Oregon
Kate Brown, Governor

Department of Transportation
Director's Office
355 Capitol St. NE, MS 11
Salem, OR 97301

DATE: March 17, 2015

TO: Senate Committee on Judiciary

FROM: Amy Joyce, Legislative Liaison

SUBJECT: SB 640

INTRODUCTION

Senate Bill 640 prohibits a public body from obtaining location information from the use of electronic devices. The bill further prohibits a public body from obtaining any contents of electronic communication. The Oregon Department of Transportation uses electronic data collection to further its mission.

DISCUSSION

The department uses electronic information in several ways. In our regulation of heavy trucks, we used license plate readers to sort trucks and quickly capture data within the weigh station, and to identify trucks that subject to our tax and safety regulations. Our Motor Carrier Transportation Division also uses the innovative Green Light Program. Truck owners voluntarily agree to carry a transponder on board and, as the truck passes over sensors at full speed, the sensors measure weight and length, the information is instantaneously checked for compliance, and the truck's safety and inspection record is verified. If the truck is in compliance the transponder receives a green light meaning the driver can continue on without a time-consuming and costly stop. A red light instructs the driver to pull into the weigh station.

Oregon's mileage fee program, an alternative for the fuel tax, is about to go live for 5,000 volunteers under the Road Usage Charge program adopted by the 2013 Legislature. ODOT's account managers will need access to location information and personal information about some subscribers – those who choose to use a technology that more accurately calculates mileage subject to the fuel tax - in order to collect the appropriate amount. The location information is transmitted electronically by the advanced mileage reporting device in the vehicle to the account manager, which allows the account manager to determine if the miles are taxable. Without location information, the basic device only transmits the miles driven and all of these are assumed to be taxable. The program becomes effective on July 1, 2015.

SB 640 provides an avenue to collect this electronic information for both the Green Light and Road Usage Charge programs because we have the subscriber's specific consent by enrolling in the programs. The bill requires extensive reporting on how the agency uses this data.

ODOT also uses Bluetooth and cellular data to determine how traffic is flowing on the transportation system, particularly travel patterns and speed. The cellular data is typically purchased from private providers, after it has been aggregated and containing no identifying

information. ODOT does not collect information about device owners. Rather, the number identifying the device itself is scrambled so we cannot determine anything about the device or its owner. ODOT is interested in how well the transportation system is functioning, not personal information about any users.

ODOT also uses this data to plan for future transportation projects and for systems such as the ODOT RealTime system in Portland. The RealTime system displays travel times between points of travel, allowing drivers to make informed decisions about the routes they travel. Despite the fact this data is scrambled, providing no opportunity for ODOT to learn anything about the device (or its owner) SB 640 would prohibit ODOT from collecting or using this type of data.

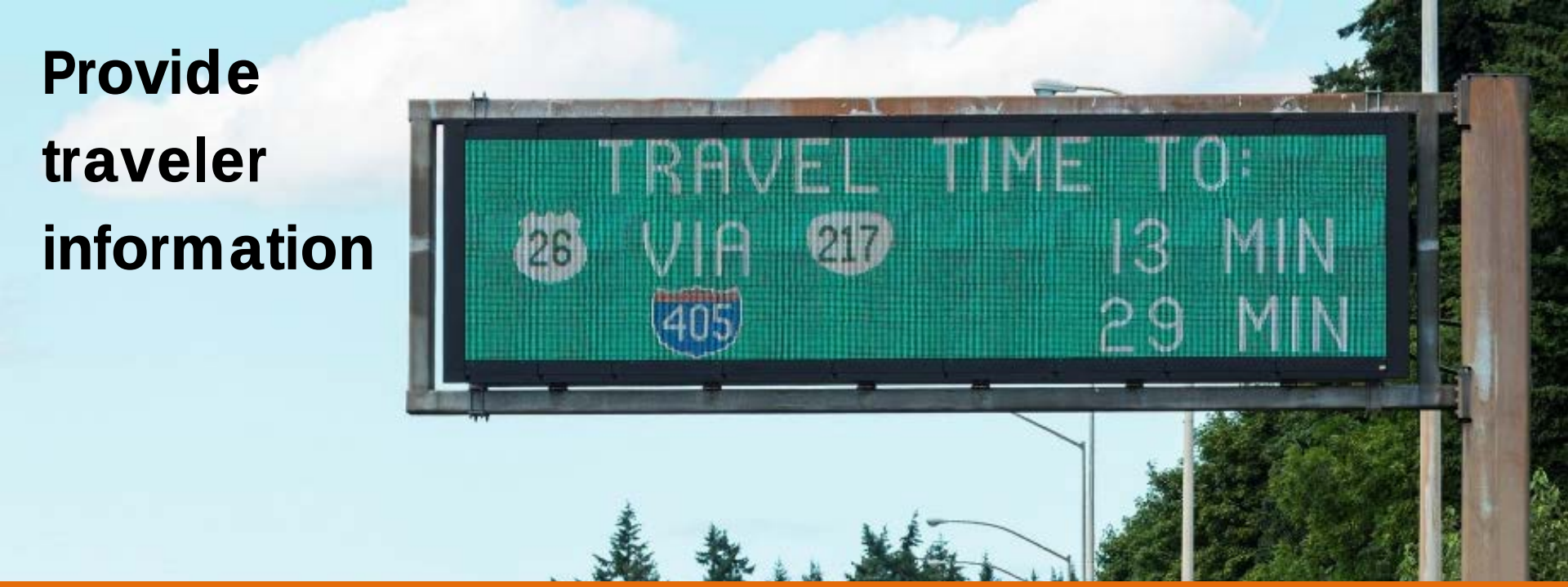
At the conclusion of the 2014 session, recognizing the heightened interest in protecting personal data and the fact ODOT uses technology in furtherance of our mission, the agency set about crafting a policy to guide our current and future electronic data collection. We gathered people from every relevant division of our agency, defined the issue, researched our current and potential future uses, and set down principles to guide our agency. The policy, which addresses collection, use, storage, and disposal of passively collected electronically data, was recently finalized. An implementation plan is already being executed. The policy is attached.

SUMMARY

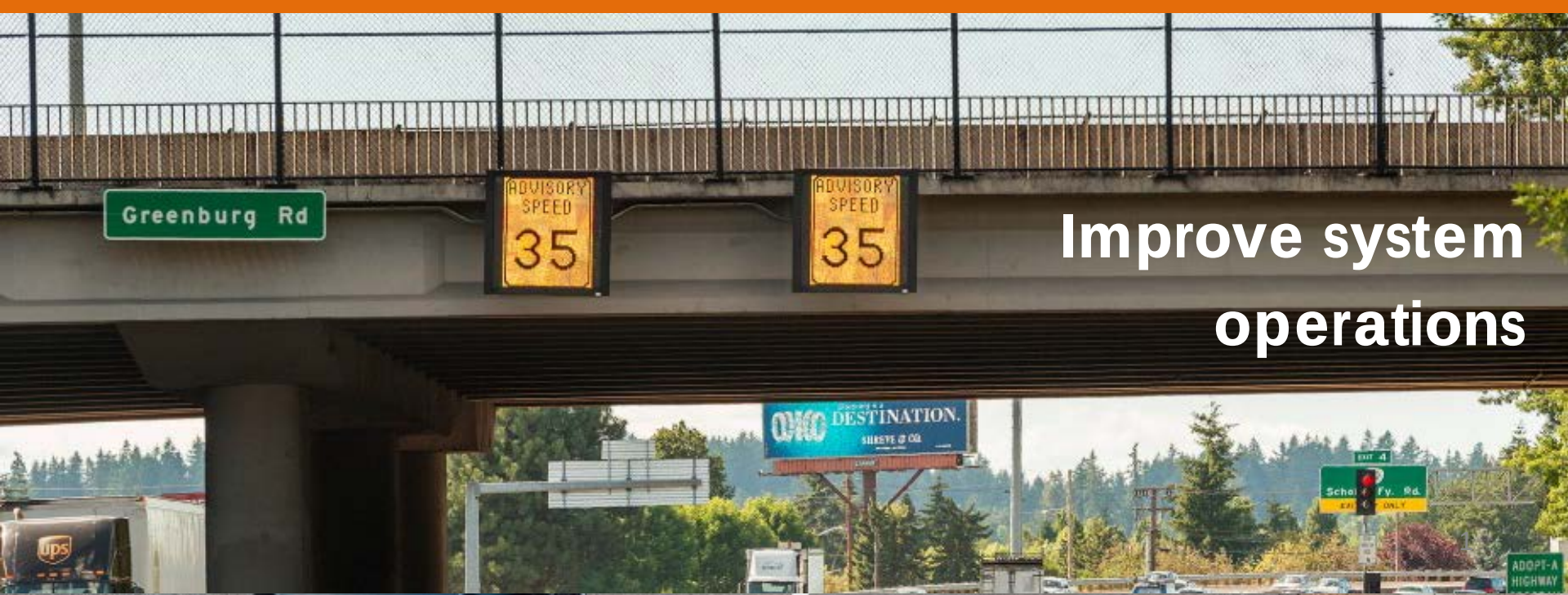
ODOT collects data electronically, both from voluntary providers and by passive collection methods, to further the agency's mission to provide a safe and effective transportation system. ODOT recently put into effect a new policy on the collection of electronic data, which protects the interests of the public. Some of ODOT's efforts using technology to more effectively and efficiently carry out our mission would be significantly constrained by this bill. We ask the committee to consider changes to the bill to accommodate these uses.

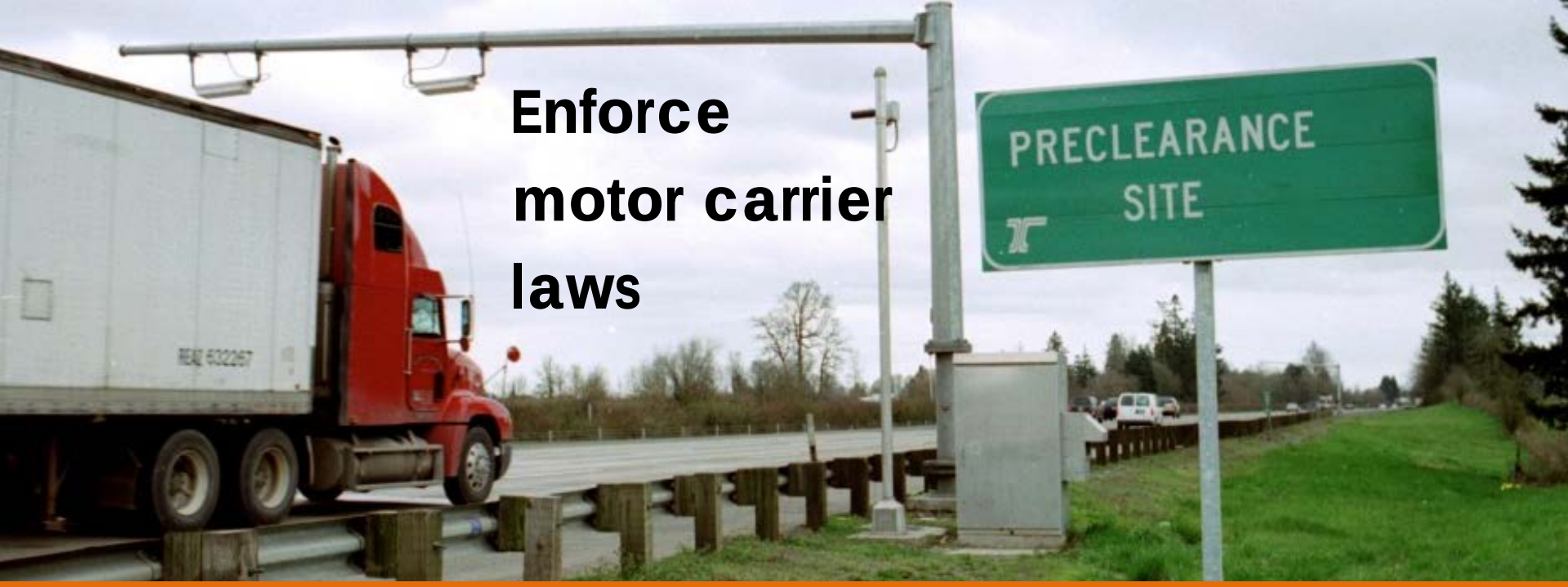
Attachments: Examples of how ODOT uses Bluetooth/cellular readers
Passive Electronic Data Collection Policy

Provide traveler information

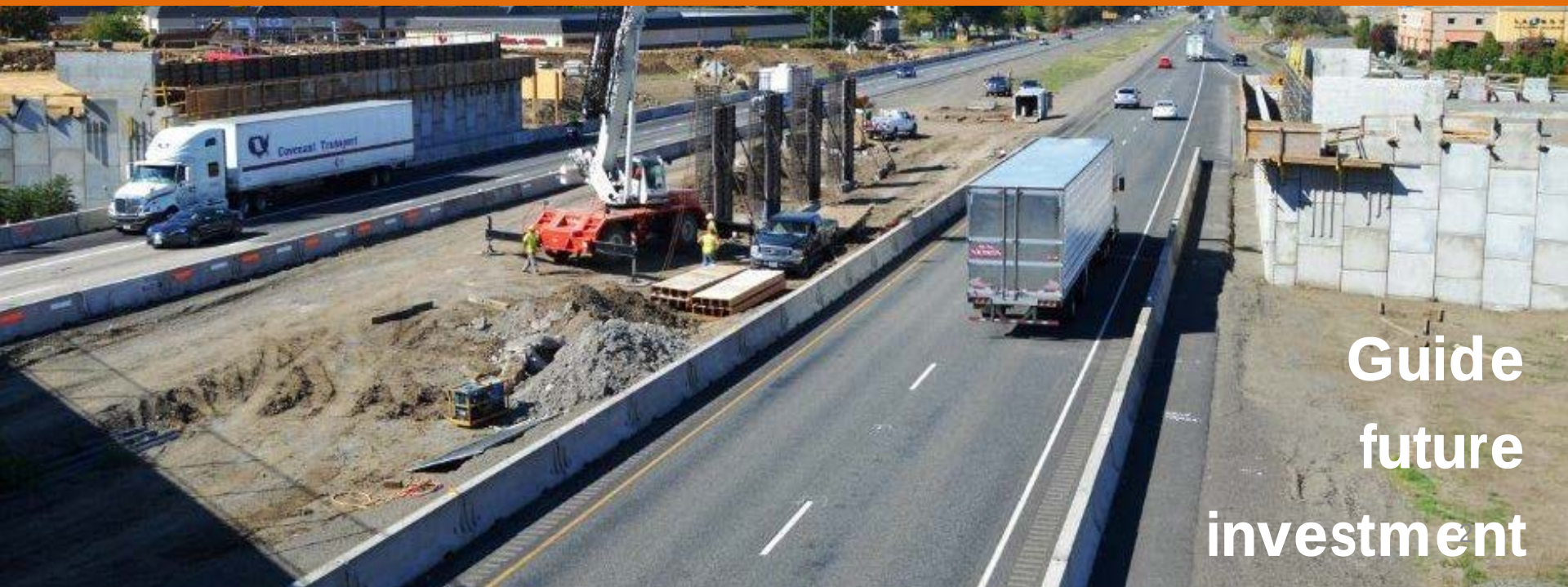


Improve system operations





Enforce motor carrier laws



Guide future investment

Oregon Department of Transportation **POLICY**	NUMBER ADM 08-01	SUPERSEDES New
	EFFECTIVE DATE 03/12/2015	PAGE NUMBER 1 of 7
	VALIDATION DATE	
	REFERENCE	
SUBJECT **Passive Electronic Data Collection**	APPROVED SIGNATURE Signature on file in Business Services	

PURPOSE

The purpose of the policy and implementation actions is to guide the Oregon Department of Transportation's (Department) collection and use of passive electronic data in a way that is transparent and ensures protection of the privacy and sensitive information of the public, including collected personally identifiable information (PII).

POLICY

The Department respects the privacy of all Oregonians and those using the state's transportation system. Passive electronic data collection will be done only to further the Department's mission to provide a safe and efficient transportation system that supports economic opportunity and livable communities for Oregonians. Passive electronic data collection shall be done to further the mission of the Department only to the minimum level necessary for that purpose, shall be maintained under tight security, and shall be destroyed as soon as the Department's use for the data ends.

BACKGROUND

Passive and Active Data

The Department collects passive and active electronic data. Passive is a term used in data collection in which the customer has little or no awareness of the data being collected and requires no explicit actions on the customer's part. For example, the Department uses a series of sensors and Bluetooth® signals emitted by cellular phones or built-in Bluetooth® systems in cars to supplement data from traffic sensors used to estimate the travel minutes to key destinations. The travel minutes are projected onto reader boards on Portland-area freeways and highways to help motorists plan their arrival time or consider taking an alternate route. The software being used for the project reads only a portion of the Bluetooth® media access control addresses (unique identifier of the device), preventing identification of a specific device, and then the truncated media access control address is encrypted. This truncated, encrypted identifier is what is transmitted to the server for calculation of travel time between points.

The opposite of passive electronic data collection is active electronic data collection. Active is a term used in data collection in which the customer actively provides and is made aware of how that information will be used. For example, when a customer downloads a smartphone application to track their bicycle rides via GPS, the customer actively accepts the terms and conditions that allow the application to use GPS to identify the position of the device. The Department can determine which bicycle routes are being used and plan improved facilities in those areas. The Department also collects data from Oregon residents through the Transportation Needs and Issues Survey to assess perceptions about the transportation system, determine how the system is used, and identify transportation related concerns. Survey forms are submitted electronically and by mail to the Department by customers.

Passive electronic data collection, and not active electronic data collection, is the subject of this passive electronic data collection policy. Customers are already aware of the Department's active electronic data collection efforts since they provide the information. Active electronic data collection is also heavily regulated by existing Department policies and state statutes. Photo or video images that are merely incidentally collected in pursuit of another, legitimate purpose such as images from a stationary or mobile scanner for surveying and mapping are not prevented from being collected, used, or displayed to the public. The Department may not subject those images to software or other tools that digitize or "read" license plates or other potentially identifying information.

Classifying and Securing Assets

The Department has a policy and guidance on classifying and securing assets. In 2009, ODOT issued the Information Asset Classification Policy (ADM 07-11). The key components of the Department's policy are:

- Identifying information owners who are responsible for classifying assets and deciding on appropriate protections;
- Classifying assets into one of four levels of sensitivity, ranging from low sensitivity/openly available to extremely sensitive (level 1 "published;" level 2 "limited;" level 3 "restricted;" level 4 "critical"); and
- Determining the appropriate level of protection for each asset based on its classification.

The Department's information owners as defined in the Information Asset Classification Policy (ADM 07-11) are responsible for classifying the passive electronic data discussed in this policy and deciding on appropriate protections. This passive electronically collected data privacy policy provides clarification of what passive electronic data is and how the Department is protecting the sensitive information in the passive electronically collected data.

Retention Schedules

The Department has retention schedules authorized by the State Archivist for the retention and disposition of public records in the Department's custody. Oregon Revised Statute (ORS) 192 and Oregon Administrative Rule (OAR) 166 describe the authority and requirements related to the creation of records retention schedules for Oregon state and local

governments. The Department's retention and disposition schedules for passive electronic data will adhere to ORS 192 and OAR 166.

DEFINITIONS

Confidentiality: A security principle that works to ensure that information is not disclosed to unauthorized subjects as defined in the Department's Information Asset Classification Policy (ADM 07-11).

Law Enforcement Agency: Has the meaning given that term in ORS 181.010(7) listed as follows:

(7) "Law enforcement agency" means:

(a) County sheriffs, municipal police departments, police departments established by a university under ORS 352.383 or 353.125 and State Police;

(b) Other police officers of this state or another state, including humane special agents as defined in ORS 181.435;

(c) A tribal government as defined in section 1, chapter 644, Oregon Laws 2011, that employs authorized tribal police officers as defined in section 1, chapter 644, Oregon Laws 2011; and

(d) Law enforcement agencies of the federal government.

Passive Electronic Data: Data in which the customer has little or no awareness of the electronic data being collected and requires no explicit actions on the customer's part. Data collection devices include but are not limited to license plate readers and Bluetooth® scanners.

Personal Information: As defined in the Oregon Consumer Identity Theft Protection Act, ORS 646A.602(11) listed as follows:

(11) "Personal information":

(a) Means a consumer's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired:

(A) Social Security number;

(B) Driver license number or state identification card number issued by the Department of Transportation;

(C) Passport number or other United States issued identification number; or

(D) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account.

(b) Means any of the data elements or any combination of the data elements described in paragraph (a) of this subsection when not combined with the consumer's first name or first initial and last name and when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised.

(c) Does not include information, other than a Social Security number, in a federal, state or local government record that is lawfully made available to the public.

Sensitive Information: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled as defined in the Department's Information Asset Classification Policy (ADM 07-11).

OBJECTIVES

a) Collection: The individual's interest in privacy in the Department's passive electronic data collection efforts must be respected. This requires disclosure of what type of information is collected. Examples of the type of information collected by the Department include the width and depth of every section of highway or the estimated number of axles that pass over a section of highway.

Sections of this adopted passive electronic data collection policy may, or may not, apply to certain divisions of the Department based on the scenario of data collection and use of the data. Some divisions of the Department use passive electronic data collection for regulatory purposes such as enforcing heavy truck regulations. Other divisions of the Department use passive electronic data collection for research, operations and planning purposes such as to improve travelers' safety, reduce travel times, and enhance individuals' ability to deal with highway disruptions. Traveler information is collected from many sources; some from the infrastructure and some from vehicles.

b) Transparency: Make passive electronic data collection transparent. Individuals should have a means of discovering the type of data collected, how it is collected, how it is used, and how it is distributed.

c) Security: Be responsible stewards of the sensitive information the Department holds. Data security technology and internal review procedures appropriate to the sensitivity of the information will be utilized. Technological and administrative safeguards shall be used to assure that access to sensitive information is restricted to duly authorized individuals.

Passive electronic data that contains or has the potential to contain sensitive information shall be destroyed in accordance with the Department's retention policies.

The department collects some images for appropriate purposes that can have the incidental effect of occasionally showing potentially identifiable information. For example, some license plates happen to be visible on the digital video log, traffic cameras, or survey photographs. One of the primary purposes of the collection of the images may be distribution to the public. The department will continue capturing appropriate images for appropriate purposes, but will restrict the use of those images for identifying purposes.

d) Anonymity: Where appropriate, the sensitive information in passive electronic data will not be collected or will be removed, cryptographically hashed, truncated, or aggregated so the data is anonymous.

e) Sharing of Passive Electronic Data: The Department shall ensure that passive electronic data provided to the public, and public and private organizations for secondary uses is stripped of personal identifiers unless otherwise provided in this policy.

Collection

Responsibility	Action
Applicable Divisions	Perform passive electronic data collection only when necessary for regulatory, research, operations and planning purposes.

Transparency

Responsibility	Action
TDD Administrator Designee	Post on the Web the type of data collected, how it is collected, how it is used, and how it is distributed.
Business Services Branch	Publish and distribute this passive electronic data collection policy and its implementation actions electronically on the Intranet; Post any data privacy policy changes on the Web.

Security

Responsibility	Action
TDD Administrator Designee	Develop an internal review process and other standard processes to ensure the Department's

	compliance with this policy.
Division Administrators	Ensure Division employees do not disclose passive electronic data to a law enforcement agency that contains or has the potential to contain personal information that is not otherwise available to the public, unless consent is given by the individuals whose information is disclosed, there is statutory authority, or the law enforcement agency obtains a search warrant based on probable cause, or an emergency circumstance exists that qualifies as an exception to the warrant requirement as defined by law.
Division Administrators	Ensure Division employees do not subject photo or video images that incidentally show license plates or other potentially identifying information to software or other tools that digitize or “read” that information.
Division Administrators	Ensure Division employees understand and follow this passive electronic data collection policy.
Division Administrators	Promptly start investigation and take proper action if deviations from this policy are reported or suspected.
Employees	Comply with this policy and related procedures.
TDD Administrator Designee	Review the effectiveness of this data privacy policy and implementation actions at least every 3 years.

Anonymity

Responsibility	**Action**
Division Administrators/Employees	Ensure Division employees secure passive electronically collected data so individual user’s personal information is not known or remains confidential through the three scenarios of data collection and retention listed as follows: • The personal or sensitive information is stripped from the data when it is collected or it is cryptographically hashed or truncated in a manner that prevents re-discovery of the original data.

- Data is aggregated after it is collected so a pattern can be determined and personal information data is autonomous and therefore not able to be connected to an individual.
- The personal information that cannot be deleted through any other means is collected and retained in accordance with state law, federal law, this policy and confidentiality agreements.

Sharing of Passive Collected Data

Responsibility	Action
Division Administrators /Employees	Ensure that sharing passive electronic data with the general public, and publicly and privately held organizations complies with the Oregon Public Records Law and other applicable state or federal laws. When sharing passive electronic data that contains sensitive information outside of the Department, an agreement must be in place unless otherwise prescribed by law. The agreement (such as a contract, a service level agreement, or a dedicated data sharing agreement) should address the following: • The data that will be shared. • The specific authority for sharing the data. • The type of data being shared. • Access methods for the shared data. • Protection of the data in transport and at rest. • Storage and disposal of data no longer required. • Backup requirements of the data if applicable. • Other applicable data handling and retention requirements.
Division Administrators /Employees	Establish procedures in all relevant contracts that contractors working on ODOT's behalf follow this policy.