need for disclosure outweighs [the plaintiff’s] interest in privacy.”³⁹⁷ Because the plaintiff’s privacy interests outweighed the need for disclosure,³⁹⁸ the court reversed the lower court’s dismissal of the plaintiff’s complaint.³⁹⁹

In 1990, in *Moresi v. State*,⁴⁰⁰ the Louisiana Supreme Court recognized an implied right of action for a violation of Article I, Section 5 of the 1974 Louisiana Constitution.⁴⁰¹ Article I, Section 5 states that “[e]very person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy,” and that “[a]ny person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality.”⁴⁰² However, as had the Supreme Court in *Bivens*, and later the New York Court of Appeals in *Brown*, discussed below, the Louisiana Supreme Court recognized a qualified immunity defense for acting in good faith.⁴⁰³ The police

³⁹³ *Id.* at [3a] (*citing* Brown v. State, 89 N.Y.2d 172, 652 N.Y.S.2d 223, 674 N.E.2d 1129 (N.Y. 1996) and Dorwart v. Caraway, 2002 MT 240, 312 Mont. 1, 58 P.3d 128 (Mont. 2002)).

³⁹⁴ *Restatement (Second) of Torts*, § 874A (1965).

³⁹⁵ *Cutter*, 183 Cal. App. 3d 836, 228 Cal. Rptr. 545 (Cal. App. 1986), *overruled in part*, Jacob B. v. County of Shasta, 40 Cal. 4th 948, 56 Cal. Rptr. 3d 477, 154 P.3d 1003 (2007) (holding that the litigation privilege applies even to a constitutionally based privacy cause of action).

³⁹⁶ *Id.* at 842, 228 Cal. Rptr. at 549.

³⁹⁷ *Id.* at 843, 228 Cal. Rptr. at 552.

³⁹⁸ *Id.* at 848, 228 Cal. Rptr. at 553.

³⁹⁹ *Id.* at 844, 228 Cal. Rptr. at 553.

⁴⁰⁰ 567 So. 2d 1081 (La. 1990).

⁴⁰¹ *Id.* at 1093.

⁴⁰² *Id.* at 1091–1092 (*quoting* LA. CONST. art. I, § 5 (1974)).

⁴⁰³ *Id.* at 1094 (*citing* Butz v. Economou, 438 U.S. 478, 506–507, 98 S. Ct. 2894, 2911, 57 L. Ed. 2d 895, 916 (1977)).

officers were acting in good faith because their “investigatory stops [were] based on reasonable, articulable suspicion [that] do not violate state constitutional law principles.”⁴⁰⁴ The officers were not liable for an intentional infliction of emotional distress, because their actions were not intentional, and the plaintiff did not allege or prove any physical harm or genuine and serious mental distress.⁴⁰⁵

In 1996, the New York Court of Appeals held in *Brown v. State*⁴⁰⁶ that “a cause of action to recover damages may be asserted against the State for a violation of the Equal Protection and Search and Seizure Clauses of the Constitution.”⁴⁰⁷ In *Brown*, an elderly woman had been attacked near a college campus by someone described as a black male.⁴⁰⁸ To assist the police with their investigation, the university provided the state police and campus police with the name and address of every black male attending the university.⁴⁰⁹ When questioning students, the state and local police stopped and interrogated every nonwhite male that they encountered during a 5-day period.⁴¹⁰ The incident led to a class action on behalf of the nonwhite males who were stopped and interrogated, who alleged that the actions of the police were unconstitutional.⁴¹¹ Following the precedent set in *Bivens*, the court held that there was an implied right of action: “implying a damage remedy here is consistent with the purpose underlying the duties imposed by these provisions and is necessary and appropriate to ensure the full realization of the rights they state.”⁴¹² However, unlike in *Bivens*, an immunity defense was not available because New York had waived immunity for the acts of its officers and employees.⁴¹³

Although in *Brown*, the New York Court of Appeals recognized an implied cause of action for a violation of the right to privacy, an appellate court in New York in *Augat v. State*⁴¹⁴ held that because the

plaintiffs had adequate common law tort remedies, their claims based on alleged violations of the right to due process or freedom of association were not cognizable.⁴¹⁵ The court distinguished the *Brown* case on the basis that the plaintiff in *Brown* did not have an adequate, alternative remedy under the common law as the plaintiffs had in *Augat*.⁴¹⁶

Finally, some states do not recognize an implied cause of action for a state constitutional violation, such as Tennessee.⁴¹⁷

VI. RIGHT TO PRIVACY UNDER STATE STATUTES

A. Introduction

In the absence of a federal statute applicable to privacy and the states, statutes in some states may be a source of privacy law applicable to the collection, use, disclosure, and/or retention by transportation agencies of secure data or monitoring data. Some states’ laws on the protection of information collected by state agencies mandate “openness on the kind of information being collected; avenues of access for the citizens to see what information is being collected about them and to make appropriate corrections; limitations on secondary usage of individual information; and security requirement for how that information is maintained.”⁴¹⁸

⁴¹⁵ *Id.* at 837, 666 N.Y.S.2d at 251–252.

⁴¹⁶ *Id.* at 837–838, 666 N.Y.S.2d at 251–252. Furthermore, the court in *Augat* did not address whether there was a cause of action for the constitutional violations alleged by the plaintiffs because their notice of intention to file was untimely. *Augat*, 666 N.Y.S.2d at 251, 244 A.D.2d at 836–837.

⁴¹⁷ *Wooley v. Madison County, Tennessee*, 209 F. Supp. 2d 836 (W.D. Tenn. 2002). See *Humble*, *supra* note 390.

⁴¹⁸ *Douma and Deckenbach*, *supra* note 2, at 308–309 (citing COLO. REV. STAT. § 24.72.204(3)(a) (2008); CONN. GEN. STAT. ANN. § 4.190 (2007); FLA. STAT. ANN. § 282.318 (2009); HAW. REV. STAT. § 286.172 (2009); MINN. STAT. § 13.01 (2005); N.Y. PUB. OFF. § 91 (2008); and OHIO REV. CODE ANN. § 1347.01 (2009)). See also DEL. CODE ANN. tit. 29, §§ 9017C-9021C (2015); IOWA CODE § 22.11 (2015) (“Each state agency shall adopt rules which describe the nature and extent of the personally identifiable information collected by the agency.”); ME. REV. STAT. tit. 1, §§ 541–42 (2015) (“Each public entity that has a publicly accessible site on the internet...shall develop a policy regarding its practices relating to personal information and shall post notice of those practices on its publicly accessible site.”); MASS. ANN. LAWS ch. 66A, § 3 (2015) (stating that “the Secretary of each executive office shall promulgate regulations to carry out purposes of this chapter which shall be applicable to all agencies.”); MINN. STAT. ANN. § 13.15 (2015) (“A governmental entity that creates, collects, or maintains electronic access data...must inform persons gaining access to the entity’s computer of the creation, collection, or maintenance of the information.”); MONT. CODE ANN. § 2-17-550-53 (2015); and TEX. GOV’T

⁴⁰⁴ *Id.* at 1094, 1096.

⁴⁰⁵ *Id.* at 1095–1096.

⁴⁰⁶ 89 N.Y.2d 172, 652 N.Y.S.2d 223, 674 N.E.2d 1129 (1996).

⁴⁰⁷ *Id.* at 188, 652 N.Y.S.2d at 232–233, 674 N.E.2d at 1138–1139.

⁴⁰⁸ *Id.* at 176–177, 652 N.Y.S.2d at 225, 674 N.E.2d at 1131.

⁴⁰⁹ *Id.* at 177, 652 N.Y.S.2d at 225–226, 674 N.E.2d at 1131–1132.

⁴¹⁰ *Id.* at 177, 652 N.Y.S.2d at 226, 674 N.E.2d at 1132.

⁴¹¹ *Id.* at 175–176, 652 N.Y.S.2d at 225, 674 N.E.2d at 1131.

⁴¹² *Id.* at 189, 652 N.Y.S.2d at 233, 674 N.E.2d at 1139–1140.

⁴¹³ *Id.* at 195, 652 N.Y.S.2d at 237, 674 N.E.2d at 1143 (citing N.Y. Court of Claims Act § 9(2)).

⁴¹⁴ 244 A.D.2d 835, 666 N.Y.S.2d 249 (3d Dep’t 1997).

Although some states ban or limit the use of certain types of technology or devices (see Section VI.E), there seem to be no state laws “that specifically address privacy rights and transportation technologies.”⁴¹⁹ Even when state privacy laws are applicable, only some states’ privacy laws authorize a private right of action for a violation of an individual’s privacy.⁴²⁰

B. Specific State Privacy Statutes

The state privacy statutes applicable to personal information collected and maintained by state agencies have a variety of names.⁴²¹ State statutory provisions that require state and/or local agencies to give notice of a breach of the security of personal data that they collect, use, or maintain are discussed in Section VII.

Some states’ statutes mirror the Privacy Act’s protection against disclosure of personal information, as well as the Privacy Act’s protection of agencies for non-intentional, non-willful disclosures.⁴²² California’s Information Practices Act (IPA) of 1977 states that:

(a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

CODE ANN. § 2054.126 (2015) (requiring state agencies to post their privacy policy on their Web site and to include a statement in their policy “specifying other policies necessary to protect from public disclosure personal information submitted by a member of the public to a state agency’s Internet site”).

⁴¹⁹ Douma and Deckenbach, *supra* note 2, at 309.

⁴²⁰ *Id.* at 308–309.

⁴²¹ See California’s Information Practices Act of 1977 (IPA), CAL. CIV. CODE § 1798, *et seq.* (2015); Illinois’ Personal Information Protection Act, 815 ILL. COMP. STAT. § 530/1, *et seq.* (2015); Louisiana’s Database Security Breach Notification Law, LA. REV. STAT. § 51:3071, *et seq.* (2015); Maine’s Notice of Risk to Personal Data Act, MAINE REV. STAT. tit. 10, § 1346, *et seq.* (2015); Michigan’s Identity Theft Protection Act, MICH. COMP. LAWS § 445.63, *et seq.* (2015); Minnesota’s Government Data Privacy Act, MINN. STAT. § 13.01, *et seq.* (2015); Nevada’s Security of Personal Information, NEV. REV. STAT. § 603A.030, *et seq.* (2015); Oklahoma’s Security Breach Notification Act, OKLA. STAT. § 24-161, *et seq.* (2015); Pennsylvania’s Breach of Personal Information Notification Act, 73 PA. CONS. STAT. § 2301, *et seq.* (2015); Rhode Island’s Identity Theft Protection Act of 2005, R.I. GEN. LAWS § 11-49.2-1, *et seq.* (2015); Tennessee’s Identity Theft Deterrence Act of 1999, TENN. CODE § 47-18-2101, *et seq.* (2015); and Virginia’s Government Data Collection and Dissemination Practices Act, VA. CODE ANN. § 2.2-3800, *et seq.* (2015).

⁴²² Indiana Fair Information Practices Act, IND. CODE ANN. §§ 4-1-6-1 to 4-1-6-8 (2015) and § 4-1-6-19(d) (2015) (defining state agency). See also Massachusetts Fair Information Practices Act, MASS. GEN. LAWS ch. 66A, §§ 1-3 (2015) (imposing duties on state agencies regarding personal data they maintain); N.Y. PUB. OFF. LAW § 95 (2015); Government Data Collection and Dissemination Practices Act, VA. CODE ANN. §§ 2.2-3800 and 2.2-3801(2) (2015).

(b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

(c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.⁴²³

California’s IPA governs the collection, use, and disclosure of personal information held by state agencies; however, the statute does not apply to city or county agencies.⁴²⁴ In California, each agency must keep only that amount of personal information that is “relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government.”⁴²⁵ As discussed in Section VI.C, the IPA provides an individual with a private right of action to redress a violation of a privacy right.

In Colorado, each governmental entity is required to create a privacy policy to standardize the “collection, storage, transfer, and use of personally identifiable information” within each such governmental entity.⁴²⁶ However, the statute does not create a “private cause of action based on alleged violations” of the section.⁴²⁷

In Massachusetts, state agencies must “maintain personal data with such accuracy, completeness, timeliness, pertinence, and relevance as is necessary to assure fair determination of a data subject’s qualifications”⁴²⁸ and have policies for safeguarding individuals’ private information.⁴²⁹ Furthermore, a state agency may not “collect or maintain more personal data than are reasonably necessary for the performance of the [agency’s] statutory function.”⁴³⁰ Holders of personal information must identify one individual who is responsible for a data system to prevent access to or the dissemination of personal data.⁴³¹ Government agencies are authorized to promulgate necessary rules and regulations.⁴³² In contrast to Colorado, Massachusetts law creates a private cause of action for a violation of its privacy law.⁴³³

The Minnesota Government Data Privacy Act (MGDPA) “regulates the *collection, creation, storage,*

⁴²³ CAL. CIV. CODE § 1798.1 (2015) (emphasis added).

⁴²⁴ CAL. CIV. CODE § 1798.14 (2015).

⁴²⁵ *Id.*

⁴²⁶ COLO. REV. STAT. § 24-72-501-02(1) (2015).

⁴²⁷ COLO. REV. STAT. § 24-72-502(3) (2015).

⁴²⁸ MASS. ANN. LAWS ch. 66A, § 2(h) (2015).

⁴²⁹ MASS. ANN. LAWS ch. 66A, § 2(a) (2015).

⁴³⁰ MASS. ANN. LAWS ch. 66A, § 2(l) (2015).

⁴³¹ MASS. ANN. LAWS ch. 66A, § 2(a) (2015).

⁴³² MASS. ANN. LAWS ch. 66A, § 3 (2015).

⁴³³ MASS. ANN. LAWS ch. 214, § 3B (2015).

maintenance, dissemination, and access to government data in government entities.”⁴³⁴ The MGDPA does not use the term “secure data,” but the Act applies to all “data in which any individual is or can be identified as the subject of that data.”⁴³⁵ The MGDPA also does not use the term “monitoring data” but defines the term “not data on individuals” to mean that there is no identification of individuals in the data.⁴³⁶

In Ohio, the privacy statutes that govern personal information systems require every state or local agency that maintains a personal information system to take steps and implement procedures to monitor the accuracy of the data and protect personal information in the system.⁴³⁷ Agencies are directed to “collect, maintain, and use” only personal information that is necessary and relevant to the agencies’ functions as required by law.⁴³⁸ The term “personal information” is defined as “any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.”⁴³⁹

Virginia’s Government Data Collection and Dissemination Practices Act (GDCDPA) states that “an individual’s privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information”⁴⁴⁰ and that procedures must be established for systems having records on individuals.⁴⁴¹ The Virginia statute applies to “any agency...or governmental entity of the Commonwealth or of any unit of local government,”⁴⁴² as well as any entity, public or private, having a contract to operate “a system of personal information....”⁴⁴³ The GDCDPA requires government agencies and entities to adhere to 10 principles of information practice.⁴⁴⁴

⁴³⁴ MINN. STAT. § 13.01, subdiv. 3 (2015) (emphasis added).

⁴³⁵ MINN. STAT. § 13.02, subdiv. 5 (2015).

⁴³⁶ MINN. STAT. § 13.02, subdiv. 4 (2015).

⁴³⁷ OHIO REV. CODE §§ 1347.0 and 1347.05(F) and (G) (amendments effective Sept. 29, 2015). The terms “state agency” and “local agency” are defined in OHIO REV. CODE § 1347.01 (2015).

⁴³⁸ OHIO REV. CODE § 1347.05(H) (2015).

⁴³⁹ OHIO REV. CODE § 1347.01(E) (2015).

⁴⁴⁰ VA. CODE ANN. § 2.2-3800(B)(1) (2015).

⁴⁴¹ VA. CODE ANN. § 2.2-3800(B)(4) (2015).

⁴⁴² VA. CODE ANN. § 2.2-3801 (2015).

⁴⁴³ *Id.*

⁴⁴⁴ VA. CODE ANN. § 2.2-3800(C)(1)-(10) (2015).

C. Whether There Are Separate Claims Based on the Owner or Type of Data or on the Collection, Use, Disclosure, or Maintenance of Data

Although some state privacy laws include a provision authorizing a private right of action for a violation of the statute,⁴⁴⁵ the statutes reviewed for the digest have not established different claims based on the owner or type of data and/or the data’s manner of collection, use, disclosure, or maintenance. Although the state statutes generally do not distinguish between intentional and non-intentional violations of the state’s requirements applicable to an agency’s handling of personal information, a few statutes were located that seem to limit a cause of action to an intentional, willful, or knowing violation of privacy.

For example, California’s IPA provides that an individual may bring a civil action against an agency if the agency:

(a) Refuses to comply with an individual’s lawful request to inspect pursuant to subdivision (a) of Section 1798.34.

(b) Fails to maintain any record concerning any individual with such accuracy, relevancy, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, opportunities of, or benefits to the individual that may be made on the basis of such record, if, as a proximate result of such failure, a determination is made which is adverse to the individual.

(c) Fails to comply with any other provision of this chapter, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual.⁴⁴⁶

The IPA does not create separate claims based on different types of data or a government agency’s means of collection, use, disclosure, or retention of the data. Under the IPA there are two possible claims for damages. First, under subsection (b) an individual may claim damages for an agency’s failure to maintain an accurate and complete record “relating to the qualifications, character, rights, opportunities of, or benefits to the individual that may be made on the basis of such record.” Second, under subsection (c) an individual may claim damages for the agency’s failure “to comply with *any other provision* of this chapter, or any rule promulgated thereunder, in such a way as to have an

⁴⁴⁵ *See, however,* COLO. REV. STAT. § 24-72-501-02(3) (2015); FLA. STAT. § 627.4091(3) (2015); and S.C. CODE ANN. § 30-2-300(3) (2015) (stating that “an affected individual may petition the court for an order directing compliance with this section, but liability may not accrue”).

⁴⁴⁶ CAL. CIV. CODE § 1798.45 (2015).

adverse effect on an individual.”⁴⁴⁷ An agency may be held liable for a violation of §§ 1798.45(b) or (c) for an individual’s actual damages, including damages for mental suffering, and reasonable attorney’s fees and costs as determined by the court.⁴⁴⁸

Massachusetts’s privacy law applies to any holder of personal information. A holder is any agency that “collects, uses, maintains or disseminates personal data or any person or entity which contracts or has an arrangement with an agency whereby it holds personal data as part or as a result of performing a governmental or public function or purpose.”⁴⁴⁹

Any holder violating any provision of the privacy law may be held “liable to any individual who suffers any damage as a result of *such violations*,” including exemplary damages.⁴⁵⁰

In Minnesota, the MGDPA does not establish different claims based on a particular type of data or how the data were collected, used, disclosed, or maintained. Rather, the MGDPA applies to all data “*collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use.*”⁴⁵¹ State agencies are responsible for the accurate “collection, use and dissemination of any set of data on individuals and other government data.”⁴⁵² When a government entity enters into a contract with a private entity for data services, “all of the data *created, collected, received, stored, used, maintained, or disseminated* by the private person in performing those functions [are] subject to the requirements” of the MGDPA.⁴⁵³ If there is a breach in security, “[a] government entity that *collects, creates, receives, maintains, or disseminates* private or confidential data on individuals must provide a notification of the breach.”⁴⁵⁴

⁴⁴⁷ CAL. CIV. CODE § 1798.45(b) and (c) (2015) (emphasis added). Under CAL. CIV. CODE § 1798.45(a), an individual may bring an action when an agency “[r]efuses to comply with an individual’s lawful request to inspect pursuant to § 1798.34(a),” in which case the plaintiff may recover attorney’s fees. CAL. CIV. CODE § 1798.46(b) (2015).

⁴⁴⁸ CAL. CIV. CODE §§ 1798.48(a) and (b) (2015).

⁴⁴⁹ MASS. ANN. LAWS ch. 66A, § 1 (2015).

⁴⁵⁰ MASS. ANN. LAWS ch. 214, § 3B (2015) (emphasis added) (stating also that “[n]otwithstanding any liability for actual damages as may be shown, such holder shall be liable for exemplary damages of not less than one hundred dollars for each violation together with such costs and reasonable attorney’s fees as may be incurred in said action”).

⁴⁵¹ MINN. STAT. § 13.02, subdiv. 7 (2015) (emphasis added).

⁴⁵² MINN. STAT. § 13.02, subdiv. 17 (2015) (emphasis added).

⁴⁵³ MINN. STAT. § 13.05, subdiv. 11 (2015) (emphasis added).

⁴⁵⁴ MINN. STAT. § 13.055, subdiv. 2(a) (2015) (emphasis added).

Likewise, in Ohio, although an action may be brought for certain intentional violations as permitted by statute, claims are not differentiated based on the type of personal information or the manner of its collection, use, disclosure, or maintenance. Ohio Rev. Code § 1347.10(A) applies to a wrongful disclosure of personal information. The statute authorizes a person to bring a cause of action against any person when the injured person has been harmed by the use of personal information contained in a personal information system. However, the claim must be based on one or more of four kinds of *intentional* conduct.⁴⁵⁵

- (1) Intentionally maintaining personal information that he knows, or has reason to know, is inaccurate, irrelevant, no longer timely, or incomplete and may result in such harm;
- (2) Intentionally using or disclosing the personal information in a manner prohibited by law;
- (3) Intentionally supplying personal information for storage in, or using or disclosing personal information maintained in, a personal information system, that he knows, or has reason to know, is false;
- (4) Intentionally denying to the person the right to inspect and dispute the personal information at a time when inspection or correction might have prevented the harm.⁴⁵⁶

In authorizing a private right of action for damages, the Ohio privacy statute does not use the terms state or local agency in Section 1347.10(A), but does use the terms state or local agency in subpart B in regard to injunctions.⁴⁵⁷ Moreover, Section 1347.10(A) does not provide that a state or local agency may be held liable for damages, but subsection (B) authorizes an action for an injunction

⁴⁵⁵ The term “system” is defined to mean, *inter alia*, “any collection or group of related records that are kept in an organized manner and that are maintained by a state or local agency, and from which personal information is retrieved by the name of the person or by some identifying number, symbol, or other identifier assigned to the person.” OHIO REV. CODE § 1347.01(F) (2015).

⁴⁵⁶ OHIO REV. CODE §§ 1347.10(A)(1)-(4) (2015). Section § 1347.10(A) states that one “who is harmed by the use of personal information that relates to him and that is maintained in a personal information system may recover damages in civil action from any person who directly and proximately caused the harm....”

⁴⁵⁷ OHIO REV. CODE § 1347.10(B) (2015) (“Any person who, or any state or local agency that, violates or proposes to violate any provision of this chapter may be enjoined by any court of competent jurisdiction. ...An action for an injunction may be prosecuted by the person who is the subject of the violation, by the attorney general, or by any prosecuting attorney.”)

against a state or a local agency.⁴⁵⁸ Although the term “individual” is defined elsewhere in the statute, the term “person” is not defined. The terms “state agency” and “local agency” are defined, but the definitions do not include natural persons.⁴⁵⁹

Section 1347.15(B) of the Ohio statute requires each state agency to adopt rules regulating access to the confidential personal information that the agency keeps. If a person is harmed by a violation of an agency rule required by subsection B, the person may bring an action in the court of claims against any person who “directly and proximately caused the harm.”⁴⁶⁰ The Ohio statute further directs that:

(1) No person shall *knowingly* access confidential personal information in violation of a rule of a state agency described in division (B) of this section.

(2) No person shall *knowingly* use or disclose confidential personal information in a manner prohibited by law....⁴⁶¹

A violation of either subsection is also a violation of a state statute as provided under Ohio Rev. Code § 124.341(A).⁴⁶²

Under Virginia’s GDCDPA, an injunction may be sought against any person or agency that is violating or that is about to violate a provision of the privacy law.⁴⁶³ There is no provision in the Virginia statute for the recovery of damages except in the limited situation of a violation of Va. Code Ann. Section 2.2-3808(A)(1). The section provides that, unless disclosure is required by law, an agency or a public officer, appointee, or employee of an agency may not require an individual to disclose his or her Social Security number or deny “any service, privilege, or right to an individual” who refused to disclose his or her Social Security number.⁴⁶⁴ If there is a *willful and knowing* violation of Section 2.2-3808(A), a civil penalty may be imposed in the amount set by the statute.⁴⁶⁵

⁴⁵⁸ *Id.*

⁴⁵⁹ OHIO REV. CODE §§ 1347.01(A) and (B) (2015). *See* OHIO REV. CODE § 1347.12(A)(5) (2015) (individual defined as a natural person).

⁴⁶⁰ OHIO REV. CODE §§ 1347.15(G) (2015).

⁴⁶¹ OHIO REV. CODE §§ 1347.15(H)(1) and (2) (2015) (emphasis added).

⁴⁶² OHIO REV. CODE §§ 1347.15(H)(4) (2015). OHIO REV. CODE § 124.341 is entitled “violation or misuse—whistleblower protection.”

⁴⁶³ VA. CODE ANN. § 2.2-3809 (2015).

⁴⁶⁴ VA. CODE ANN. § 2.2-3808(A)(1) (2015).

⁴⁶⁵ VA. CODE ANN. § 2.2-3809 (2015) (providing that if an agency or a specific public officer, appointee, or employee of an agency commits a violation, a court may impose a civil penalty of not less than \$250 or more than \$1,000 and that for a second or subsequent violation a court may impose a penalty of not less than \$1,000 or more than \$2,500).

D. Privacy Policies Required by States

Some states direct government agencies to adopt and implement privacy regulations and/or to display a privacy policy.⁴⁶⁶

Arkansas requires a state agency having a Web site to include a privacy policy on its Web site and to describe the data being collected and how the data will be used.⁴⁶⁷

Arizona law requires government agencies to “develop and establish commercially reasonable procedures to ensure that entity identifying information or personal identifying information that is collected or obtained by [a] governmental agency is secure and cannot be accessed, viewed or acquired unless authorized by law.”⁴⁶⁸ Arizona also mandates that agency Web sites have a privacy policy disclosing the information “gathering and dissemination practices” related to the Internet.⁴⁶⁹ The statute requires that agencies describe at a minimum the information an agency obtains from individuals online,⁴⁷⁰ how the information is to be used,⁴⁷¹ and the circumstances under which an agency would disclose the information to other entities.⁴⁷²

California requires agencies that collect PII to establish a privacy policy and provide a copy of the policy to subscribers.⁴⁷³

Illinois requires that Web sites of state agencies not “use permanent cookies or other invasive tracking programs that monitor and track website viewing habits,”⁴⁷⁴ unless the tracking adds user value and is “disclosed through a comprehensive online privacy statement.”⁴⁷⁵

Similarly, South Carolina requires state agencies to develop privacy policies to ensure that personal information is only used to fulfill a legitimate public purpose and directs that agencies “minimize instances where personal information is disseminated.”⁴⁷⁶

⁴⁶⁶ *See* CAL. STS. & HIGH. § 31490 (2015); MASS. ANN. LAWS ch. 66A, § 3 (2015) (stating that “the Secretary of each executive office shall promulgate regulations to carry out the purposes of this chapter which shall be applicable to all agencies....”); and TEXAS TRANSP. CODE §§ 730.004–730.007 (2015). *See also* Ben F. Overton & Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion*, 25 FLA. ST. U. L. REV. 25, 44–50 (1997).

⁴⁶⁷ ARK. CODE ANN. §§ 25-1-114(a)-(b) (2015).

⁴⁶⁸ ARK. CODE ANN. §§ 41-4172 (2015).

⁴⁶⁹ ARK. CODE ANN. §§ 41-4152 (2015).

⁴⁷⁰ ARK. CODE ANN. §§ 41-4152(2) (2015).

⁴⁷¹ ARK. CODE ANN. §§ 41-4152(4) (2015).

⁴⁷² ARK. CODE ANN. §§ 41-4172(5) (2015).

⁴⁷³ CAL. STS. & HIGH. § 31490 (2015).

⁴⁷⁴ 5 ILL. COMP. STAT. § 177/10 (2015).

⁴⁷⁵ 5 ILL. COMP. STAT. § 177/10(b)(2) (2015).

⁴⁷⁶ S.C. CODE ANN. §§ 30-2-20 and 30-2-300(3) (2015).

E. State Laws Banning or Restricting the Use of Certain Technology

New Hampshire prohibits highway surveillance, a term that the state defines as “the act of determining the ownership of a motor vehicle or the identity of a motor vehicle’s occupants...through the use of a camera or other imaging device or any other device....”⁴⁷⁷ There are some exceptions, such as for investigations of particular violations or for the operation of a toll collection system.⁴⁷⁸

Other states ban the use of specific technology. As of 2013, according to one source, 12 states banned speed cameras; 9 states banned red light cameras; and several states were considering banning the use of such cameras.⁴⁷⁹

A Pennsylvania statute provides:

(1) No automated red light enforcement system shall be utilized in such a manner as to take a frontal view recorded image of the vehicle as evidence of having committed a violation.

(2)...[C]amera equipment deployed as part of an automated red light enforcement system as provided in this section must be incapable of automated or user-controlled remote intersection surveillance by means of recorded video images. Recorded images collected as part of the automated red light enforcement system must only record traffic violations and may not be used for any other surveillance purposes....⁴⁸⁰

There is an exemption allowing for the issuance of a court order for the above data to be provided for “criminal law enforcement action.”⁴⁸¹

Furthermore, the statute provides that information collected

shall not be deemed a public record under...the Right-to-Know Law. The information shall not be discoverable by court order or otherwise, nor shall it be offered in evidence in any action or proceeding which is not directly related to a violation of this section or any ordinance or resolution of the city....⁴⁸²

Some states, such as California, regulate EDRs by requiring manufacturers to disclose data-tracking

⁴⁷⁷ N.H. REV. STAT. ANN. §§ 236:130(I)-(III)(b)-(e) (2015).

⁴⁷⁸ *Id.*

⁴⁷⁹ See Emmarie Huetteman, *Traffic Cameras Draw More Scrutiny by States*, N.Y. TIMES, Apr. 1, 2013, available at: http://www.nytimes.com/2013/04/02/us/traffic-cameras-draw-more-scrutiny-by-states.html?_r=0 (last accessed Oct. 12, 2015). See also Douma and Deckenbach, *supra* note 2, at 309 (citing CAL. VEH. CODE §§ 21455.5 (Supp. 2003) and 21455.6 (2000); N.J. STAT. ANN. § 39:4-103.1 (2002); OR. REV. STAT. § 810.343-39 (2007); UTAH CODE ANN. § 41-69-608 (2005); and WIS. STAT. § 349.02 (2005) (banning photo radars)).

⁴⁸⁰ 75 PA. CONS. STAT., Vehicles, §§ 3116(e)(1) and (2) (2015).

⁴⁸¹ *Id.*

⁴⁸² 75 PA. CONS. STAT., Vehicles, § 3116(e)(3) (2015).

devices installed in their automobiles.⁴⁸³ Virginia law provides that data may be accessed from a device on a motor vehicle that collects electronic information, not just devices installed by manufacturers, only by the vehicle’s owner or the owner’s agent or legal representative.⁴⁸⁴

Although there are federal regulations that apply to EDRs, the federal regulations are not designed to protect driver privacy and do not require an owner’s consent to the release of data after an accident.⁴⁸⁵

F. State Legislative Trends and Proposed Legislation

With one exception, transportation agencies responding to the survey reported that there are no proposed changes in state law or regulations that would affect their collection of secure data or monitoring data.⁴⁸⁶ The National Conference of State Legislatures publishes information on proposed state legislation.⁴⁸⁷

1. California

In California, Senate Bill 34, introduced December 1, 2014, would regulate operators of an Automatic License Plate Reader (ALPR) to ensure, *inter alia*, that the data an operator collects is protected by “specified security procedures and a usage and privacy policy with respect to that information.”⁴⁸⁸ The bill provides that “[i]n addition to any other

⁴⁸³ Douma and Deckenbach, *supra* note 2, at 309 (citing CAL. VEH. CODE § 9951(c) (2014)); Phillips and Kohm, *supra* note 3, at P16; Garry, Douma, and Simon, *supra* note 2, at 125 N 109 (citing CAL. VEH. CODE § 9951(a) (2012); COLO. REV. STAT. § 12-6-402(a) (2012); ME. REV. STAT. tit. 29-A, § 1972(3) (2012); and N.H. REV. STAT. § 357-G:1(III) (2012)).

⁴⁸⁴ VA. CODE ANN. § 46.1088.6(B) (2015).

⁴⁸⁵ Phillips and Kohm, *supra* note 1, at P19 (citing 49 C.F.R. §§ 563.1–563.12 and § 563.11).

⁴⁸⁶ Alabama DOT, Arkansas DOT, Arizona DOT, District of Columbia DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, North Dakota DOT, Oklahoma DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The exception was the Oregon DOT (citing HB 2919, HB 2356, HB 2596, HB 3142, HB 3154, SB 316, SB 377, SB 514, SB 601, SB 639, SB 640, SB 641, SB 711, and SB 904). The Maine DOT and Ohio DOT did not respond to the question.

⁴⁸⁷ See NCSL *Privacy and Security*, <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-and-security.aspx>, and NCSL *Automated License Plate Readers/State Legislation*, <http://www.ncsl.org/research/telecommunications-and-information-technology/2014-state-legislation-related-to-automated-license-plate-recognition-information.aspx> (last accessed Oct. 12, 2015).

⁴⁸⁸ For full text see http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160SB34&search_keywords=privacy (last accessed Oct. 12, 2015).

sanctions, penalties, or remedies provided by law, an individual who has been harmed by a violation of this title may bring a civil action in any court of competent jurisdiction against a person who knowingly caused that violation.⁴⁸⁹ As of June 2015, the bill had been re-referred to the Assembly Committee on Privacy and Consumer Protection.

2. Florida

In Florida, the Florida Privacy Protection Act, introduced in February 2015, would have protected digital data from unreasonable searches and seizures, including a prohibition of the use of certain technology by law enforcement without a warrant. The bill died in the Judiciary Committee on April 28, 2015.⁴⁹⁰ A similar bill in the Senate died in the Criminal Justice Committee on May 1, 2015.⁴⁹¹

3. Georgia

As in other states, there is a bill pending in the Georgia legislature on the use of ALPRs. House Bill 93 would allow law enforcement to exchange data obtained from ALPRs, prohibit law enforcement from retaining information gathered from ALPRs for more than 90 days, and impose criminal penalties for the misuse of captured license plate data.⁴⁹²

4. Illinois

A bill entitled “Freedom from Automatic License Plate Reader Surveillance Act” was introduced this term in the Illinois Senate to limit the use of ALPRs by the state to toll collection, traffic enforcement, and criminal investigations.⁴⁹³ A similar bill was introduced in the House entitled the “Automated License Plate Recognition System Act” to limit the use of ALPRs to investigations by law enforcement agencies. If enacted, unless the data are necessary for an ongoing investigation, any data collected by ALPRs could be retained only for 30 days.⁴⁹⁴

⁴⁸⁹ Senate Bill 34 § 1798.90.54(a).

⁴⁹⁰ House Bill 571. Status: April 28, 2015, died in the Judiciary Committee.

⁴⁹¹ Senate Bill 1530. Status: May 1, 2015, died in the Criminal Justice Committee.

⁴⁹² House Bill 93. Status: April 2, 2015, House Withdrawn, recommitted.

⁴⁹³ Senate Bill 1753. Status: March 27, 2015, re-referred to Assignments. See <http://www.ilga.gov/legislation/default.asp> (must link to “Senate Bills 1701–1800”) (last accessed Oct. 12, 2015).

⁴⁹⁴ House Bill 3289. Status: May 15, 2015, re-referred to Assignments.

5. Massachusetts

There are several bills pending in the Massachusetts legislature to regulate the use of ALPRs.⁴⁹⁵ House Bill 3102 would allow the data to be used only by law enforcement agencies for legitimate law enforcement purposes and by the department of transportation for the purpose of assessing and collecting tolls.⁴⁹⁶ Senate Bill 1817 and House Bill 3009 are similar, but would expand the permissible uses of ALPRs to parking enforcement, to the control of access to secured areas, and for “the immediate comparison of captured plate data with data held by the Registry of Motor Vehicles, Department of Criminal Justice Information Services, the National Crime Information Center, and the Federal Bureau of Investigation...”⁴⁹⁷ Each bill has been referred to the Joint Committee on Transportation.

6. New York

In New York, a bill would establish a New York state automatic identification technology privacy task force.⁴⁹⁸ With some exceptions for law enforcement functions, the bill would prohibit the disclosure of highway, bridge, tunnel, and other thoroughfare toll and transit records.⁴⁹⁹ Another bill proposes to establish an email privacy act in regard to electronic messaging and individual location.⁵⁰⁰ A fourth bill introduced in the Senate also would prohibit the disclosure of highway, bridge, tunnel, and other thoroughfare toll and transit records except for law enforcement purposes or to support public entities’ official functions.⁵⁰¹

7. North Carolina

In North Carolina, House Bill 876 requires a search warrant to obtain locational data from a cell

⁴⁹⁵ S. 1817, Status: April 15, 2015, referred to Committee on Transportation; H. 3009, Status: January 20, 2015, referred to the Committee on Transportation; SH 3102, Status: January 20, 2015, in Joint Committee on Transportation.

⁴⁹⁶ Draft H. 3102 §§ 2(a)–(b). See <https://malegislature.gov/Bills/189/House/H3102> (last accessed Oct. 12, 2015).

⁴⁹⁷ Draft Bills S. 1817 and H. 3009 §§ 2(a)(1)–(2), (4). See <https://malegislature.gov/Bills/189/Senate/S1817> and <https://malegislature.gov/Bills/189/House/H3009> (last accessed Oct. 12, 2015).

⁴⁹⁸ Assembly Bill A00119. Status: January 7, 2015, referred to Consumer Affairs and Protection. See <http://assembly.state.ny.us/leg/> (keyword “privacy”) (last accessed Oct. 12, 2015).

⁴⁹⁹ Assembly Bill A03975. Status: June 2, 2015, reported referred to rules.

⁵⁰⁰ Assembly Bill A00793. Status: January 7, 2015, referred to codes.

⁵⁰¹ Senate Bill S02173. Status: May 28, 2015, referred to governmental operations.

phone or other electronic device and provides that a violation would be punishable as a Class 1 misdemeanor.⁵⁰² Bills applicable to ALPRs are pending in both chambers of the North Carolina legislature. Senate Bill 182 simply provides that any law enforcement agency using an ALPR must adopt a written policy governing its use, whereas House Bill 829 restricts the use of ALPRs to four purposes, including for electronic toll collection and specific law enforcement purposes.⁵⁰³ Furthermore, the House version creates a right of civil action against anyone who knowingly violates the law.⁵⁰⁴

8. Pennsylvania

In Pennsylvania, Senate Bill 854 would make it unlawful “for any person to utilize tracking technology without lawful authority or consent.”⁵⁰⁵ House Bill 401 entitled “Protecting Pennsylvanians’ Privacy Act” would require a government entity to obtain a search warrant prior to obtaining locational information on an electronic device and would impose a civil penalty for a violation.⁵⁰⁶

9. Texas

In Texas, under House Bill 3929, if an ALPR were to be used for anything other than a “valid law enforcement purpose,” it would become a Class A misdemeanor.⁵⁰⁷ A bill in the Senate, which provides that an ALPR may be used only for investigating a criminal offense or a report of a missing person, mandates that all of the images and data collected from an ALPR are to be destroyed no later than the seventh day after collection.⁵⁰⁸

VII. WHETHER STATE DATA BREACH NOTIFICATION LAWS APPLY TO TRANSPORTATION AGENCIES

A. Definition of a Data Breach

A data breach may be defined “as a loss or theft of, or other unauthorized access to, data containing

⁵⁰² House Bill 876 [Edition 1]. Status: April 15, 2015, referred to Committee on Judiciary.

⁵⁰³ Senate Bill 182 [Edition 2]. Status: April 4, 2015, referred to the Committee on Transportation; House Bill 829 [Edition 2], Status: April 28, 2015, re-referred to the Committee on Rules, Calendar, and Operations of the House.

⁵⁰⁴ House Bill 829 § 20-183.26(a).

⁵⁰⁵ Senate Bill 854. Status: May 28, 2015, referred to Judiciary.

⁵⁰⁶ House Bill 401. Status: February 9, 2015, referred to Judiciary.

⁵⁰⁷ House Bill 3929. Status: May 14, 2015, placed on General State Calendar.

⁵⁰⁸ Senate Bill 1286. Status: March 18, 2015, referred to Criminal Justice.

sensitive personal information that results in the potential compromise of the confidentiality or integrity of the data.”⁵⁰⁹ In Ohio, the term “breach of the security of the system” is defined to mean an

unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a state agency or an agency of a political subdivision and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.⁵¹⁰

B. States Having Data Breach Notification Statutes

As of January 2015, all states except Alabama, New Mexico, and South Dakota have laws requiring that notice be given to the public if there is a security breach involving data having personal information.⁵¹¹ The term “personal information” may be

⁵⁰⁹ Froomkin, *supra* note 213, at 1025 (footnote omitted) (internal quotation marks omitted). See discussion of state notification laws in Dana Rosenfeld and Donnelly McDowell, *Moving Target: Protecting Against Data Breaches Now and Down the Road*, 28 ANTITRUST ABA 90 (2014) [hereinafter Rosenfeld and McDowell]; John A. Fisher, *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215 (2013) [hereinafter Fisher]; Jill Joerling, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J.L. & POL’Y 467 (2010) [hereinafter Joerling]; and Robert Sprague and Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91 (2009) [hereinafter Sprague and Ciocchetti].

⁵¹⁰ OHIO REV. CODE § 1347.12(B)(1) (2015).

⁵¹¹ See National Conference of State Legislatures, *Security Breach Notification Laws* (2015) (*citing* ALASKA STAT. § 45.48.010, *et seq.*; ARIZ. REV. STAT. § 44-7501; ARK. CODE § 4-110-101, *et seq.*; CAL. CIV. CODE §§ 1798.29 and 1798.80, *et seq.*; COLO. REV. STAT. § 6-1-716; CONN. GEN. STAT. § 36a-701b; DEL. CODE tit. 6, § 12B-101, *et seq.*; FLA. STAT. §§ 501.171, 282.0041, and 282.318(2)(i); GA. CODE §§ 10-1-910-912 and § 46-5-214; HAW. REV. STAT. § 487N-1, *et seq.*; IDAHO STAT. §§ 28-51-104-107; 815 ILL. COMP. STAT. §§ 530/1-530/25; IND. CODE § 4-1-11, *et seq.* and 24-4.9, *et seq.*; IOWA CODE §§ 715C.1-715C.2; KAN. STAT. § 50-7a01, *et seq.*; KY. REV. STAT. §§ 365.732 and 61.931-61.934; LA. REV. STAT. §§ 51:3071, *et seq.* and §§ 40:1300.111-1300.116; ME. REV. STAT. tit. 10 § 1347; *et seq.*; MD. CODE COM. LAW § 14-3501, *et seq.*, MD. STATE GOV’T CODE §§ 10-1301-1308; MASS. GEN. LAWS § 93H-1, *et seq.*; MICH. COMP. LAWS §§ 445.63 and 445.72; MINN. STAT. §§ 325E.61 and 325E.64; MISS. CODE § 75-24-29; MO. REV. STAT. § 407.1500; MONT. CODE §§ 2-6-504 and 30-14-1701, *et seq.*; NEB. REV. STAT. §§ 87-801-807; NEV. REV. STAT. §§ 603A.010, *et seq.* and 242.183; N.H. REV. STAT. §§ 359-C:19-C:21; N.J. STAT. §§ 56:8-161-163; N.Y. GEN. BUS. LAW § 899-aa and N.Y. STATE TECH. LAW § 208; N.C. GEN. STAT. §§ 75-61 and 75-65; N.D. CENT. CODE § 51-30-01, *et seq.*, OHIO REV. CODE §§ 1347.12, 1349.19, and 1349.191-192; OKLA. STAT. §§ 74-3113.1 and 24-161-166; OREGON REV. STAT. §§ 646A.600-646A.628; 73 PA. STAT. § 2301, *et seq.*; R.I. GEN.

defined to include a person's name, Social Security number, driver's license number, credit card numbers, security codes, PINs, or passwords.⁵¹² For example, the Ohio statute provides that an agency must disclose a breach of the security of personal information data. Personal information is defined to be

an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

- (i) Social security number;
- (ii) Driver's license number or state identification card number;
- (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.⁵¹³

LAWS § 11-49.2-1, *et seq.*; S.C. CODE § 39-1-90; TENN. CODE § 47-18-2107; TEX. BUS. & COM. CODE §§ 521.002-521.053 and TEX. ED. CODE § 37.007(b)(5); UTAH CODE § 13-44-101, *et seq.*; VT. STAT. tit. 9, §§ 2430 and 2435; VA. CODE §§ 18.2-186.6 and 32.1-127.1:05; WASH. REV. CODE §§ 19.255.010 and 42.56.590; W. VA. CODE § 46A-2A-101, *et seq.*; WIS. STAT. § 134.98; WYO. STAT. § 40-12-501, *et seq.*; and D.C. CODE § 28-3851, *et seq.*), available at: <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (last accessed Oct. 12, 2015). See also Mintz Levin, State Data Security Breach Notification Laws (2015) [hereinafter State Breach Notification Laws], available at: http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf (last accessed Oct. 12, 2015) (analyzing state laws by data and consumers protected; the statutes' definition of a breach; covered entities; notice procedures, timing, and exemptions; whether encryption is a safe harbor; preemption; penalties; and whether the statutes create a private right of action) and Sprague and Ciochetti, *supra* note 509, at 104–105 (also including citations to breach notification statutes).

⁵¹² See ALASKA STAT. § 45.48.090(7)(A) (2015); CAL. CIV. CODE § 1798.29(g) (2015); GA. CODE ANN. § 10-1-911(c) (2015); HAW. REV. STAT. § 487 N-1 (2015); IDAHO CODE § 28-51-104(5) (2015); 815 ILL. COMP. STAT. § 530/5 (2015); IND. CODE § 4-1-11-3 (2015); KANSAS STAT. ANN. § 50-7a01(g) (2015); LA. REV. STAT. §§ 3073(4)(a) and (b) (2015); MAINE REV. STAT. tit. 10, § 1347(6) (2015); MASS. GEN. LAWS ch. 93H, § 1(a) (2015); MICH. COMP. LAWS 445.63 §§ 3(q) and (r) (2015) (defining personally identifying information and personal information, respectively); MONTANA CODE ANN. §§ 2-6-501(4) (a) and (b) (2015); NEV. REV. STAT. § 603A.040 (2015); NEW JERSEY STAT. ANN. § 56:8-161 (2015); OHIO REV. CODE § 1347.01(E) (2015); OKLA. STAT. §§ 24-162(6) and 74-3113.1(D)(2) (2015); 73 PA. CONS. STAT. § 2302 (2015); R.I. GEN. LAWS § 11-49.2-5(c) (2015); S.C. CODE § 39-1-90(D)(3) (2015); VERMONT STAT. tit. 9, ch. 62 § 2430(5)(A) (2015) (defining the term “personally identifiable information”); VA. CODE § 18.2-186.6(A) (2015); WASH. REV. CODE § 19.255.010(5) (2015); W. VA. CODE, art. 2A, § 46A-2A-101(6) (2015); WIS. STAT. § 134.98(1)(b) (2015); and 14 V.I. CODE § 2208(e) (2015).

⁵¹³ OHIO REV. CODE § 1347.12(A)(6)(a) (effective Sept. 29, 2015). See also OHIO REV. CODE § 1347.01(E) (2015).

Washington State's breach notification law applies to personal information, a term that

(5) ...means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (a) Social security number;
- (b) Driver's license number or Washington identification card number; or
- (c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.⁵¹⁴

(6) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.⁵¹⁵

C. Applicability of the Statutes to Government Agencies

Although the breach notification statutes apply to businesses and commercial entities as defined in each statute, in at least 23 states, the statutes also apply to government agencies.⁵¹⁶

⁵¹⁴ WASH. REV. CODE § 19.255.010(5) (2015).

⁵¹⁵ WASH. REV. CODE § 19.255.010(6) (2015)..

⁵¹⁶ ALASKA STAT. §§ 45.48.090(2)(B) and (3) (2015) (stating that the term “covered person” includes a government agency, meaning “a state or local governmental agency, except for an agency of the judicial branch”); see also ALASKA STAT. § 45.48.090(4) (2015) (defining the term “information collector” to mean a “covered person who owns or licenses personal information in any form” on a state resident); CAL. CIV. CODE § 1798.14 (2015) (directing an agency to maintain only relevant and necessary personal information in its records); GA. CODE § 10-1-911(2) (2015) (defining the term “data collector” to include “any state or local agency or subdivision thereof...or other government entity,” but excepting agency records maintained primarily for traffic safety, law enforcement, or licensing purposes); HAW. REV. STAT. § 487 N-1 (2015) (chapter also applying to a government or instrumentality of the state or any county); IDAHO CODE § 28-51-104(1) (2015) (defining the term “agency” to mean any public agency as defined in IDAHO CODE § 74-101); 815 ILL. COMP. STAT. § 530/5 (2015) (stating that the term “data collector” includes government agencies); INDIANA CODE § 4-1-11-4 (2015) (defining the term “state agency” as set forth in INDIANA CODE § 4-1-10-2); see also INDIANA CODE § 4-1-11-5(a) (2015) (requiring state agencies to disclose security breaches); KANSAS STAT. § 50-7a01(f) (2015) (defining term “person” to include a government or governmental subdivision or agency or other entity) and KAN. STAT. § 3073(1) (2015) (defining the term “agency” to include the state, its political subdivision, agency, or similar body); MAINE REV. STAT. tit. 10, § 1347(5) (2015) (defining the term “person” to include agencies of state government); see also MAINE REV. STAT. § 1347(3) (2015) (defining the term “information broker” as being inapplicable to a governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes); MASS. GEN. LAWS, ch. 93H, § 1(a) (2015) (defining the term “agency” to include

The statutes typically provide that encryption is a defense to a claim for a data breach for any missing, lost, or stolen data.⁵¹⁷ For example, the California breach notification law requires that

[a]ny agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose *unencrypted* personal information was, or is reasonably believed to have been, acquired by an unauthorized person.⁵¹⁸

“any agency, ...authority of the commonwealth, or any of its branches, or of any political subdivision thereof”); MICH. COMP. LAWS 445.63 § 3(a) (2015) (defining the term “agency” to include “a department, board, commission, office, agency, authority, or other unit of state government of this state”); MONTANA CODE § 2-6-501(6)(a) (2015) (defining a state agency to include “an agency, authority, ...or other instrumentality of the legislative or executive branch of state government,” as well as “an employee of a state agency acting within the course and scope of employment”); NEV. REV. STAT. § 603A.030 (2015) (defining the term “data collector” to include “any governmental agency...that...handles, collects, disseminates or otherwise deals with nonpublic personal information”); N.J. STAT. ANN. § 56:8-161 (2015) (defining a public entity to include the state, county, public agency, political subdivision, or other state public body); OHIO REV. CODE §§ 1347.01(A) and (b) (2015) (defining state agency and local agency, respectively); *see also* OHIO REV. CODE § 1347.01(D) (2015) (defining the term “maintain” to mean state or local ownership of, control over, responsibility for, or accountability for data systems and §§ 1347.12(A)(1) and (B)(1) (2015) (defining agency of a political subdivision); OKLA. STAT. § 24-162(2) (2015) (stating that the term “entity” includes “governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity...”); 73 PA. CONS. STAT. § 2302 (2015) (defining the term “entity” to include a state agency or a political subdivision of the Commonwealth); R.I. GEN. LAWS § 11-49.2-3(a) (2015) (applying to “[a]ny state agency or person that owns, maintains or licenses computerized data that includes personal information...”); S.C. CODE §§ 37-1-301(18) and (20) 39-1-90 (2015) (statute applying also to a “governmental subdivision”); TENN. CODE § 47-18-2102(9) (2015) (defining the term “person” to include a “governmental agency...and any other legal or commercial entity however organized...”); VERMONT STAT. tit. 9, ch. 62, § 2430(3) (2015) (defining the term “data collector” to include the state, state agencies, and political subdivisions of the state); VA. CODE § 18.2-186.6 (2015) (defining the term “entity” to include governments, governmental subdivisions, agencies, or instrumentalities; *see also* VA. CODE § 42.56.590(b) (2015) (stating that the term “agency” has the same meaning as in § 42.56.010); W. VA. CODE § 46A-2A-101 (2015) (defining the term “entity” to include governments, governmental subdivisions, agencies, or instrumentalities); WIS. STAT. § 134.98(1)(a)(2) (2015) (defining the term “entity” to include the state and any office, department, independent agency, or state government body, as well as a city, village, town, or county); 14 V.I. CODE § 2208(b) (2015) (applicable to any agency maintaining computerized data with personal information).

⁵¹⁷ Joerling, *supra* note 509, at 471.

⁵¹⁸ California Security Breach Information Act § 1798.29 (a) (emphasis added).

In Ohio, the statute defines the term “agency of a political subdivision” to mean “each organized body, office, or agency established by a political subdivision for the exercise of any function of the political subdivision, except that ‘agency of a political subdivision’ does not include an agency that is a covered entity as defined in 45 C.F.R. 160.103, as amended.”⁵¹⁹

In some states there is a good faith defense to the disclosure of personal information as long as the personal information was not used for illegitimate purposes and there were no other unauthorized disclosures of the data.⁵²⁰

D. State Breach Notification Laws Authorizing Civil Penalties or Claims for Damages

1. Overview

Although some breach-notification laws provide for enforcement and civil penalties, it appears that only in 13 states and the District of Columbia would a person injured by a data breach have a private right of action,⁵²¹ and that at least 4 states exempt government agencies from “enforcement proceedings.”⁵²²

Of the states in which the breach notification laws apply to government agencies, the states differ in regard to a right of action against government agencies for a violation of the statute. In some states, no action is permitted against government entities or there is no provision for a private right of action. Some state statutes provide for the imposition of a civil penalty for a violation of the breach notification statute, whereas other states authorize a claim for damages. Some breach notification statutes delegate authority to the attorney general to bring an action for a violation.

⁵¹⁹ OHIO REV. CODE § 1347.12(A)(1) (2015).

⁵²⁰ Joerling, *supra* note 509, at 471.

⁵²¹ Alaska (but not against government agencies), California, Delaware (treble damages and reasonable attorney’s fees), Louisiana (actual damages), Maryland, Massachusetts (in certain situations), Minnesota, New Hampshire, North Carolina, Rhode Island, South Carolina, Virginia, Washington, and the District of Columbia. *See State Breach Notification Laws, supra* note 511. *See* Joerling, *supra* note 509, at 479 N 63 (citing California Security Breach Information Act, CAL. CIV. CODE § 1798.84 (2009); D.C. CODE ANN. § 28-3853(a) (2009); N.H. REV. STAT. ANN. § 359-C:21(I) (2009); N.C. GEN. STAT. ANN. § 75-65 (2007); OR. REV. STAT. ANN. § 646A.624 (2009); S.C. CODE ANN. § 37-20-170 (2008); TENN. CODE ANN. § 47-18-2107(h) (2009); and WASH. REV. CODE ANN. § 19.255.010(10)(9) (2007)). *See also* Sprague and Ciocchetti, *supra* note 509, at 106 (at that time identifying the District of Columbia and 11 states—California, Delaware, Hawaii, Illinois, Louisiana, Maryland, Nevada, North Carolina, Rhode Island, Tennessee, and Washington).

⁵²² Joerling, *supra* note 509, at 476 (*citing* HAW. REV. STAT. ANN. § 487N-2 (2009); FLA. STAT. ANN. § 817.5681 (2006); ME. REV. STAT. ANN. tit. 10, § 1349 (2008); and TENN. CODE ANN. § 47-18-2107 (2009)).

Some of the statutory provisions regarding enforcement, such as for damages or a civil penalty, apply to an agency's failure to give notice of a security breach, whereas some provisions apply to any violation of the state's privacy act protecting personal information maintained by an agency.

2. No Action Permitted Against Government Agencies

In some states no action is permitted against government agencies.⁵²³

3. No Provision for a Private Right of Action

In some states there appears to be no provision for a private right of action.⁵²⁴

4. Liability for Civil Penalties

Some states' statutes provide for the imposition of a civil penalty for a violation of a state statute protecting personal information and/or a violation of a requirement that an agency give notice of a breach of the security of personal information.⁵²⁵

In some states, however, a civil penalty will not be assessed unless an agency's action was willful or intentional. For example, in Idaho, "[a]ny agency, individual or commercial entity that *intentionally*

⁵²³ See HAW. REV. STAT. § 487N-3(a) (2015); MAINE REV. STAT. § 1349(2)(A) (2015) (provisions on enforcement and for imposition of civil penalties for violations of Maine's statute on Notice of Risk to Personal Data not applicable to the state).

⁵²⁴ See GA. CODE § 10-1-910, *et seq.* (2015); 815 ILL. COMP. STAT. § 530/20 (2015) (no specific penalty found that applies to government agencies but a violation constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act); IND. CODE § 4-1-11-2, *et seq.* (2015) (no provision located that permitted a civil action or imposed a civil penalty for a violation); N.J. STAT. ANN. § 56:8-166 (2015) (although stating that it is "unlawful...to willfully, knowingly or recklessly violate sections 10 through 13 of this amendatory and supplementary act," no provision located authorizing a cause of action or imposing a specific civil penalty).

⁵²⁵ ALASKA STAT. § 45.48.080(a) (2015) (stating that an information collector that is a governmental agency is liable to the state for a civil penalty of up to \$500 for each state resident who was not notified under ALASKA STAT. 45.48.010–45.48.090 but total civil penalty may not exceed \$50,000); MICH. COMP. LAWS § 445.72(14) (2015) (applicable to § 445.72's security breach requirements and providing that "[t]he aggregate liability of a person for civil fines under subsection (13) for multiple violations of subsection (13) that arise from the same security breach shall not exceed \$750,000). See MICH. COMP. LAWS § 445.72(15) (2015) (stating that "[s]ubsections (12) and (13) do not affect the availability of any *civil remedy* for a violation of state or federal law"); R. I. GEN. LAWS § 11-49.2-6(a) (2015) (stating that a breach of the state's Identity Theft Protection Act "is a civil violation for which a penalty of not more than a hundred dollars (\$100) per occurrence and not more than twenty-five thousand dollars (\$25,000) may be adjudged against a defendant").

fails to give notice [of a security breach] in accordance with section 28-51-105, Idaho Code, shall be subject to a fine of not more than twenty-five thousand dollars (\$25,000) per breach of the security of the system."⁵²⁶

Montana Code Section 30-14-142(2) provides that if a court finds that "a person is willfully using or has willfully used" an unlawful method, act, or practice, a civil fine of not more than \$10,000 may be imposed for each violation. A willful violation occurs when the party committing the violation knew or should have known that the conduct was a violation of Section 30-14-103.⁵²⁷

5. Liability for Damages

Several states authorize an action for damages for a violation of the state's statute protecting personal information and/or for failure to give notice of a breach of the security of personal information.⁵²⁸

As stated, California's IPA provides that an individual may bring a civil action against an agency whenever the agency refuses to comply with an individual's lawful request to inspect under Section 1798.34(a); fails to maintain accurate and complete records concerning an individual as further provided in the statute; or "[f]ails to comply with any other provision of this chapter, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual."⁵²⁹

In Ohio, Section 1347.12(G) authorizes the attorney general to conduct an investigation and bring a civil action for an alleged failure by a state agency or an agency of a political subdivision to comply with Section 1347.12.⁵³⁰

In South Carolina, a resident who is injured by a violation of the state statute that applies to a breach of the security of "business data" may

⁵²⁶ IDAHO CODE § 28-51-107 (2015) (emphasis added).

⁵²⁷ MONT. CODE § 30-14-142(4) (2015). See also MONT. CODE § 30-14-1705 (2015) (incorporating MONT. CODE § 30-14-142(1)) (authorizing the courts to impose also a civil fine for violating an injunction or temporary restraining order).

⁵²⁸ LA. REV. STAT. § 3075 (2015) (authorizing a civil action "to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information"); TENN. CODE ANN. §§ 47-18-2104 and 22105 (2015) (providing, respectively, for a private right of action and for civil penalties for a violation of the Tennessee Identity Theft Deterrence Act of 1999).

⁵²⁹ CAL. CIV. CODE § 1798.45(a)–(c) (2015). See also CAL. CIV. CODE § 1798.46(b) (2015) (allowing for attorney's fees and other litigation costs for violations of §§ 1798.45(b) or (c)) and § 1798.53 (2015) (allowing actions for invasion of privacy except against state or local government agency employees).

⁵³⁰ OHIO REV. CODE § 1347.12(G) (effective Sept. 29, 2015).

(1) institute a civil action to recover damages in case of a wilful [sic] and knowing violation;

(2) institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section; ...and

(4) recover attorney's fees and court costs, if successful.⁵³¹

Furthermore, under South Carolina law, a person “who knowingly and *wilfully* [sic] violates this section is subject to an administrative fine in the amount of one thousand dollars for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.”⁵³²

In Virginia, although the attorney general is authorized to impose a civil penalty for a security breach, the statute also provides that an individual is not limited “from recovering direct economic damages from a violation....”⁵³³

In Washington, a customer who is injured by a violation of the state's statutory requirement that a notice be given of a breach in the security of personal information may institute a civil action for damages;⁵³⁴ however, an agency is not required to disclose a technical breach of the security system that does not seem reasonably likely to subject a customer to a risk of criminal activity.⁵³⁵

Finally, it may be noted that a number of class actions have been brought against private companies for damages allegedly caused by a breach of security and a theft of PII. However, some cases have been dismissed for lack of standing on the ground that the risk of future injury caused by a breach, such as a possible identity theft, in and of itself is “too speculative to confer standing,”⁵³⁶ or because the plaintiff was unable to show an actual injury-in-fact.⁵³⁷

6. Power Delegated to the Attorney General

Some of the privacy statutes delegate authority to the attorney general to bring an action for a

breach of the statute.⁵³⁸ In Oklahoma, Oklahoma Statute Section 24-165(A) provides for enforcement and a civil penalty for a violation of the Security Breach Notification Act: “A violation of this act that results in injury or loss to residents of this state may be enforced by the Attorney General or a district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act.”

Subsection (B) grants the attorney general or a district attorney exclusive authority to bring an action either for actual damages for a violation of the act or for a civil penalty not to exceed \$150,000 “per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.”⁵³⁹

Vermont's statute on Protection of Personal Information with respect to all data collectors grants the attorney general with some exceptions “sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter....”⁵⁴⁰

In Virginia, the attorney general “may impose a civil penalty not to exceed \$150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation.”⁵⁴¹ However, the section does not “limit an individual from recovering direct economic damages from a violation....”⁵⁴²

The West Virginia Breach of Security Information law provides that the attorney general has exclusive authority to bring an action; that no civil penalty may be assessed unless the court finds that the defendant has engaged in a course of *repeated and willful violations* of article 2A; and that no civil penalty may exceed \$150,000 “per breach of security of the system or series of breaches of a similar nature that are discovered in a single investigation.”⁵⁴³

⁵³⁸ KAN. STAT. § 50-7a02(g) (2015) (empowering the attorney general “to bring an action in law or equity to address violations of this section and for other relief that may be appropriate”); MASS. GEN. LAWS ch. 93H, § 3 (2015) (stating that the “attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate”); OHIO REV. CODE § 1347.12(G) (2015) (stating that the attorney general may conduct an investigation and bring a civil action for an alleged failure by a state agency or agency of a political subdivision to comply with § 1347.12); 73 PA. CONS. STAT. § 2308 (2015) (providing that the attorney general has exclusive authority to bring an action for a violation of the state's Breach of Personal Notification Act).

⁵³⁹ OKLA. STAT. § 24-165(B) (2015).

⁵⁴⁰ VT. STAT. tit. 9, § 2435(g)(1) (2015).

⁵⁴¹ VA. CODE § 18.2-186.6(I) (2015).

⁵⁴² *Id.*

⁵⁴³ W. VA. CODE § 46A-2A-104(b) (2015) (emphasis added).

⁵³¹ S.C. CODE §§ 31-1-90(G) (2015).

⁵³² S.C. CODE § 31-1-90(H) (2015) (emphasis added).

⁵³³ VA. CODE § 18.2-186.6(I) (2015).

⁵³⁴ WASH. REV. CODE § 42.56.59(10)(a) (2015).

⁵³⁵ WASH. REV. CODE § 42.56.59(10)(d) (2015).

⁵³⁶ Rosenfeld and McDowell, *supra* note 509, at 93 (*citing In re TJX Cos. Retail Sec. Breach Litig.*, 527 F. Supp. 2d 209 (D. Mass. 2007) (*affirmed by, in part, vacated by, in part, remanded*, Amerifirst Bank v. TJX Cos. (*In re TJX Cos. Retail Sec. Breach Litig.*), 2009 U.S. App. LEXIS 6636 (1st Cir. Mass., Mar. 30, 2009)).

⁵³⁷ *Id.*; Sprague and Ciochetti, *supra* note 509, at 101 (*citing Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 631 (7th Cir. 2007) (applying Indiana law)).

7. Miscellaneous Provisions

Nevada's statute on the Security of Personal Information provides for a right of action by the data collector, rather than a right of action against the data collector.⁵⁴⁴

The Wisconsin statute provides only that when there is an unauthorized acquisition of personal information, the “[f]ailure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.”⁵⁴⁵

VIII. REMEDIES AT COMMON LAW FOR INVASION OF PRIVACY

A. States that Recognize an Invasion of Privacy at Common Law

The disclosure of private facts when a disclosure would be offensive and objectionable to a reasonable person may give rise to an action in tort for an invasion of privacy.⁵⁴⁶ Although a violation of the right to privacy may create a cause of action, a plaintiff must meet the elements of the tort to maintain a claim.⁵⁴⁷ As discussed in Section IX.A, even if an individual alleges a privacy claim at common law against a transportation agency, in some states the agencies would have sovereign immunity.

Some courts have adopted the *Restatement of Torts (Second)* as the basis for an action for an invasion of privacy.⁵⁴⁸ Michigan courts, which have

⁵⁴⁴ NEV. REV. STAT. § 603A.900 (2015) (stating that “[a] data collector that provides the notification required pursuant to NEV. REV. STAT. § 603A.220 may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector” and recover damages, reasonable costs of notification, reasonable attorney’s fees and costs, and punitive damages when appropriate”).

⁵⁴⁵ WIS. STAT. § 134.98(4) (2015).

⁵⁴⁶ *Opperman v. Path*, 87 F. Supp. 3d 1018, 1062 (N.D. Cal. 2014).

⁵⁴⁷ *Ruffin-Steinback v. De Passe*, 82 F. Supp. 2d 723, 734 (E.D. Mich. 2000) and *Rycroft v. Gaddy*, 281 S.C. 119, 124, 314 S.E.2d 39, 43 (1984).

⁵⁴⁸ Eric S. Pasternack, *HIPAA in the Age of Electronic Health Records*, 41 RUTGERS L.J. 817, 831 (2010) [hereinafter Pasternack] (citing Thomas J. Smedinghoff, *The Emerging Law of Data Security: A Focus on the Key Legal Trends*, 934 PRACTISING LAW INSTITUTE 13, 22 (2008)). See *Dwyer v. Am. Express Co.*, 273 Ill. App. 3d 742, 652 N.E.2d 1351 (Ind. App. Ct. 1995) (holding that based on the *Restatement (Second)* a credit card issuer’s compilation of a customer’s personal information and dissemination of customer lists to third parties was not a breach of privacy) and *Lewis v. LeGrow*, 258 Mich. App. 175, 188, 670 N.W.2d 675, 685 (Mich. Ct. App. 2003) (stating that “[t]he Legislature has not defined what constitutes an invasion of privacy, but when interpreted in light of the common-law right to privacy, it is clear that it includes keeping sexual relations private”).

“long recognized the common law tort of invasion of privacy,”⁵⁴⁹ have relied on William Prosser’s four bases on which a claim in tort may be made for an invasion of privacy: “(1) the intrusion upon another’s seclusion or solitude, or into another’s private affairs; (2) a public disclosure of private facts about the individual; (3) publicity that places someone in a false light in the public eye; and (4) the appropriation of another’s likeness for the defendant’s advantage.”⁵⁵⁰

Although New York⁵⁵¹ and Virginia⁵⁵² do not recognize a common law right to privacy, Arkansas, Alabama, California, Delaware, the District of Columbia, Indiana, Iowa, Michigan, Minnesota, Missouri, New Jersey, South Carolina, Texas, Vermont, and Washington are among the jurisdictions that do recognize a right to privacy at common law.⁵⁵³

⁵⁴⁹ *Dalley v. Dykema Gossett, PLLC*, 287 Mich. App. 296, 788 N.W.2d 679, 686 (Mich. Ct. App. 2010) (citing *Lewis v. LeGrow*, 258 Mich. App. 175, 670 N.W.2d 675 (2003)).

⁵⁵⁰ *Lewis v. LeGrow*, 258 Mich. App. 175 at 193, 670 N.W.2d at 687 (citing William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960)). See also *Ross v. Trumbull County*, 2001 Ohio App. LEXIS 495, at *1 (2001).

⁵⁵¹ See *Burck v. Mars, Inc.*, 571 F. Supp. 2d 446, 450 (S.D. N.Y. 2008). Although New York does not have a common law right to privacy, there is a statutory right to privacy against commercial appropriation. See also *Lohan v. Perez*, 924 F. Supp. 2d 447, 453 (E.D.N.Y. 2013); *Allison v. Clos-Ette Too*, 2014 U.S. Dist. LEXIS 143517, at *1 (S.D.N.Y. Sept. 15, 2014), *report and recommendation adopted sub nom.*, 2014 U.S. Dist. LEXIS 143066, at *1 (S.D.N.Y. Oct. 7, 2014); and *Hunt v. Conroy*, 2014 U.S. Dist. LEXIS 52305, at *1 (N.D.N.Y. Apr. 16, 2014).

⁵⁵² *Wiest v. E-Fense, Inc.*, 356 F. Supp. 2d 604, 612 (E.D. Va. 2005).

⁵⁵³ See *Phillips v. Smalley Maintenance Services, Inc.*, 711 F.2d 1524, 1533 (1983) (“Since 1948, beginning with the case of *Smith v. Doss*, 251 Ala. 250, 37 So. 2d 118 (1948), Alabama has recognized the tort of ‘invasion of the right to privacy.’”); *Milam v. Bank of Cabot*, 327 Ark. 256, 937 S.W.2d 653 (1997); *Metter v. Los Angeles Examiner*, 35 Cal. App. 2d 304, 95 P.2d 491 (1939); *Peay v. Curtis Publishing Co.*, 78 F. Supp. 305 (D.D.C. 1948); *State v. Holden*, 54 A.3d 1123 (Del. Super. Ct. 2010); *Davis v. General Finance & Thrift Corp.*, 80 Ga. App. 708, 57 S.E.2d 225 (1950); *Continental Optical Co. v. Reed*, 119 Ind. App. 643, 86 N.E.2d 306 (1949); *Bremmer v. Journal-Tribune Publishing Co.*, 247 Iowa 817, 76 N.W.2d 762 (1956); *Tate v. Woman’s Hops. Found.*, 56 So. 3d 194 (La. 2011); *Dalley v. Dykema Gossett, PLLC*, 287 Mich. App. 296, 788 N.W.2d 679, 686 (2010) (quoting *Lewis v. LeGrow*, 258 Mich. App. 175, 670 N.W.2d 675 (2003)); *Meyerkord v. Zipantoni Co.*, 276 S.W.3d 319 (Mo. App. 2008); *Frey v. Dixon*, 141 N.J. Eq. 481, 58 A.2d 86 (1948); *Holloman v. Life Ins. Co.*, 192 S.C. 454, 7 S.E.2d 169 (1940); *Russell v. American Real Estate Corp.*, 89 S.W.3d 204 (Tex. App., Corpus Christi 2002); *Pion v. Bean*, 2003 VT 79, 833 A.2d 1248 (2003); and *Mayer v. Huesner*, 126 Wash. App. 114, 107 P.3d 152 (2005).

B. Invasion of Privacy

There are four potential bases for a claim in tort for an invasion of privacy that may apply to an unauthorized use or disclosure of personal data: public disclosure of private facts, intrusion upon seclusion, misappropriation, and false light.⁵⁵⁴ Not all states that allow a claim for invasion of privacy recognize all four types of claims.

1. Public Disclosure of Private Facts

Although some states recognize “the tort of invasion of privacy based on [an] unreasonable public disclosure of private facts,”⁵⁵⁵ it appears that most jurisdictions require that a disclosure of personal information must have been made to the general public, “usually through the media.”⁵⁵⁶ For a claim to be actionable, the disclosure has to have revealed, for instance, “‘unpleasant or disgraceful or humiliating illnesses’ or ‘hidden physical or psychiatric problems.’”⁵⁵⁷

For example, in *Lake v. Wal-Mart Stores Inc.*,⁵⁵⁸ concerning the publication of nude photos by Wal-Mart employees, the court stated:

Lake and Weber allege in their complaint that a photograph of their nude bodies has been publicized. One’s naked body is a very private part of one’s person and generally known to others only by choice. This is a type of privacy interest worthy of protection. Therefore, without consideration of the merits of Lake and Weber’s claims, we recognize the torts of intrusion upon seclusion, appropriation, and publication of private facts. Accordingly, we reverse the court of appeals and the district court and hold that Lake and Weber have stated a claim upon which relief may be granted and their lawsuit may proceed.⁵⁵⁹

However, a tort action for public disclosure is unlikely to succeed if the injury from a disclosure is minimal.⁵⁶⁰

⁵⁵⁴ *Restatement (3d) of Torts*. See Martha Tucker Ayres, *Confidentiality and Disclosure of Health Information in Arkansas*, 64 ARK. L. REV. 969, 994 (2011) (footnote omitted) [hereinafter Ayres].

⁵⁵⁵ Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL’Y L. & ETHICS 325, 331 (2002) [hereinafter Pritts] (citing, e.g., *Ozer v. Borquez*, 940 P.2d 371, 377 (Colo. 1997) (stating that “[t]he requirement of public disclosure connotes publicity, which requires communication to the public in general or to a large number of persons, as distinguished from one individual or a few”) and *Lake v. Wal-Mart Stores Inc.*, 582 N.W.2d 231, 235 (Minn. 1998) (establishing the common law right to privacy in Minnesota, including the torts of “intrusion upon seclusion, appropriation, and publication of private facts”).

⁵⁵⁶ Ayres, *supra* note 554, at 995 (stating that a recovery in tort for an invasion of privacy is limited as the disclosure or communication must be “to the public at large”); see Pritts, *supra* note 555, at 331.

⁵⁵⁷ Pasternack, *supra* note 548, at 833 (footnote omitted).

⁵⁵⁸ 582 N.W.2d 231, 235 (Minn. 1998).

⁵⁵⁹ *Id.*

⁵⁶⁰ Pasternack, *supra* note 548, at 833 (footnote omitted).

2. Intrusion upon Seclusion

A second cause of action for an invasion of privacy for disclosing personal data is for intrusion upon seclusion. The tort of intrusion upon seclusion does not require a showing that a disclosure was made to the general public.⁵⁶¹ In an Arkansas case, the court observed that the tort of intrusion requires “specific intrusive action as opposed to disclosing private information.”⁵⁶² In California, there must be proof of an “intrusion into a private place, conversation or matter...in a manner highly offensive to a reasonable person.”⁵⁶³ In *Rhoades v. Penn-Harris-Madison School Corporation*,⁵⁶⁴ a federal court in Indiana held that an intrusion claim requires physical contact or an invasion of a plaintiff’s physical space.⁵⁶⁵

In *Watkins v. Cornell Companies, Inc.*, a case in which the plaintiffs sued for intrusion upon seclusion but knew they were being filmed, a federal court in Texas held that

[i]ntrusion on seclusion requires proof of (1) an intentional intrusion, physically or otherwise, upon another’s solitude, seclusion, or private affairs or concerns, which (2) would be highly offensive to a reasonable person. ...*Liability does not turn on publication of any kind*. The core of the tort of invasion of privacy is the offense of prying into the private domain of another, not the publicity that may result from such prying.⁵⁶⁶

There are various defenses to a claim for intrusion, including that the plaintiff did not intend to keep the information private; that under the circumstances the plaintiff did not have a reasonable expectation of privacy; or that the plaintiff voluntarily and without any coercion consented to the disclosure.⁵⁶⁷ Under Pennsylvania law, an intrusion claim cannot exist when “a defendant legitimately obtains information from a plaintiff.”⁵⁶⁸ In *Doe v. Di Genova*,⁵⁶⁹ a federal court in the District of Columbia held that there is no claim for

⁵⁶¹ See *Restatement (Second) § 652(B)*. See also Reid v. Pierce County, 136 Wash. 2d 195, 206, 961 P.2d 333, 339–340 (1998).

⁵⁶² *Dunbar v. Cox Health Alliance, LLC*, 446 B.R. 306, 313–314, 2011 Bankr. LEXIS 812 (E.D. Ark. 2011).

⁵⁶³ *Grant v. United States*, 2011 U.S. Dist. LEXIS 61833, at *1, 20 (E.D. Cal. 2011) (citing CAL. CIV. CODE § 47(b)), adopted by, claim dismissed, 2011 U.S. Dist. LEXIS 78119, at *1 (E.D. Cal. 2011).

⁵⁶⁴ 574 F. Supp. 2d 888 (N.D. Ind. 2008).

⁵⁶⁵ *Id.* at 907–908 N 3.

⁵⁶⁶ 2013 U.S. Dist. LEXIS 66376, at *1, 21–22 (N.D. Tex. 2013) (citations omitted) (internal quotation marks omitted) (emphasis added).

⁵⁶⁷ Ayres, *supra* note 554, at 995 (footnotes omitted)

⁵⁶⁸ *Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331, 342–343 (E.D. Pa. 2012).

⁵⁶⁹ *Doe v. Di Genova*, 642 F. Supp. 624, 632 (D. D.C. 1986) (holding that under the Privacy Act, Doe was entitled to an order prohibiting the release of records).

intrusion when an intrusion is reasonable under the circumstances or when an intrusion is not “serious.”

One issue for an intrusion claim is whether a disclosure is sufficiently offensive. In *Cooney v. Chicago Public Schools*,⁵⁷⁰ involving a firm’s disclosure of personal information on former Chicago public school employees, the court, in ruling that there were no actionable claims, drew a distinction between personal information and private information. Names and Social Security numbers are personal information, but the court held that their disclosure was not “facially embarrassing and highly offensive....”⁵⁷¹

One case was located for the digest in which the court held that the complaint stated a claim against the Secretary of the North Carolina DOT for intrusion into seclusion. North Carolina recognizes the tort of intrusion into seclusion. In *Toomer v. Garrett*,⁵⁷² the plaintiff alleged that the secretary disclosed and distributed the contents of Toomer’s personnel file to the media, thus violating the plaintiff’s right to privacy.⁵⁷³ Although the state, its agencies, and officials who are sued in their official capacities usually are immune from claims under North Carolina law, the court held that the action was allowable because of the plaintiff’s allegations of malice and bad faith on the part of the DOT officials.⁵⁷⁴ Therefore, the defendants were not “entitled to dismissal of plaintiff’s claims for tortious invasion of privacy on the basis of official capacity immunity.”⁵⁷⁵

In *Behar v. Pennsylvania Department of Transportation*,⁵⁷⁶ the court held that the transportation department’s interest in public safety outweighed the plaintiff’s interest in the privacy of the plaintiff’s medical information. The plaintiff challenged a Pennsylvania Department of Transportation

⁵⁷⁰ *Cooney v. Chicago Public Schools*, 407 Ill. App. 3d 358, 943 N.E.2d 23 (2010).

⁵⁷¹ *Id.* at 367, 943 N.E.2d at 32.

⁵⁷² 155 N.C. App. 462, 574 S.E.2d 76 (N.C. App. 2002).

⁵⁷³ *Id.* at 466–467, 574 S.E.2d at 82.

⁵⁷⁴ *Id.* at 480–481, 574 S.E.2d at 91.

⁵⁷⁵ *Id.* at 481, 573 S.E.2d at 91. The court also held that the plaintiff’s complaint was sufficient to state (1) § 1983 claims for federal substantive due process and equal protection violations for injunctive relief against individual defendants in their official capacities and for damages in their individual capacities; (2) state substantive due process and equal protection claims for injunctive relief against individual defendants in their official capacities; (3) a breach of contract claim against the State, NCDOT, and individual defendants in their official and individual capacities; and (4) ...invasion of privacy, gross negligence, and civil conspiracy against individual defendants in their individual capacities.

Id. at 484, 574 S.E.2d at 93.

⁵⁷⁶ 791 F. Supp. 2d 383 (M.D. Pa. 2011).

(PennDOT) regulation that required health care professionals to inform PennDOT of every patient older than 15 who had certain designated medical conditions that could affect a patient’s ability to drive a vehicle.⁵⁷⁷ The plaintiff argued that the regulation violated privacy rights and would cause individuals to avoid seeking medical care to assure that they would not lose their driving privilege.⁵⁷⁸ In Pennsylvania, although patients have a right to privacy in their medical information, the courts use a seven-factor test to balance the individual’s interests against the state’s interests in public health and safety.⁵⁷⁹ The court held that “the privacy interests of [the plaintiff’s] patients are outweighed by the state’s compelling interest,” because the “operation of vehicles on Pennsylvania roadways compels a broader consideration of issues than those asserted by” the plaintiff.⁵⁸⁰ The court also held, *inter alia*, that the plaintiff lacked standing.⁵⁸¹

3. Claims for Appropriation or False Light

Because they are mentioned in the *Restatement*, privacy claims based on misappropriation or false light will be noted briefly. For a plaintiff to make a claim for misappropriation or for false light, a plaintiff’s information must have been revealed to the public by the media, the same element that is usually required for a claim for a public disclosure of private facts.⁵⁸²

C. Applicability of a Common Law Right of Privacy to Transportation Agencies

In the absence of constitutional or statutory remedies, tort law must be used to remediate a violation of a claimed right to privacy.⁵⁸³ One commentator argues that there are several problems in respect to the use of the common law of torts for a privacy violation arising out of a disclosure of data collected by ITS and other technology.⁵⁸⁴

First, it is difficult to predict how the courts would apply the principles previously discussed because “there is no reported court decision regarding tort liability for invasion of privacy in a context similar to ITS.”⁵⁸⁵ Second, for there to be a claim, the

⁵⁷⁷ *Id.* at 388. See also 67 PA. CONS. CODE § 85.6 (2015).

⁵⁷⁸ *Behar*, 791 F. Supp. 2d at 397.

⁵⁷⁹ *Id.* at 398.

⁵⁸⁰ *Id.*

⁵⁸¹ *Id.* at 390–400.

⁵⁸² Ayres, *supra* note 554, at 998, 1000 (footnote omitted).

⁵⁸³ Douma and Deckenbach, *supra* note 2, at 295.

⁵⁸⁴ Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 151, 179 (1995) [hereinafter Dorothy Glancy].

⁵⁸⁵ *Id.*

defendant's conduct would have to have been intentional as mere negligence ordinarily will not suffice.⁵⁸⁶ Third, the law in some states demands that a violation of privacy must have been the result of "willful or outrageous" conduct, something that the writer argues is unlikely with regard to "routine" ITS operations.⁵⁸⁷ Finally, the commentator posits that some state or local government agencies are protected by sovereign immunity from common law privacy claims.⁵⁸⁸

In sum, the common law has not recognized a cause of action for a violation of privacy resulting from a disclosure of data collected on individuals when they are "on the public streets."⁵⁸⁹ An intentional disclosure of secure data may state a claim in those states recognizing the common law tort of intrusion into seclusion. There is authority, however, that the disclosure of personal information, such as Social Security numbers and similar PII considered to be secure data, does not state a claim because the data are not embarrassing or highly offensive.

IX. WHETHER TRANSPORTATION AGENCIES ARE POTENTIALLY LIABLE FOR A DISCLOSURE OF DATA

A. Whether a Claim for a Release of Data Is Barred by Sovereign Immunity or a State Tort Claims Act

Many states' tort claims or governmental immunity acts retain sovereign immunity except for certain designated claims or government functions. The survey asked transportation agencies whether they have immunity under state law from claims for a negligent or intentional disclosure of data. Seven transportation agencies reported that they have immunity from such claims,⁵⁹⁰ whereas eight agencies stated that they would not have immunity.⁵⁹¹

The liability of a public entity in tort varies from state to state depending on the extent to which the

state legislature has waived immunity, as well as on the courts' interpretation of the applicable legislation.⁵⁹² It is important to note that in states where a tort claims act permits a plaintiff to sue a public entity in tort, the legislation may have specific exceptions, exemptions, or exclusions to liability. In its response to the survey, the Florida DOT cited its state's statute on sovereign immunity in which the State of Florida for itself and its agencies and subdivisions "waives sovereign immunity for liability for torts, *but only to the extent specified in this act.*"⁵⁹³ The Illinois Local Governmental and Governmental Employees Immunity Act has "an extensive list of immunities based on specific governmental functions."⁵⁹⁴ As observed by the North Carolina court in *Turner v. N.C. DOT*,⁵⁹⁵ the DOT may be sued for negligence only as provided in the tort claims act. Because tort claims acts and similar legislation affecting governmental immunity are in derogation of the common law, the courts typically strictly construe the legislation.⁵⁹⁶

A defense for discretionary decisions made by public entities is one recognized under some states' common law and/or is a defense that has been codified in state tort claims legislation. In the *Toomer* case, the plaintiff's complaint did not allege a waiver by North Carolina of its sovereign immunity that "shields the

⁵⁹² See LARRY W. THOMAS, *Tort Liability of Highway Agencies*, in *SELECTED STUDIES IN TRANSPORTATION LAW*, Vol. 4 (Transportation Research Board of the National Academies of Science, Engineering, and Medicine, Washington D.C., 2003).

⁵⁹³ FLA. STAT. § 768.28(1) (2015) (emphasis added). Although the applicable Florida Statute must be consulted in its entirety, FLA. STAT. § 768.28(1) further provides that

[a]ctions at law against the state or any of its agencies or subdivisions to recover damages in tort for money damages against the state or its agencies or subdivisions for injury or loss of property, personal injury, or death caused by the negligent or wrongful act or omission of any employee of the agency or subdivision while acting within the scope of the employee's office or employment under circumstances in which the state or such agency or subdivision, if a private person, would be liable to the claimant.

⁵⁹⁴ *Sexton v. City of Chicago*, 976 N.E.2d 526, 540 (Ill. App. 2012) (some internal quotation marks omitted).

⁵⁹⁵ 733 S.E.2d 871, 874 (N.C. Ct. App. 2012) (holding that the DOT owed no duty to the decedents for failing to install warning signs on a road as there was no violation of the Manual on Uniform Traffic Control Devices and the DOT had no knowledge of an unsafe road condition).

⁵⁹⁶ *Nawrocki v. Macomb County Road Commission*, 463 Mich. 143, 151, 615 N.W.2d 702, 707 (Mich. 2000) (Supreme Court of Michigan holding that "prior decisions of this Court...improperly broadened the scope of the highway exception" to governmental immunity and holding that the court was "duty bound to overrule past decisions that depart from a narrow construction and application of the highway exception....").

⁵⁸⁶ *Id.*

⁵⁸⁷ *Id.* at 180.

⁵⁸⁸ *Id.*

⁵⁸⁹ Garry, Douma, and Simon, *supra* note 2, at 104 (citing Kendra Roseberg, *Location Surveillance by GPS: Balancing an Employer's Business Interest with Employee Privacy*, 6 WASH. J.L. TECH. & ARTS 143, 150–154 (2010)).

⁵⁹⁰ Alabama DOT (citing ALABAMA CONST. (1901), Art. I, § 14); Arkansas DOT, Florida DOT, Indiana DOT (citing IND. CODE § 34-13-3), MoDOT, Oregon DOT, and Rhode Island DOT. The Montana DOT's response was "none known." The Maine DOT and Ohio DOT did not respond to the question.

⁵⁹¹ Arizona DOT, District of Columbia DOT, City of Minneapolis–Public Works Dept., North Dakota DOT, Oklahoma DOT, South Carolina DOT, and Utah DOT. The Maine DOT and Ohio DOT did not respond to the question.

State, its agencies, and officials sued in their official capacities....”⁵⁹⁷ Moreover, the court stated that

[t]he essence of the doctrine of *public official immunity* is that public officials engaged in the performance of their governmental duties involving the exercise of judgment and discretion, and acting within the scope of their authority, may not be held liable for such actions, *in the absence of malice or corruption*.⁵⁹⁸

Most states have a tort claims act or similar legislation with a provision that immunizes a state agency for its exercise or performance of discretionary functions; the exemption usually is identical or similar to the one in the Federal Tort Claims Act (FTCA). The FTCA grants jurisdiction to federal district courts of

civil actions on claims against the United States, for money damages...for injury or loss of property, or personal injury or death caused by the *negligent or wrongful act or omission* of any employee of the Government while acting within the scope of his office or employment, under circumstances where the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred.⁵⁹⁹

However, the FTCA does not allow a civil action against the United States for:

Any claim based upon an act or omission of an employee of the Government, exercising due care, in the execution of a statute or regulation, whether or not such statute or regulation be valid, or based upon *the exercise or performance or the failure to exercise or perform a discretionary function or duty* on the part of a federal agency or an employee of the Government, whether or not the discretion involved be abused.⁶⁰⁰

The courts generally have held that a government decision or function is discretionary in nature when the decisionmaking at issue occurred at the planning-level and/or the decisionmaking involved the consideration or evaluation of broad policy factors.⁶⁰¹

⁵⁹⁷ *Toomer*, 155 N.C. App. at 480, 574 S.E.2d at 91.

⁵⁹⁸ *Id.* at 481, 574 S.E.2d at 91 (emphasis added).

⁵⁹⁹ 28 U.S.C. § 1346(b)(1) (2015) (emphasis added).

⁶⁰⁰ 28 U.S.C. § 2860(a) (2015) (emphasis added). *See, e.g.*, CAL. GOV'T CODE § 820.2 (2015) (concerning discretionary acts); IND. CODE § 34-14-3-3(7) (2015); IOWA CODE § 669.14(1) (2015); KAN. STAT. ANN. § 75-6104(e) (2015); NEB. REV. STAT § 81-8,219(1) and ch. 41 (2015); OHIO REV. CODE § 2743.02 (2015); OK. STAT. § 155(5) (2015); TEXAS CIV. PRAC. & REM. CODE § 101.056 (2015); UTAH CODE § 63G-7-301(5)(a) (2015); VA. CODE § 33.1-70.1 (2015); and WIS. STAT. §§ 893.80 and 893.82 (2015).

⁶⁰¹ *Miotke v. Spokane*, 101 Wash. 2d 307, 334, 678 P.2d 803, 819 (1984) (stating that in *Evangelical United Brethren Church v. State*, 67 Wash. 2d 246, 407 P.2d 440 (1965), the court created a narrow exception to governmental immunity from tort liability in instances in which public officials engage in discretionary acts based on a four-part inquiry). *See Weiss v. Fote*, 7 N.Y.2d 579, 167 N.E.2d 63, 200 N.Y.S.2d 409 (1960).

Whether a governmental decision is discretionary and entitled to immunity is a question of law decided by the court.⁶⁰²

In *Axtell v. University of Texas*,⁶⁰³ a Texas appellate court held that the disclosure by a state agency of confidential information was not actionable because the state had retained its immunity under the state tort claims act. In *Axtell*, a student sued a state university and its employees for sending the student's educational records by a telefax machine to a local radio station without the student's consent.⁶⁰⁴ The trial court dismissed the action because of the university's immunity as a state institution. The plaintiff argued on appeal that the university lacked immunity because the Texas Tort Claims Act “provides a limited waiver of sovereign immunity when [a] personal injury is ‘caused by a condition or use of tangible personal or real property if the governmental unit would, were it a private person, be liable to the claimant according to Texas law.’”⁶⁰⁵ *Axtell* argued that the tangible personal property, i.e., the telefax machine, used to disclose his confidential information was the cause of his injuries.⁶⁰⁶

The court held, however, that the university employees' negligence was not their use of a telefax machine, but their release of the plaintiff's information by whatever means.⁶⁰⁷ Thus, the Texas Tort Claims Act's limited waiver of immunity that applies to the use of tangible personal or real property did not apply to the disclosure of the plaintiff's information.⁶⁰⁸ Because immunity for the release of personal information had not been waived, the court affirmed the trial court's dismissal of the plaintiff's action.⁶⁰⁹

In *Tivnan v. Registrar of Motor Vehicles*,⁶¹⁰ the plaintiff sued employees of the Registry of Motor Vehicles for issuing a duplicate driver's license in his name to another individual in violation of the Annotated Laws of Massachusetts Law Chapter 66A.⁶¹¹ The imposter ruined the plaintiff's credit and amassed over \$150,000 in debt in the name of the plaintiff.⁶¹² The court held that the privacy issue was governed by the Massachusetts Tort Claims Act

⁶⁰² *Truman v. Griese*, 2009 S.D. 8, 33, 762 N.W.2d 75, 85 (2009).

⁶⁰³ 69 S.W.3d 261 (Tex. App. 2002).

⁶⁰⁴ *Id.* at 263.

⁶⁰⁵ *Id.* at 264 (quoting TEX. CIV. PRAC. & REM. CODE ANN. § 101.021(2) (1997)).

⁶⁰⁶ *Id.*

⁶⁰⁷ *Id.* at 266.

⁶⁰⁸ *Id.*

⁶⁰⁹ *Id.* at 267.

⁶¹⁰ 50 Mass. App. Ct. 96, 734 N.E.2d 1182 (2000).

⁶¹¹ *Id.* at 96–97, 734 N.E.2d at 1183.

⁶¹² *Id.* at 97, 734 N.E.2d at 1183.

(MTCA).⁶¹³ The MTCA superseded the Annotated Laws of Massachusetts Chapter 214, Section 3B, which provided that “parties injured by the violation of G. L. c. 66A [may] claim damages for injury against public employers....”⁶¹⁴ The case was dismissed because under the MTCA, “the issuance of a license [is] specifically immunized” under Section 10(e).⁶¹⁵

On the other hand, in *Torres v. Attorney General*,⁶¹⁶ the plaintiff alleged that the Department of Social Services violated the General Laws of Massachusetts Chapter 66A when the department released information to the Assistant Attorney General containing the plaintiff’s geographic location.⁶¹⁷ The Supreme Judicial Court of Massachusetts held that the release was a violation of Massachusetts law. First, the plaintiff did not consent to the access to his personal data, and, second, there was “no legislative intent to grant the office of the Attorney General access to personal data held by one State agency simply because a data subject has brought a suit against one or more other State agencies.”⁶¹⁸ The case was remanded to the Superior Court for an assessment of damages, attorney’s fees, and costs.⁶¹⁹

In sum, unless a state law provides for a cause of action against state agencies for a disclosure of secure data or monitoring data, a transportation agency may have immunity on one of several bases: The agency’s sovereign immunity may not have been waived; a state tort claims or the equivalent may waive immunity only for specific transportation or highway functions; a tort claims act may exclude or exempt certain transportation or highway functions from liability; or the transportation agency may have immunity for the performance of its functions that involve the exercise of discretion. However, some states’ privacy law provides a private right of action for a violation of the statute that is an exception to a transportation agency’s sovereign immunity or that is an exception to immunity that otherwise exists under the state’s tort claims act or equivalent.

⁶¹³ MASS. ANN. LAWS ch. 258.

⁶¹⁴ *Tivnan*, 50 Mass. App. Ct. at 97, 734 N.E.2d at 1183 (citing MASS. ANN. LAWS, ch. 214, § 3B and MASS. GEN. LAWS, ch. 66A).

⁶¹⁵ *Id.* at 102, 734 N.E.2d at 1186 (citing MASS. ANN. LAWS, ch. 258, § 10(e)). The plaintiff also failed to make a proper presentment as required under § 4 of the MTCA. *Id.* at 103, 734 N.E.2d at 1187 (citing MASS. ANN. LAWS, ch. 258, § 4).

⁶¹⁶ 391 Mass. 1, 460 N.E.2d 1032 (1984).

⁶¹⁷ *Id.* at 2–3, 460 N.E.2d at 1033.

⁶¹⁸ *Id.* at 11–12, 460 N.E.2d at 1038–1039.

⁶¹⁹ *Id.* at 16, 460 N.E.2d at 1041.

B. Claims Against Transportation Agencies Arising Out of the Disclosure of Secure Data or Monitoring Data

1. Disclosure of Secure Data

Nine transportation agencies reported that there are laws in their state that provide an individual with a cause of action against the agency for the disclosure of secure data.⁶²⁰ (Seven agencies stated that there are no such laws in their state.)⁶²¹ The statutes the agencies cited range from allowing a plaintiff to recover actual damages to a more limited recovery of damages. Some of the cited statutes impose criminal liability for a violation rather than allow for a recovery of damages.

The Oregon DOT identified Oregon Revised Statutes (ORS) Section 802.191(1), which permits a recovery of actual damages:

A person aggrieved by an intentional violation of ORS 802.175 (Definitions for ORS 802.175 to 802.191) to 802.187 (Relationship to other privacy statutes) may bring an action at law against a person who has knowingly obtained or used personal information about the aggrieved person in violation of ORS 802.175 (Definitions for ORS 802.175 to 802.191) to 802.187 (Relationship to other privacy statutes). The action shall be for *actual damages or \$2,500, whichever is greater*, plus attorney fees and court costs reasonably incurred in the action.⁶²²

The City of Minneapolis–Public Works Department cited the Minnesota Government Data Practices Act (MGDPA) as governing authority. Section 13.05, subdivision 3 of the MGDPA states that in respect to the duties of a responsible authority the

[c]ollection and storage of all data on individuals and the use and dissemination of private and confidential data on individuals shall be limited to that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government.⁶²³

The MGDPA includes limitations on the collection and use of data: “Private or confidential data on an individual shall not be collected, stored, used, or

⁶²⁰ Alabama DOT (reporting that tort claims could be brought against individual officials), Arkansas DOT, Arizona DOT, District of Columbia DOT (reporting that the District of Columbia Municipal Regulations (DCMR) in 1 DCMR § 1500 provide “in part that individuals that misuse or destroy public records are subject to penalty”), Florida DOT, North Dakota DOT, Oregon DOT, South Carolina DOT, and Utah DOT (providing a copy of its requirements for the handling of Bluetooth data).

⁶²¹ Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, Oklahoma DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT.

⁶²² OR. REV. STAT. § 802.191(1) (2015) (emphasis added).

⁶²³ MINN. STAT. § 13.025, subdiv. 3 (2015).

disseminated by government entities for any purposes other than those stated to the individual at the time of collection in accordance with section 13.04, except as provided in this subdivision.”⁶²⁴

Section 13.04, subdivision 1 of the MGDPA provides that “[t]he rights of individuals *on whom the data is stored or to be stored* shall be as set forth in this section.”⁶²⁵

Damages are recoverable for a violation of the MGDPA as provided in Section 13.08, subdivision 1:

Notwithstanding section 466.03, a responsible authority or government entity which violates any provision of this chapter is liable to a person or representative of a decedent who suffers any damage as a result of the violation, and the person damaged or a representative in the case of private data on decedents or confidential data on decedents may bring an action against the responsible authority or government entity to cover any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, the government entity shall, in addition, be liable to exemplary damages of not less than \$1,000, nor more than \$15,000 for each violation. The state is deemed to have waived any immunity to a cause of action brought under this chapter.⁶²⁶

Unless a state privacy law provides otherwise, it appears that a transportation department would be held liable in some states only for an *intentional* disclosure, but not for an unintentional disclosure, of secure data. One source states that “tort liability for invasion of privacy requires *intentional conduct* on the part of the defendant. A few states expressly disapprove [of] negligence as a basis for privacy tort liability.”⁶²⁷ As noted, the federal Privacy Act applies only to intentional or willful disclosures. On the other hand, in some states a public authority may be held liable for the unintentional disclosure of secure data. Under Minnesota’s MGDPA, actual damages are recoverable for a disclosure of private or confidential data, and exemplary damages as provided in the statute when there is a willful breach of the MGDPA.⁶²⁸

Moreover, in the event of an unintentional release of secure data there may be a good faith defense that also may be codified in some state statutes. For example, Iowa Code Section 22.10(3) does not permit an award of damages against an agency when the agency shows that it made reasonable efforts to prevent disclosure or “had good reason to believe

and in good faith believed” that it was complying with the statute.⁶²⁹

Other statutory provisions cited by the transportation agencies authorize the recovery of attorney’s fees under the state’s FOIA or provided that a violation of the FOIA constituted a misdemeanor. For example, the Arkansas FOIA permits an “action to enforce the rights granted by this chapter” and further allows for the recovery of “reasonable attorney fees and other litigation expenses reasonably incurred by a plaintiff who has substantially prevailed unless the court finds that the position of the defendant was substantially justified or that other circumstances make an award of these expenses unjust....”⁶³⁰ In its response, the department referred to another provision in the state’s FOIA that states that “[a]ny person who negligently violates any of the provisions of this chapter shall be guilty of a Class C misdemeanor.”⁶³¹

The Arizona DOT referred to a provision of its laws on motor vehicle records providing that “[a] person who violates this section is guilty of a class 1 misdemeanor.”⁶³²

The South Carolina DOT cited Title 39 of the South Carolina Code. Section 39-1-90(A) requires that a person conducting business in the state and owning or licensing a data system that includes PII must disclose a data breach to state residents.⁶³³ The notification statute appears to apply only to persons and organizations conducting business in the state.⁶³⁴

No transportation agency responding to the survey reported having had a claim in the past 5 years for an unintentional disclosure of secure data.⁶³⁵ Nevertheless, some cases were located for the digest involving claims against state agencies for disclosing secure data such as PII.

As seen in *Kiminski*, the court dismissed a § 1983 action against a state agency’s officials and employees because of a former employee’s accessing of the plaintiffs’ motor vehicle data, because there was no constitutional right to privacy in the information

⁶²⁹ IOWA CODE § 22.10(3)(b)(2) (2015).

⁶³⁰ ARKANSAS CODE ANN. § 25-19-107(d) (2015).

⁶³¹ ARKANSAS CODE ANN. §§ 25-19-104 (2015).

⁶³² ARIZ. REV. STAT. § 28-457 (2015).

⁶³³ S.C. CODE § 39-1-90(A) (2015).

⁶³⁴ See S.C. CODE § 39-1-90(D)(2) (2015) that refers to § 37-20-110(10) (defining a person to mean a natural person, an individual, or an organization as defined in § 37-1-301(20)).

⁶³⁵ Alabama DOT, Arkansas DOT, Arizona DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Maine DOT, Montana DOT, and Ohio DOT did not respond to the question.

⁶²⁴ MINN. STAT. § 13.025, subdiv. 4 (2015).

⁶²⁵ MINN. STAT. § 13.04, subdiv. 1 (2015) (emphasis added).

⁶²⁶ MINN. STAT. § 13.08, subdiv. 1 (2015) (emphasis added).

⁶²⁷ Dorothy Glancy, *supra* note 584, at 179–80 (emphasis added).

⁶²⁸ MINN. STAT. § 13.08, subdiv. 1 (2015).

even though the data were protected by the DPPA.⁶³⁶ As discussed previously, in that court the plaintiff's only remedy was a statutory claim under the DPPA.

In *Collier*, the disclosure of the plaintiff's personal information protected by the DPPA did not state a cause of action for a constitutional violation of privacy under § 1983, but did state a cause of action under § 1983 for a clear violation of the statutory duty imposed by the federal DPPA.⁶³⁷

In *Toomer*, under the circumstances of that case the arbitrary disclosure by the DOT Secretary of a former employee's personnel file that contained PII was held to state a § 1983 claim. The reason was that the secretary's intentional, malicious action was a violation of the Fourth Amendment, an action that also stated a claim under North Carolina's common law right to privacy against government intrusion into seclusion.⁶³⁸

In *Behar*, the court upheld a PennDOT regulation that allegedly violated the plaintiff's right to privacy because of the necessity of balancing the individual's privacy interest in medical matters against Pennsylvania's interest in public safety on its roadways.⁶³⁹

Other cases located for the digest include *Bates v. Franchise Tax Bd.*,⁶⁴⁰ in which the plaintiffs sued two state agencies and individuals who worked in those agencies under California's IPA.⁶⁴¹ The IPA imposes "limitations on the right of governmental agencies to disclose *personal* information about an individual."⁶⁴² Although public entities in California are immune from suit in the absence of a constitutional or statutory provision that "declares them to be liable,"⁶⁴³ Section 1798.45 of the IPA provides for a private right of action against a state agency that violates the IPA.⁶⁴⁴ In the event of a violation of Sections 1798.48(b) or (c), an agency may be held liable to a plaintiff for actual damages, including damages for mental suffering and attorney's fees.⁶⁴⁵

However, in *Bates* the court held that because the IPA does not have a claims procedure functionally

equivalent to California's Government Claims Act, the plaintiffs could not avoid the requirement to file their claim for damages under the Government Claims Act. The court held that IPA Sections 1798.5 and 1798.48 "constitute[] a statutory expression of governmental liability for damages, which, under Government Code section 815, controls over the immunity provided in Government Code section 860.2."⁶⁴⁶ Although the court held that the plaintiffs had an otherwise viable claim under the IPA, the plaintiffs failed to comply with the Government Claims Act,⁶⁴⁷ "a prerequisite to a damages action against the State."⁶⁴⁸

A New York decision involved Section 202(4)(a) of the New York Vehicle and Traffic Law pursuant to which the commissioner has the "discretion to contract with the highest responsible bidder or bidders to furnish" certain registration information for the period specified in the statute.⁶⁴⁹ Subsection (4)(b) required the commissioner to "notify each vehicle registrant that the registration information specified in paragraph (a) of this subdivision has been or will be furnished to the contracting party."⁶⁵⁰ In *Lamont v. Commissioner*,⁶⁵¹ decided prior to the Congress's enactment of the DPPA, a federal court in New York held that the state's sale of vehicle registration lists to a contractor who used the information to compile directories was not an invasion of privacy because the information was not "vital or intimate."⁶⁵² According to the court, as of the date of the *Lamont* case, 18 other states had similar statutes.⁶⁵³

In sum, it appears that in some states a claim is possible under state law against a transportation agency for a disclosure of secure data such as PII. Moreover, unless a state privacy statute applies both to intentional and unintentional disclosures of secure data, a plaintiff may have to show that an agency's violation was intentional. Unless a privacy statute authorizes the recovery of specified or liquidated damages or provides for a civil penalty for a violation, a plaintiff would have to prove actual damages.

2. Disclosure of Monitoring Data

Six agencies reported that there are laws in their state that provide an individual with a cause of action for the intentional disclosure of monitoring

⁶³⁶ *Kiminski*, 2013 U.S. Dist. LEXIS 157829, at *25 (citation omitted).

⁶³⁷ *Collier*, 477 F.3d at 1308–1309.

⁶³⁸ *Toomer*, 155 N.C. App. at 470, 481, 574 S.E.2d at 84, 91.

⁶³⁹ *Behar*, 791 F. Supp. 2d at 398, 390–400.

⁶⁴⁰ 124 Cal. App. 4th 367, 21 Cal. Rptr. 3d 285 (2004).

⁶⁴¹ *Id.* at 373, 21 Cal. Rptr. 3d at 288.

⁶⁴² *Id.* at 376, 21 Cal. Rptr. 3d at 290 (emphasis added).

⁶⁴³ *Id.* at 381, 21 Cal. Rptr. 3d at 294 (citing CAL. GOV'T CODE § 815(a) (internal quotation marks omitted)).

⁶⁴⁴ *Id.* at 381–382, 21 Cal. Rptr. 3d at 294–295 (quoting CAL. CIV. CODE § 1798.45).

⁶⁴⁵ *Id.* at 382, 21 Cal. Rptr. 3d at 295 (quoting CAL. CIV. CODE § 1798.48).

⁶⁴⁶ *Id.*

⁶⁴⁷ CAL. GOV'T CODE § 905.2.

⁶⁴⁸ *Bates*, 124 Cal. App. 4th at 382, 21 Cal. Rptr. 3d at 295.

⁶⁴⁹ N.Y. VEH. & TRAF. LAW § 202(4)(a)).

⁶⁵⁰ N.Y. VEH. & TRAF. LAW § 202(4)(b)).

⁶⁵¹ 269 F. Supp. 880 (S.D.N.Y. 1967).

⁶⁵² *Id.* at 883.

⁶⁵³ *Id.* (citations omitted).

data.⁶⁵⁴ Nine agencies reported that there are no such laws in their state regarding the intentional disclosure of monitoring data.⁶⁵⁵

As for specific information, the Arkansas DOT cited Arkansas Code Annotated Section 12-12-1807 that pertains to the use of ALPRs in Arkansas:

(a) A person who violates this subchapter shall be subject to legal action for damages to be brought by any other person claiming that a violation of this subchapter has injured his or her business, person, or reputation.

(b) A person so injured shall be entitled to actual damages or liquidated damages of one thousand dollars (\$1,000), whichever is greater, and other costs of litigation.

No cases were located for the digest, and the transportation agencies did not report any claims involving an agency's intentional release of monitoring data.⁶⁵⁶ No statutes were located for the digest that provide a cause of action specifically for the disclosure of monitoring data of the type collected by ITS. Finally, it appears that the approach in some states is to deal with monitoring data on an issue by issue basis by limiting or prohibiting the use of certain technology or by limiting or prohibiting the use of certain secure or monitoring data.

C. Liability of Contractors for Data Disclosure

Nine transportation agencies reported that they have contracts with persons or private entities to collect and/or maintain secure data or monitoring data.⁶⁵⁷ Copies of or links to agreements furnished by the agencies are included in Appendix C. As commentators have observed, "federal and state agencies have increasingly relied on outsourcing the gathering and managing of information to private

⁶⁵⁴ Arkansas DOT, District of Columbia DOT (reporting that "1 DCMR §1500 states in part that individuals that misuse or destroy public records are subject to penalty"), Florida DOT, City of Minneapolis–Public Works Dept. (*citing* Minnesota Government Data Practices Act, MINN. STAT. § 13.01, *et seq.*), South Carolina DOT (citing notification of data breach law, S.C. CODE § 39-1-90), and Utah DOT. The Florida DOT referred to the waiver of immunity, FLA. STAT. § 768.28(1).

⁶⁵⁵ Alabama DOT, Arizona DOT, Indiana DOT, MoDOT, Montana DOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, and Utah DOT.

⁶⁵⁶ Alabama DOT, Arkansas DOT, Arizona DOT, District of Columbia DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Maine DOT, Montana DOT, and Ohio DOT did not respond to the question.

⁶⁵⁷ Arizona DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oregon DOT, Rhode Island DOT, and Utah DOT. The Maine DOT, Montana DOT, and Ohio DOT did not respond to the question.

companies because they do not face the same liabilities and limitations placed [on] government agencies."⁶⁵⁸ For example, the California Public Contract Code prohibits release of proprietary information by a party contracting with a state agency.⁶⁵⁹

Although there are fewer restraints on and/or judicial scrutiny of data collected or maintained by private contractors,⁶⁶⁰ the Intelligent Transportation Society of America has issued nonbinding guidelines for its members in "an effort to self-regulate on the issue of data security and privacy protection."⁶⁶¹

D. Causes of Action Alleged Against Private Companies for Privacy Violations

A review of some complaints against private companies for a data breach illustrates the causes of action that plaintiffs are alleging.

For example, in *Antman v. Uber Technologies, Inc.*,⁶⁶² filed March 12, 2015, in the Northern District of California (San Francisco Division), the plaintiff brought a class action alleging that the defendant failed to "secure and safeguard" Uber's drivers' PII that was stolen in 2014. The complaint included one count for a violation of California's IPA Sections 1798.81.5 and 1798.82⁶⁶³ and another count for a violation of California's Unfair Competition Law.⁶⁶⁴

In *Webb v. Premera Blue Cross*,⁶⁶⁵ filed April 6, 2015, in the Western District of Washington, also a class action, the plaintiffs alleged that PII, financial information, and medical records "were compromised" because of a data breach that occurred at Premera Blue Cross in approximately May 2014.⁶⁶⁶ The plaintiff alleged that the data breach involved the theft of names, addresses, birth dates, Social Security numbers, credit card information, and private medical data.⁶⁶⁷ The plaintiff alleged, *inter alia*,

⁶⁵⁸ Douma and Deckenbach, *supra* note 2, at 312 (footnote omitted). *See also* Froomkin, *supra* note 213, at 1022, 1024 (citing Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.–C. L. REV. 435, 439 (2008)).

⁶⁵⁹ CAL. PUB. CODE § 10426(c) (2015).

⁶⁶⁰ Douma and Deckenbach, *supra* note 2, at 322.

⁶⁶¹ Phillips and Kohm, *supra* note 1, at P21 (*citing ITS America's Fair Information and Privacy Principles 1*, ITS America, available at <http://www.itsa.org/images/media-center/itsaprivacyprinciples.pdf> (last accessed Oct. 12, 2015)).

⁶⁶² Case No. 3:15-CV-01175, 2015 U.S. Dist. LEXIS 141945 (N.D. Calif. 2015) [hereinafter *Antman Compl.*].

⁶⁶³ *Id.* at 3.

⁶⁶⁴ *Id.* at 12 and 14 (citing CAL. BUS. & PROF. CODE § 17200, *et seq.*).

⁶⁶⁵ Case No. 2:2015-cv-00539 (W.D. Wash. 2015) [hereinafter *Webb Compl.*].

⁶⁶⁶ *Id.* at 1.

⁶⁶⁷ *Id.* at 2.

that Premera had made representations “regarding [the] confidentiality of private medical, financial, and personal information on which Plaintiffs and Class members relied in obtaining and purchasing Premera Blue Cross health insurance coverage.”⁶⁶⁸ The plaintiffs also claimed that the defendant “was not in compliance with many standards of data security.”⁶⁶⁹ The complaint alleges that the defendant’s conduct violated HIPPA, Washington’s Data Breach Notification Law,⁶⁷⁰ and the plaintiffs’ right to privacy at common law,⁶⁷¹ as well as constituted negligence,⁶⁷² breach of contract,⁶⁷³ and unjust enrichment.⁶⁷⁴

X. DISCLOSURES OF DATA UNDER THE FEDERAL OR A STATE FOIA OR STATE PUBLIC RECORDS DISCLOSURE LAW

A. Introduction

Three transportation agencies responding to the survey reported receiving requests to disclose secure data pursuant to a FOIA or other state public records disclosure law,⁶⁷⁵ whereas nine agencies reported that they had not received any requests for secure data.⁶⁷⁶ Four agencies advised that they had received requests for monitoring data,⁶⁷⁷ but eight agencies stated that they had not received any requests for monitoring data.⁶⁷⁸

B. The Federal FOIA and Release of Data

The federal Freedom of Information Act of 1966⁶⁷⁹ creates a strong presumption of public access to agency records.⁶⁸⁰ Documents that are not required

⁶⁶⁸ *Id.* at 4.

⁶⁶⁹ *Id.* at 5.

⁶⁷⁰ *Id.* at 16 (citing WASH. REV. CODE § 19.255.010).

⁶⁷¹ *Id.* at 24.

⁶⁷² *Id.* at 17.

⁶⁷³ *Id.* at 21.

⁶⁷⁴ *Id.* at 22.

⁶⁷⁵ Arkansas DOT, Indiana DOT, and City of Minneapolis–Public Works Dept. The Maine DOT and Ohio DOT did not respond to the question.

⁶⁷⁶ Alabama DOT, Arizona DOT, MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Montana DOT’s response was “not known.”

⁶⁷⁷ Arkansas DOT, Arizona DOT, District of Columbia DOT, and City of Minneapolis–Public Works Dept. The Maine DOT and Ohio DOT did not respond to the question.

⁶⁷⁸ Alabama DOT, Indiana DOT (stating that details are not available), North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Montana DOT’s response was “none known.”

⁶⁷⁹ Pub. L. No. 89-487, 80 Stat. 250, codified at 5 U.S.C. § 552, *et seq.* (2015).

⁶⁸⁰ 5 U.S.C. § 552(d) (2015).

to be published by an agency are subject to disclosure unless the information comes within one of nine exemptions.⁶⁸¹ Thus, unless a request for government data is protected from disclosure by an exemption in the FOIA or by another law, it appears that a request for data may be allowable.⁶⁸² However, at least one court has ruled that an agency need not disclose records automatically but must weigh the effects of disclosure and nondisclosure and determine the best course to follow.⁶⁸³

C. State FOIA or Public Records Disclosure Laws and a Release of Data

Likewise, state statutes that allow for the disclosure of data collected by state agencies may include an exemption permitting a transportation agency to withhold data. The New York Public Officers Law requires an agency to make available for public inspection and copying all records except those that come within certain exemptions that are similar to the exemptions in the federal FOIA.⁶⁸⁴

First, an applicable FOIA or public records disclosure law may exempt certain personal data from disclosure. In Pennsylvania, it is not necessary to disclose “[a] record, the disclosure of which would be reasonably likely to result in a substantial and demonstrable risk of physical harm to the personal security of an individual.”⁶⁸⁵ Although Michigan’s FOIA includes a presumption in favor of disclosure, one exemption protects “[i]nformation of a personal nature” from disclosure “if public disclosure... would constitute a clearly unwarranted invasion of an individual’s privacy.”⁶⁸⁶ Similar to Michigan’s FOIA, the Illinois FOIA prohibits inspection and copying of “[p]rivate information, unless disclosure is required by another provision of [the Illinois FOIA], a state or federal law or court order.”⁶⁸⁷ The Illinois FOIA provides that personal information contained in public records may not be inspected or copied if the disclosure would constitute “a clearly unwarranted invasion of personal privacy” unless

⁶⁸¹ 15 U.S.C. §§ 552(b)(1)–(9) (2015).

⁶⁸² 5 U.S.C. § 552(a) (2015).

⁶⁸³ *Gen. Servs. Admin. v. Benson*, 415 F.2d 878, 880 (9th Cir. 1969).

⁶⁸⁴ N.Y. PUB. OFF. LAW § 87(2) (2015).

⁶⁸⁵ 65 PA. CONS. STAT. §§ 67.708(b)(1)(i)–(ii) (2015). *See also* Glancy, *supra* note 4, at 301.

⁶⁸⁶ MICH. COMP. LAWS SERV. § 15.231, *et seq.* (2015) and *see id.* § 15.243(a) (2015). *See also* Michigan Fed’n of Teachers v. University of Michigan, 481 Mich. 657, 753 N.W.2d 28 (Mich. 2008) (holding that names and addresses of teachers were part of a FOIA privacy exemption and therefore could not be disclosed) and Robert M. Vercrey & Susan K. Friedlaender, *Employee Privacy Rights in the Public and Private Employment Sector*, 68 MICH. B.J. 608, 609 (1989).

⁶⁸⁷ 5 ILL. COMP. STAT. § 140/7(1)(b) (2015).

the subject of the information consents in writing to the disclosure.⁶⁸⁸

Second, state FOIAs or the equivalent may exempt records that are specifically prohibited from disclosure by laws other than the state's FOIA or other public records disclosure law. In Pennsylvania, “[a] record of information[] identifying an individual who applies for or receives social services” may not be disclosed.⁶⁸⁹ In *Bullock v. Southeastern Pennsylvania Transportation Authority*,⁶⁹⁰ a case decided by the Office of Open Records,⁶⁹¹ Bullock requested SEPTA's Americans with Disabilities Act paratransit reports, including medical assessments, records, and written results and recommendations.⁶⁹² Because paratransit services “are social services[] and.. all the records requested relate to the application for, evaluation of and eligibility for the services,” the requested records were exempt from disclosure.⁶⁹³

In Illinois, “information specifically prohibited from disclosure by federal or State law or rules and regulations implemented by federal or State law” may not be disclosed.⁶⁹⁴ New York and Wisconsin have similar exemptions.⁶⁹⁵

In New York, the Committee on Open Government issued an advisory opinion with respect to a request directed to the New York State DOT by a reporter for the *Albany Times Union* for a list of “safety deficient locations.”⁶⁹⁶ The DOT denied the request based on an exemption in N.Y. Public Officers Law Section 87(2)(a) and 23 U.S.C. § 409. The DOT argued that the information had been collected with the assistance of federal funds and that Section 409 provides that such information “shall not be subject to discovery or admitted into evidence in a Federal or State court proceeding....”⁶⁹⁷

⁶⁸⁸ 5 ILL. COMP. STAT. § 140/7(1)(c) (2015).

⁶⁸⁹ 65 PA. CONS. STAT. § 67.708(b)(28) (2015).

⁶⁹⁰ In the Matter of Janice Bullock, Complainant v. Southeastern Pennsylvania Transportation Authority, Docket No. AP 2010-0343 at 1 (2010) [hereinafter In re: Bullock].

⁶⁹¹ Although final determinations by the Office of Open Records are binding, they are subject to judicial review. See <https://www.dced.state.pa.us/public/oor/fd/FinalDetermination.pdf>.

⁶⁹² In re: Bullock, *supra* note 690, at 1 (citing 65 PA. CONS. STAT. § 67.708(b)(28)).

⁶⁹³ *Id.* at 3.

⁶⁹⁴ 5 ILL. COMP. STAT. 140/7(a) (2015).

⁶⁹⁵ See N.Y. PUB. OFF. § 87(2)(a) (2015); WIS. STAT. § 19.36(1) (2015).

⁶⁹⁶ State of New York Department of State Committee on Open Government, FOIL-AO-12395 (Dec. 1, 2000) [hereinafter FOIL-AO-12395], available at: <http://docs.dos.NYgov/coog/ftext/f12395.htm> (last accessed Oct. 12, 2015).

⁶⁹⁷ 23 U.S.C. § 409.

Nevertheless, the Committee ruled that Section 409 did not exempt the records from disclosure, because the statute “precludes the use of certain records in a litigation context; it does not, however, exempt records from disclosure in every instance.”⁶⁹⁸ The Committee stated that the request should not have been denied on the basis of 23 U.S.C. § 409 unless the requestor intended to use the records for litigation purposes.⁶⁹⁹ The Committee also ruled that the records may be exempt under N.Y. Public Officers Law Section 87(2)(g), which exempts certain inter-agency or intra-agency materials when they are “reflective of opinion, advice, recommendation and the like.”⁷⁰⁰ In this case, the requested information was not intra/inter-agency communications but rather statistical or factual data that were not exempt from disclosure.⁷⁰¹

Another example is *Commissioner of Public Health v. Freedom of Information Commission*,⁷⁰² involving a request by a newspaper for all records associated with a report that a physician had engaged in violations of the applicable standard of care.⁷⁰³ The report included an exhibit with records from the Practitioner Data Bank and the Healthcare Data Bank. The Supreme Court of Connecticut stated that federal statutes and regulations “strongly suggest that records” contained in the databases are not subject to disclosure under the FOIA.⁷⁰⁴ The court held that the Commissioner of Public Health could not disclose records that were received from the federal Healthcare Data Bank or the Practitioner Data Bank to an unauthorized person unless the records also originated from the agency's own files and disclosure was required under the federal or Connecticut's FOIA.⁷⁰⁵

A third exemption may be predicated on the possible loss of federal or state funding. In Pennsylvania it is not necessary to disclose “[a] record, the disclosure of which...would result in the loss of Federal or State funds by an agency or the Commonwealth....”⁷⁰⁶

Fourth, data may be exempt from disclosure when the data are used for law enforcement purposes. In New York, when an individual requested the New York City DOT to provide a list of the locations of cameras used in the City's Red Light Camera

⁶⁹⁸ FOIL-AO-12395, *supra* note 696.

⁶⁹⁹ *Id.*

⁷⁰⁰ *Id.*

⁷⁰¹ *Id.*

⁷⁰² 311 Conn. 262, 86 A.3d 1044 (Conn. 2013).

⁷⁰³ *Id.* at 265–266, 86 A.3d at 1046–1047.

⁷⁰⁴ *Id.* at 280, 86 A.3d at 1055.

⁷⁰⁵ *Id.* at 265, 86 A.3d at 1053–1055.

⁷⁰⁶ 65 PA. CONS. STAT. §§ 67.708(b)(1)(i)–(ii) (2015). See also Glancy, *supra* note 4, at 301.

Program,⁷⁰⁷ the DOT denied the request on the ground that the list was used only for law enforcement purposes.⁷⁰⁸ The New York Committee on Open Government ruled that the location of the cameras did not come within the law enforcement exemption in N.Y. Public Officers Law Section 87(2)(e). Moreover, because a camera's location is disclosed on the citation that an individual receives, there is "nothing secret" about the location of cameras.⁷⁰⁹

A District of Columbia case, *Wemhoff v. District of Columbia*,⁷¹⁰ illustrates how the secondary uses of roadside-collected data may present privacy issues. In *Wemhoff*, the plaintiff made a FOIA request for the names and addresses of motorists who received traffic violations because of being photographed by a red light camera. Wemhoff sought the information to solicit individuals for his lawsuit.⁷¹¹

The court's examination of the relevant provision of the DPPA, discussed *supra*, focused on the importance of maintaining drivers' privacy: "This [narrow] construction ensures that individuals' statutorily recognized rights to the privacy of their motor vehicle records are not sacrificed whenever a litigant raises the possibility of a tenuous connection between the protected information and issues tangentially related to a conceivable litigation strategy."⁷¹²

The court denied the request because it was not a "permissive use" within the meaning of the DPPA, and the disclosure would violate the DPPA and District of Columbia law.⁷¹³

Another possible exemption is that some states' agencies may be able to withhold data from the public under a "deliberative process" privilege, an exemption

⁷⁰⁷ State of New York Department of State Committee on Open Government, FOIL-AO-12412 (Dec. 19, 2000), [hereinafter FOIL-AO-12412], available at: <http://docs.dos.ny.gov/coog/ftext/f12412.htm> (last accessed Oct. 12, 2015). Each agency promulgates its own regulations and procedures regarding the availability of records. N.Y. PUB. OFF. § 87(1)(b). After an agency's decision the agency shall "immediately forward to the committee on open government a copy of such appeal when received by the agency and the ensuing determination thereon." N.Y. PUB. OFF. § 89(4)(a). If the request is denied or ignored, the person requesting the record may commence an action to compel compliance with the request. N.Y. PUB. OFF. § 89(4)(b)–(c). See generally DIGITAL MEDIA LAW PROJECT, *Access to Public Records in New York*, available at: <http://www.dmlp.org/legal-guide/access-public-records-new-york> (last accessed Oct. 12, 2015).

⁷⁰⁸ FOIL-AO-12412, *supra* note 707 (internal quotation marks omitted).

⁷⁰⁹ *Id.*

⁷¹⁰ 887 A.2d 1004, 1004–1006 (D. C. App. 2005).

⁷¹¹ *Id.* at 1009.

⁷¹² *Id.* at 1011 (citing *Pichler v. UNITE*, 339 F. Supp. 2d 665, 668 (E.D. Pa. 2004) (internal quotation marks omitted)).

⁷¹³ *Id.* at 1012.

that may be applicable to some data collected and maintained by transportation agencies.⁷¹⁴

D. Agency Waiver of Privacy Exemption

Exemptions under a FOIA or similar legislation may be waived. If an agency freely discloses "confidential information to a person without restricting that person's ability to disclose that information," the agency will waive its FOIA exemption.⁷¹⁵ It has been held that if a federal agency voluntarily discloses information that is subject to the FOIA's deliberative process privilege, the agency waives the right to claim later that the information is exempt.⁷¹⁶

E. Whether Both FOIA Requests and Discovery Requests May Be Used to Obtain a Transportation Agency's Data

Transportation agencies may receive requests under a FOIA or an equivalent public records disclosure law for secure data or monitoring data.⁷¹⁷ Indeed, in their responses to the survey nine transportation agencies reported receiving discovery requests and subpoenas for secure data,⁷¹⁸ whereas two agencies stated that they had not received such requests and subpoenas.⁷¹⁹ Seven transportation agencies reported receiving discovery requests and subpoenas for monitoring data,⁷²⁰ but five agencies

⁷¹⁴ *Shell Oil Co. v. IRS*, 772 F. Supp. 202, 203 (D. Del. 1991).

⁷¹⁵ Patrick Lightfoot, *Waiving Goodbye to Nondisclosure Under FOIA's Exemption 4: The Scope and Applicability of the Waiver Doctrine*, 61 CATH. U. L. REV. 807, 808 (2012).

⁷¹⁶ *Shell Oil Co.*, 772 F. Supp. at 211 (holding that the IRS was required to release information requested by an oil company under FOIA that an IRS employee had previously read at a public meeting because a public reading of the document constituted a waiver of the FOIA exemptions).

⁷¹⁷ See App. B, DOT responses to question 14(a) and (b).

⁷¹⁸ Alabama DOT, Arizona DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, and Rhode Island DOT. The Arizona DOT reported that "[a] public records report that provides request details is not available." The District of Columbia DOT and the Florida DOT responded that the information on requests is not available. Although not responding directly to question 15(a) or (b) that distinguishes between secure data and monitoring data, the Ohio DOT stated that the department responds to public records requests and discovery requests and subpoenas on a daily basis.

⁷¹⁹ Arkansas DOT and South Carolina DOT. Montana DOT's and Utah DOT's response was not known.

⁷²⁰ Alabama DOT, Arizona DOT, City of Minneapolis–Public Works Dept., MoDOT, Oklahoma DOT, Oregon DOT, and Rhode Island DOT. The Arizona DOT stated that "[a] public records report that provides request details is not available." The Florida DOT responded that the information on request is not available.

had not received such discovery requests and subpoenas.⁷²¹

The use of a FOIA or similar statute for the purpose of discovery in litigation typically is not permitted; thus, FOIA requests should not be used as a primary means of discovery in civil litigation.⁷²² Indeed, some courts have held that they will not allow FOIA to be used as a substitute for discovery.⁷²³ In *N.L.R.B. v. Sears, Roebuck & Co.*,⁷²⁴ the National Labor Relations Board sought to set aside a district court's order directing it to disclose certain memoranda to Sears, Roebuck & Co. (Sears) pursuant to the FOIA. The Supreme Court held that Sears's rights under the FOIA were "neither increased nor decreased by reason of the fact" that Sears claimed a greater interest in the memoranda than an "average member of the public."⁷²⁵ The purpose of the FOIA is to inform the public about agency action, not to benefit private litigants.⁷²⁶

In *Columbia Packing Co., Inc. v. United States Dept. of Agriculture*,⁷²⁷ the First Circuit relied on the Supreme Court's decision in *Sears, Roebuck & Co.*, in holding that whether a FOIA disclosure is warranted is not affected by a party's request for documents during discovery.⁷²⁸ Furthermore, if

⁷²¹ Arkansas DOT, District of Columbia DOT, Indiana DOT, North Dakota DOT, and South Carolina DOT. The Montana DOT's and the Utah DOT's responses were "not known."

⁷²² *Mercy Hosp. v. NLRB*, 449 F. Supp. 594, 597 (S.D. Iowa 1978) (quoting *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132 (1975)); *Johnson v. United States Department of Justice*, 758 F. Supp. 2, 4 (D.D.C. 1991) (holding that "FOIA is not a discovery statute"). Scholars likewise argue that a FOIA is meant to address public access to information and not to aid private litigants in litigation. See Robert C. Davis, *Discovery in Environmental Litigation*, 25 A.F. L. Rev. 168, 176–177 (1985); George K. Chamberlin, Annotation, *Use of Freedom of Information Act as Substitute for, or as Means of, Supplementing Discovery Procedures Available to Litigants in Federal Civil, Criminal, or Administrative Proceedings*, 57 A.L.R. Fed. 903 (2001).

⁷²³ See, e.g., *Renegotiation Bd. v. Bannerkraft Clothing Co.*, 415 U.S. 1, 20, 94 S. Ct. 1028, 1038, 39 L. Ed. 2d 123, 137 (1974).

⁷²⁴ 421 U.S. 132, 135–136, 95 S. Ct. 1504, 44 L. Ed. 2d 29 (1975). The memoranda in dispute were generated by the Board's Office of the General Counsel when deciding whether to permit the filing of unfair labor practice complaints with the Board.

⁷²⁵ *Id.*, 421 U.S. at 143 N 10, 95 S. Ct. 1504, 44 L. Ed. 2d 29.

⁷²⁶ *Id.*, 421 U.S. at 143, 95 S. Ct. 1504, 44 L. Ed. 2d 29. See, however, *Reunion, Inc. v. Federal Aviation Administration*, 2010 U.S. Dist. LEXIS 42934, at *1, 2–3, 5 (S.D. Miss. 2010) (holding when the plaintiff sought to obtain certain records from the FAA and the Office of the Secretary of Transportation that "[u]nder present law there is no statutory prohibition to the use of FOIA as a discovery tool").

⁷²⁷ 563 F.2d 495 (1st Cir. 1977).

⁷²⁸ *Id.* at 499 (declining to consider Columbia Packing Corporation's interest in enlarged discovery in regard to whether to order disclosure under the FOIA).

government data are exempt under the FOIA, it is not presumed that the information is thereby privileged within the meaning of the discovery rules.⁷²⁹ When there is a FOIA request, a party's need for the information is "irrelevant" in contrast to discovery when a qualified privilege is asserted and a litigant's need for the information is a key factor for the court's consideration.⁷³⁰

CONCLUSION

The Supreme Court has not recognized a constitutional right to privacy in one's personal or locational information.⁷³¹ Thus, it does not appear that the disclosure of secure data, including an individual's PII, or of monitoring data would violate a right to privacy under the U.S. Constitution. A privacy right does not implicate the U.S. Constitution unless the asserted privacy right is recognized by the Court as a "fundamental right" or one that is "implicit in the concept of ordered liberty" that is not outweighed by a compelling governmental interest in disclosure.⁷³² As one case has held, even if the government's dissemination of information injures one's reputation, the disclosure does not in and of itself state a cause of action for the violation of a constitutional right.

In *Lambert*, the court stated that there is no privacy interest of a constitutional dimension unless a disclosure of personal information could lead to bodily harm or is of a "sexual, personal, and humiliating nature...."⁷³³ Although the DPPA creates a federal statutory right to privacy for PII collected by state DMVs, even the disclosure of the same PII has been held not to violate a constitutional right to privacy.⁷³⁴ Thus, the government's disclosure of secure data, such as a person's Social Security number, has not been held to violate a constitutional right to privacy.⁷³⁵

It has been held also that "the Fourth Amendment is not "a general constitutional 'right to privacy.'"⁷³⁶ In the *Katz* case, the Supreme Court stated that "what a person knowingly exposes to the public...is not a subject of Fourth Amendment protection."⁷³⁷

⁷²⁹ *Friedman v. Bache Halsey Stuart Shields, Inc.*, 738 F.2d 1336, 1344 (D.C. Cir. 1984).

⁷³⁰ *Id.*

⁷³¹ Phillips and Kohm, *supra* note 1, at P4; Garry, Douma, and Simon, *supra* note 2, at 103.

⁷³² See *Lambert*, 517 F.3d at 440.

⁷³³ *Id.*

⁷³⁴ *Kiminski*, 2013 U.S. Dist. LEXIS 157829, at *40 (citation omitted).

⁷³⁵ *Lambert*, 517 F.3d at 443 (citations omitted).

⁷³⁶ *Katz*, 389 U.S. at 350, 88 S. Ct. at 510, 19 L. Ed. 2d at 581 (footnotes omitted).

⁷³⁷ *Id.*, 389 U.S. at 351, 88 S. Ct. at 511, 19 L. Ed. 2d at 581 (citation omitted).

The Court more recently has stated that individuals using public highways have a diminished expectation of privacy.⁷³⁸ No cases were located for the digest holding that the use of technology to enhance and record the visual observation of motorists' use of public highways violates a constitutional right to privacy.

Because a constitutional right in personal or locational data has not been established, it does not appear that a complaint against a transportation agency's officers or agents for the disclosure of secure data or monitoring data would state a claim under 42 U.S.C. § 1983. Even if government officials, who are acting within their discretionary authority, are sued in their individual capacities for the violation of a constitutional or statutory right, they have qualified immunity as long as "their conduct does not violate *clearly established* statutory or constitutional rights of which a reasonable person would have known."⁷³⁹ Furthermore, one court has gone even further and held that it would be "unfair to charge an official with knowledge of the law in the absence of a previously decided case with *clearly analogous facts*."⁷⁴⁰ Thus, a disclosure of secure data or monitoring data would not appear to state a § 1983 claim for a violation of privacy, because a clearly established constitutional or statutory right to one's privacy in such data has not been established.

Although a violation of the federal DPAA may give rise to a claim under the statute, the courts also have held that a disclosure of the very same data protected by the DPAA does not state a claim under § 1983 for a violation of a constitutional right to privacy. Likewise, in *Toomer*, the court held that the disclosure of secure data in the form of a former employee's personnel file did not violate a constitutional right to privacy for the purpose of a § 1983 claim.⁷⁴¹ However, as seen in *Toomer*, there may be a violation of the Fourth Amendment and a resulting § 1983 claim whenever a government official acts with a "high level of culpability, including deliberate indifference, malice, willfulness, and retaliation."⁷⁴² Unless there has been egregious, arbitrary action in disclosing an individual's data, it does not seem that an unintentional disclosure of secure data or an intentional disclosure of monitoring data would state a

⁷³⁸ *Houghton*, 526 U.S. at 303, 306, 119 S. Ct. at 1302–1303, 143 L. Ed. 2d at 417 and *Knotts*, 460 U.S. at 281, 103 S. Ct. at 1085, 75 L. Ed. 2d at 62.

⁷³⁹ *Harlow*, 457 U.S. 800, 818, 102 S. Ct. 2727, 73 L. Ed. 2d 396 (1982) (citation omitted) (emphasis added).

⁷⁴⁰ *Borucki*, 827 F.2d at 848 (footnote omitted) (citations omitted) (emphasis added).

⁷⁴¹ *Toomer*, 155 N.C. App. at 469, 574 S.E.2d at 84 (citing *Kallstrom*, *supra*).

⁷⁴² *Id.*, 155 N.C. App. at 470, 574 S.E.2d at 84.

claim for a violation of a constitutional or statutory right to privacy under § 1983.

As for state privacy law, at least 10 state constitutions have provisions for the protection of an individual's right to privacy. Some state constitutions provide and some courts have held that an individual's right to privacy must be balanced against a compelling state interest in disclosure. Some state courts have held that an individual has a cause of action for monetary damages for violations of state constitutional provisions. However, although some state constitutions and state statutes do create privacy rights in data collected and held by government agencies, there seem to be no state laws "that specifically address privacy rights and transportation technologies."⁷⁴³ In any case, only some states appear to have privacy laws (e.g., California, Minnesota, and Massachusetts) that include a private right of action for damages for a violation of the statute.⁷⁴⁴ Unless a privacy statute authorizes the recovery of specific or liquidated damages or provides for a civil penalty for a violation, it appears that a plaintiff would have to prove that the release of secure data or monitoring data caused the plaintiff to incur actual damages.

Most states do recognize one or more rights to privacy at common law.⁷⁴⁵ A privacy claim at common law requires that the defendant's conduct was intentional, as mere negligence ordinarily will not suffice.⁷⁴⁶ In some states, a violation of common law privacy must have been the result of "willful or outrageous" conduct.

Even when there is a cause of action for a violation of a state common law right to privacy, transportation agencies in some states will have sovereign immunity. As seen, in *Axtell*, the court held that the intentional disclosure by a state institution of confidential information was not actionable, because the state had retained its immunity under the state tort claims act. However, in the *Toomer* case, the department did not have immunity because of the plaintiff's allegations of malice and bad faith on the part of the Secretary of the DOT who purposely released the plaintiff's personnel file and PII.⁷⁴⁷ Nevertheless, no case was located for the digest in which a court held a transportation agency liable in tort for an unintentional disclosure of secure data or for an intentional disclosure of monitoring data in a context similar to ITS.⁷⁴⁸

⁷⁴³ Douma and Deckenbach, *supra* note 2, at 309.

⁷⁴⁴ *Id.* at 308–09.

⁷⁴⁵ See *Phillips v. Smalley Maintenance Services, Inc.*, 711 F.2d 1524, 1533 (1983) (citations omitted).

⁷⁴⁶ Dorothy Glancy, *supra* note 584, at 179.

⁷⁴⁷ *Toomer*, 155 N.C. App. at 480–481, 574 S.E.2d at 91.

⁷⁴⁸ See Dorothy Glancy, *supra* note 584, at 179.

Some transportation agencies reported having received requests to disclose secure data or monitoring data pursuant to a FOIA or other state public records disclosure law. In some instances, such data will be exempt from disclosure, because the data would violate personal privacy, because another federal or state law prohibits disclosure of the data, or because the statute exempts data from disclosure that are used for law enforcement purposes.

Finally, with the few exceptions discussed in the digest, there have been no reported claims against transportation agencies regarding their collection, use, disclosure, and/or retention of secure data or monitoring data. Furthermore, the agencies responding to the survey did not report having a claim arising out of their disclosure either of secure data or monitoring data, regardless of whether a disclosure was intentional or unintentional.

APPENDICES

The following appendices are available online at www.trb.org by searching for *NCHRP LRD 71*.

Appendix A: Project Survey Questions, A1–6

Appendix B: Summary of Survey Responses, B1–27

Appendix C: Copies of Policies, Procedures, Regulations, and Contracts on the Collection of Secure Data and Monitoring Data, C1–108

Appendix D: List of Transportation Agencies Responding to the Survey, D1

ACKNOWLEDGMENTS

This study was performed under the overall guidance of the NCHRP Project Committee SP 20-6. The Committee is chaired by MICHAEL E. TARDIF, Friemund, Jackson and Tardif, LLC. Members are RICHARD A. CHRISTOPHER, HDR Engineering; TONI H. CLITHERO, Vermont Agency of Transportation; JOANN GEORGALLIS, California Department of Transportation; JAMES H. ISONHOOD, Mississippi Office of the Attorney General; THOMAS G. REEVES, Consultant, Maine; MARCELLE SATTIEWHITE JONES, Jacob, Carter and Burgess, Inc.; ROBERT J. SHEA, Pennsylvania Department of Transportation; JAY L. SMITH, Missouri Department of Transportation; and JOHN W. STRAHAN, Consultant, Kansas.

MEGHAN P. JONES provided liaison with the Federal Highway Administration, and GWEN CHISHOLM SMITH represents the NCHRP staff.

Transportation Research Board

500 Fifth Street, NW
Washington, DC 20001

NON-PROFIT ORG.
U.S. POSTAGE

PAID

COLUMBIA, MD
PERMIT NO. 88

The National Academies of

SCIENCES • ENGINEERING • MEDICINE

The nation turns to the National Academies of Sciences, Engineering, and Medicine for independent, objective advice on issues that affect people's lives worldwide.

www.national-academies.org

Subscriber Categories: Administration and Management • Law

ISBN 978-0-309-37548-1



These digests are issued in order to increase awareness of research results emanating from projects in the Cooperative Research Programs (CRP). Persons wanting to pursue the project subject matter in greater depth should contact the CRP Staff, Transportation Research Board of the National Academies of Sciences, Engineering, and Medicine, 500 Fifth Street, NW, Washington, DC 20001.