

ADJUSTMENTS TO THE PUBLIC RECORDS ACT TO ALLOW FOR ADVANCED TRANSPORTATION OPERATIONS AND MANAGEMENT

INTRODUCTION

The State of Washington's Public Records Act (PRA), passed as a ballot initiative in 1972, was designed to provide more transparency in the government decision-making process. That law also directly acknowledged that citizens have privacy rights that deserve protections. However, the current version of the PRA was not written to account for how new technology has changed the collection of data, how those data are used both for business applications and to manage the transportation system, and how those data can be used by unscrupulous individuals to harm the residents of the state.¹

Individuals provide substantial amounts of data with specific details about themselves to private transportation companies and others in connection with those individual's requests for services from transportation companies. Those who share their data often are unaware that this information may be released under the public records act when held by government agencies. Government agencies have a long history of coordinating and working with private transportation companies to manage traffic, provide adequate parking, and maintain safe and walkable communities.

To develop a remedy to these concerns, a series of engagement meetings took place with key public, private and non-profit stakeholders to understand their primary interests regarding data sharing and the Public Records Act. The PRA research team² determined where tension exists between the interests of stakeholder organizations, and even within stakeholder organizations. The amendment developed and refined through these stakeholder meetings was designed to address these tensions and has been well received by those stakeholders. While some stakeholder issues with public agency collection, use and sharing of data remain to be resolved, those issues must be addressed outside the PRA.

PROPOSED AMENDMENT

The suggested PRA amendment tries to balance the sometimes-competing data sharing views of different stakeholders. The primary change is to exempt individual movement and location data from mandated release by government agencies. The primary amendment to the PRA, within RCW 42.56.330, is as follows:

(4) Data collected, owned, used, or retained by any agency that includes an individual's name, account information or other financial information as defined in RCW 9.35.005, location, travel history, receipt of goods, or transportation transactions. Such data includes without limitation (i) information uniquely identifiable to a device, (ii) Global Positioning System (GPS) coordinates, (iii) media access control (MAC) addresses, (iv) Bluetooth identifiers, (v) wireless (Wi-Fi) networking data, or (vi) cellular network data.

(a) Such data may be disclosed if it is in aggregate form.

(b) Such data is not exempt from disclosure if it identifies an agency vehicle or agency employee acting within the scope of employment, unless exempt under RCW 42.56.230(7), RCW 42.56.250(9), RCW 42.56.240(13), or other law.

(c) The exemption in this paragraph (4) does not prevent the disclosure of reports or studies based in whole or in part on such data so long as exempted data is in aggregate form or is removed or redacted from the disclosed record.

The full amendment text also includes some clarifying definitions and clarifications. A copy of the suggested amendment and a short paper describing all issues highlighted in the stakeholder meetings are available upon request.

¹ An excellent paper on the ability to re-identify individuals from location data is "[Unique in the Crowd](#)" by Yves-Alexandre de Montjoye, et. al. (2013.)

² The Project Team consisted of the University of Washington, WSDOT, and Milligan Partners. Stakeholders included one or more representatives from 9 government agencies, 4 trade associations, 8 companies supplying transportation services, 4 non-profit advocacy groups, and 3 news organizations.

INTRODUCTION

The State of Washington’s Public Records Act (PRA) was originally passed as a ballot initiative in 1972 by a vote of the people. The legislation was designed to provide more transparency in the decision-making process at all levels of government. At the same time, the law also directly acknowledged that citizens have privacy rights that deserve protections.

However, the current version of the PRA was not written to account for how new technology has changed the collection of data, how those data are used both for business applications and to manage the transportation system, and how those data can be used by unscrupulous individuals to harm the residents of the state.¹

In an attempt to remedy some of these concerns, our team met with key public, private and non-profit stakeholders that operate in the State of Washington to understand their primary interests as they relate to data sharing and the Public Records Act. In particular, we were interested in determining where tension exists between the interests of stakeholder organizations, or even within stakeholder organizations. This outreach resulted in four key areas of interest, which we will discuss in detail in this report. These key areas of interest are as follows:

- I. Protecting individual privacy (Pg. 3)
- II. Protecting proprietary business information (Pg. 5)
- III. Maintaining open government (Pg. 7)
- IV. Sharing of data by government agencies when the PRA exempts that data from release (Pg. 9)

The suggested PRA amendment exempts individual movement and location data from automatic release by government agencies, and tries to balance the sometimes-competing views of different stakeholders. However, many of the stakeholder concerns detailed below touch on issues that are outside the scope of the PRA. Some of these issues include the amount of personal data collected by the government and the private sector, the types of data private companies share with the government, and the voluntary sharing of data by government agencies outside of the PRA process. When possible, we suggest legislative or regulatory avenues that might be better equipped to address these concerns.

¹ An excellent paper on the ability to re-identify individuals from location data is “[Unique in the Crowd](#)” by Yves-Alexandre de Montjoye, et. al. (2013.)

I. PROTECTING INDIVIDUAL PRIVACY

In the course of managing the transportation system, governments have a strong interest in using location and travel data that may be personally identifying. These data may be gathered by government agencies themselves or may be collected from private companies such as transportation network companies (TNCs). These data, if not adequately protected, could potentially reveal private and intimate details about individuals, jeopardizing their freedom to travel, compromising their freedom of association, and putting their safety at risk.

Summarized Stakeholder Concerns: Individual Privacy

1. Many companies, government agencies, and privacy advocates expressed concern that anonymized location data could easily be used to re-identify individuals with common data science tools unless the data were first aggregated.

The suggested PRA revision directly addresses this concern by exempting from release data that describe the location or movements of individuals or devices, as devices can often be associated with specific individuals (See Suggested Amendment to 42.56.330 Section 2(4)).

2. Most stakeholders generally agreed that the sharing of data in an aggregated format that prevents re-identification of individuals or the ability to reveal proprietary business information is appropriate. However, there wasn't a consensus regarding the level of aggregation needed to achieve this goal.

The suggested PRA revision states that aggregated data are releasable (See Suggested Amendment to 42.56.330 Section 2(4)(a)) Government agencies must "reasonably determine" the level of aggregation that will prevent re-identification (Section 2(4)).

The suggested PRA revision allows for the release of aggregated data while exempting unaggregated data that could be used to identify individuals or devices. The revision protects personally identifying information by setting minimum thresholds for aggregation before release.

3. Many TNCs stated that they would be more inclined to share data with the government for regulatory or research purposes if they knew their customer's information would be protected.

The suggested revisions directly address concerns regarding the dissemination of individualized data (See Suggested Amendment to 42.56.330 Section 2(4)). Note, however, that the PRA does not compel private companies to share data with government agencies. The decision to share data would need to be addressed outside of the PRA, either through regulatory or contractual requirements, or by voluntary decisions.

4. Some public agency representatives wondered if government-generated data that could be used to identify individual government employees would be exempt from the PRA disclosure, while

The proposed amendment exempts from release under the PRA data that describe the location or movements of individuals or devices, greatly limiting the potential reidentification of individuals

other stakeholders indicated that it was in the public interest to ensure the public could review the actions of agency employees while they were working.

The suggested PRA revision does not exempt the individualized data of government employees and vehicles, but it also does not affect existing PRA exemptions that protect government employee data (See Suggested Amendment to 42.56.330 Section 2(4)(b)).

5. Advocates for workers and marginalized populations expressed concern that these groups are disproportionately harmed by the release of individualized transportation data. At the same time, some of these organizations felt that marginalized groups and workers would benefit from the secure use of these data to address important equity concerns. In particular, they expressed concern that existing information asymmetries allow private companies to conceal information that could be useful in negotiating wage and working conditions.

The draft legislation addresses both of these concerns by preventing the required release of individually identifiable data to the public (See Suggested Amendment to 42.56.330 Section 2(4)), while permitting government agencies to collect, analyze, and review data for the purposes of transportation management and policy analysis.

While individually identifiable data are not releasable under the PRA, these data can be used by agencies to compute aggregate statistics which allow for transportation management and policy analysis, including addressing equity concerns.

6. Some media organizations and worker advocates expressed some doubt as to whether the current PRA language poses a significant risk to individual privacy, and expressed greater concern regarding government and corporate use of those data.

In addition, some privacy advocates were concerned that the suggested PRA amendment could unintentionally lead to an expansion of government data collection that threatens civil liberties and democracy and disproportionately harms marginalized and vulnerable communities.

The suggested PRA revision is premised on the idea that individualized data can be used to identify individuals and therefore should be shielded from indiscriminate public release as a precaution.

The suggested PRA revision does not address broader concerns about the collection of data by governments or corporations, including the impact of data collection on marginalized communities. Such concerns would be best addressed in a separate piece of privacy legislation (as examples, see the proposed Washington Privacy Act introduced in 2020, European Union's GDPR, California's CCPA, and Japan's "Act on the Protection of Personal Information" (Act No. 57 of 2003 as last amended in 2018)", among others.) Advocates and other stakeholders may consider using the suggested PRA revision to springboard discussions with legislators and the public on these critical additional privacy issues.

II. PROTECTING PROPRIETARY BUSINESS INFORMATION

Transportation data collected by government agencies from private businesses may contain proprietary business information about how those businesses operate. Unless this sensitive business information is exempted from public release, rival firms could potentially obtain it to the adverse impact of the data sharer.

Summarized Stakeholder Concerns: Proprietary Business Information

1. Many government agencies, TNCs and other mobility service providers acknowledged that companies would be more willing to share data with the government for regulatory, research, planning, and Mobility as a Service (MaaS)² systems, if they knew the data would be protected from public release.

The suggested PRA revision directly addresses some of these concerns by exempting from release data that describe the location or movements of individuals or devices, as these data can reveal proprietary business information about the operations of TNCs (See Suggested Amendment to 42.56.330 Section 2(4)).

2. TNCs, other mobility service providers, and privacy advocates generally agreed with the release of data to the public in an aggregated format that would prevent the re-identification of individuals or the exposure of proprietary business information. However, TNCs were concerned with the release of disaggregated information, such as transaction information, that could be used to reverse engineer pricing and other business models.

The draft legislation addresses this concern by requiring any data released be aggregated to a level at which it cannot be associated with an individual or individual transaction (See Suggested Amendment to 42.56.330 Section 2(4)).

3. There is an ongoing legal debate about what exactly constitutes proprietary business information (PBI). As a result, companies felt they have little assurance that courts will protect their data from release. The Washington Supreme Court has ruled that a company's trade secrets may be disclosed under the Public Records Act if the disclosure is in the public interest, giving private sector stakeholders little certainty regarding the privacy of their trade secrets.

The most sensitive business information is protected from release under the PRA, improving protections for proprietary business information.

² Mobility as a Service is the integration of various forms of transportation services into a single mobility service accessible on demand. For example, a smartphone application could connect a traveler with nearby transit, hail a ride share, or locate the nearest dockless scooter. For more information: see <https://maas-alliance.eu/homepage/what-is-maas/>

By exempting the release of non-aggregated movement and location data, the revision codifies the protection of the most sensitive proprietary business information or PBI (individual trip and transaction data) in state statute (See Suggested Amendment to 42.56.330 Section 2(4)).

4. Different modal operators in the TNC market felt that they were at a competitive disadvantage in comparison to other modes due to more onerous requirements for data sharing.

This concern is addressed in the draft legislation by requiring aggregation to a level at which personally identifiable information (PII) cannot be reidentified (See Suggested Amendment to 42.56.330 section 2(4)).

5. Some TNCs said they want advance notice of PRA requests so they can legally object to release of that data if they feel they might reveal PBI.

Currently, agencies may notify the subject of any Public Records Request before releasing data. The suggested amendment does not change this standard, and also exempts private mobility and location information from release. TNCs and local government agencies may make agreements or contracts around notification requirements in their data sharing agreements. Furthermore, The Public Records Act allows the subject of a Public Records Request to ask a court for an injunction if they believe the requested data is protected by an exemption to the PRA³.

6. Some TNCs said they want to ensure that Public Records Officers are adequately trained on what is and is not releasable under the PRA.

Public Records Officer training is not addressed in the suggested PRA revision. Instead, it is up to each government agency to appropriately train their staff on any changes to the PRA. However, the standards set forth in the suggested revision are written to ensure reasonable ease of application by most government employees

7. Non-profit advocates pointed out that the individualized data that companies consider PBI can in fact be powerful tools for evaluating and advancing equity.

The suggested PRA revision would address these concerns since it would allow governments to more easily collect individual trip and transaction information for the purposes of oversight or regulation (See 42.56.330 section 1(10)).

8. Media organizations expressed doubt that some TNC's would be interested in sharing data due to their desire to avoid further regulation.

The suggested PRA revision would exempt from public release any individualized data that TNC's share with the government. How much data TNC's are willing to share, or are required to share, is a matter of both business judgment and regulatory policy and is therefore outside the scope of the PRA.

³ Washington RCW 42.56.540

III. MAINTAINING OPEN GOVERNMENT

While exempting individualized location and travel information from public records release protects individual privacy and proprietary business information, it also limits the openness and transparency of state government. This section lists responses to some of the open government concerns raised by stakeholders

Summarized Stakeholder Concerns: Maintaining Open Government

1. Some government accountability advocates wanted to ensure that the PRA revision struck a balance between individual privacy and government accountability and transparency.

The suggested PRA revision endeavors to strike this balance by exempting the release of data that identify the location or movement of specific individuals or devices, but that allow release of aggregated data that do not contain PII and that limit the potential for release of PBI.

Additionally, under current law meta-data (data that describe the variables submitted) are subject to release under the PRA⁴. The suggested PRA revision does not affect the ability of the public to request meta-data that does not identify an individual. Doing so allows government accountability advocates to understand whether, and how, data in the hands of government agencies can be used to answer specific policy and accountability questions, without revealing personally identifying location information about Washington residents.

The amendment endeavors to balance government transparency and privacy by allowing release of aggregated statistics, but protecting individual location records

2. Media organizations and non-profit advocates expressed concern that public agencies would not make available aggregated data summaries that answered questions that the agency does not wish to see reported, or when insufficient resources prevent the agency from performing important studies.

Nothing in the suggested PRA Revision prevents an agency from disclosing data outside the PRA process to a qualified professional (such as a consultant, nonprofit entity, or educational institution that possesses the requisite qualifications for handling PII in a secure manner) to perform additional policy studies or review the process used in aggregating data. Any such sharing of PII would have to provide adequate protections against the further disclosure of the relevant data.

In addition, journalists and public advocates will still be able to compel release of meta-data, such as Data Dictionaries and database schema, that will allow those organizations to determine whether data in the hands of public agencies can answer questions they have about public policy or performance.

⁴ O’Neill v. City of Shoreline, 240 P.3d 1149, 1151 (Wash. 2010)

3. TNC representatives generally expressed concern about knowing what the government is using their data for, and how the data are being disseminated among government agencies.

The PRA does not regulate what data governments request from TNCs and how they use those data. These concerns would need to be addressed in a data sharing agreement between parties.

4. Advocates and researchers expressed a desire to access individualized data held by government agencies to run their own analyses.

There are no "permitted uses" within the PRA. There are data that must be released and data that are exempt from release under the PRA.

The suggested PRA revision prevents the compulsory release of PII and PBI associated with the detailed location data. However, nothing in the PRA or the revision prevents an agency from voluntarily disclosing data to a qualified professional to review the process used in aggregating those data or performing additional policy studies. A qualified professional could include a third-party consultant, nonprofit entity, or educational institution accepted by an agency as possessing the requisite qualifications for handling PII in a secure manner. Any such review would have to provide adequate protections against the further disclosure of the relevant data.

5. Some advocates were concerned that restricting access to individual-level data would reduce the public's access to important information about government decision making.

The suggested amendments are narrowly tailored so that they would only restrict access to data with PII or PBI. Nothing in our amendment would limit the ability of advocates to gain access to aggregated data or meta-data used to make government decisions.

IV. SHARING OF DATA BY GOVERNMENT AGENCIES WHEN THE PRA EXEMPTS THAT DATA FROM RELEASE

The suggested PRA revision exempts personally identifiable transportation data from compulsory release through the Public Records Act. However, the suggested revision does not prevent the voluntary release of exempt data by governments. This section details the ways governments may still decide to share personally identifiable information with other agencies and outside partners.

Summarized Stakeholder Concerns: Sharing of Data Exempted from Release

1. Many government agencies have a desire to acquire individualized transportation data for the purposes of better managing and regulating the transportation system, including for purposes of ensuring equitable mobility; some agency representatives stated that these data should not be shared outside of the compiling agency for any reason other than the original regulatory purpose. Others expressed an openness to sharing when accompanied by an appropriate level of control and a data sharing agreement.

The PRA only prevents compulsory release of data to the public via the PRA process. It does not prevent voluntary release of data. Government may still share PII or PBI data across agencies or externally, subject to relevant privacy laws and data sharing agreements.

2. Non-profit advocates expressed concern that marginalized groups are disproportionately harmed by the release or sharing of individualized transportation data, especially with law enforcement agencies.

The draft legislation partially addresses these concerns by preventing the compulsory release of individually identifiable data through the PRA (Section 2(4)). This includes the compulsory release of data through the PRA to a law enforcement agency. However, data could still be shared by government agencies either voluntarily or by court order (See 42.56.330 Section 5(b)). Strengthening agency data sharing policies, privacy laws and other legal protections could further safeguard the rights of individuals.

In addition, the suggested PRA revision could be amended to require that government agencies create a publicly available log that documents who they have shared data with and why those data were shared, every time they shared individual location or movement data with any outside party.

3. Some TNCs expressed concern that their data submitted for regulatory compliance could be shared with other governmental entities without their consent.

The draft legislation partially addresses these concerns by preventing the compulsory release of individually identifiable data through the PRA (See Suggested Amendment to 42.56.330 Section 2(4)). However, data could still be shared by government agencies outside of the PRA process. Strengthening agency data sharing policies and data sharing agreements could further protect PBI.

The amended PRA prevents compulsory release of data but does not prohibit voluntary sharing of data. Agreements or statutory changes outside of the PRA are needed to control voluntary sharing of data.

SUGGESTED PUBLIC RECORDS ACT LEGISLATION

1 **Amendment to 42.56.330.**

2 AN ACT Relating to the privacy of individualized travel,
3 location and transportation transaction information; amending
4 RCW 42.56.330.

5 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

6 **Sec. 1.** FINDINGS. The legislature finds that:

7 (1) Washington's public records act mandates robust disclosure
8 of public records, reflecting that the people of Washington
9 State do not yield their sovereignty to the agencies that serve
10 them.

11 (2) Washington residents value privacy as an essential element
12 of their individual freedom, and the Washington State
13 Constitution explicitly recognizes persons' rights to privacy in
14 Article I, section 7.

15 (3) Out of respect for Washington residents' constitutionally
16 protected privacy expectations, the legislature has repeatedly
17 amended the public records act to narrowly exempt data that, if
18 released, would violate individuals' privacy.

19 (4) Individuals provide substantial amounts of data with
20 specific details about themselves to private transportation
21 companies and others in connection with those individual's
22 requests for and receipt of services from transportation
23 companies. However, those who share their data may be unaware
24 that this information may be released under the public records
25 act if held by government agencies.

26 (5) Government agencies have a long history of coordinating and
27 working with private transportation companies to manage traffic,
28 provide adequate parking, and maintain safe and walkable
29 communities.

30 (6) In coordination with the private sector, government agencies
31 currently have access to individuals' travel and location data,
32 and the Washington Supreme Court recently determined in *Lyft*,

1 *Inc. v. City of Seattle* (2018) that this information may be
2 obtained through the public records act.

3 (7) The legislature finds that travel, location, and other
4 transportation data, if not adequately protected, could
5 potentially reveal private and intimate details about
6 individuals, implicating their freedom to travel, their freedom
7 of association, and putting their safety at risk.

8 (8) The Legislature also finds that location and other travel
9 data is uniquely likely to enable an observer to identify an
10 individual, even if other individually identifying data is
11 removed or anonymized.

12 (9) The legislature also finds the public derives profound
13 benefits from easy and convenient access to data, and encourages
14 government agencies to continue making data publicly available
15 in a manner that does not uniquely identify individuals or
16 implicate their freedom of movement and association.

17 (10) The Legislature intends to adjust the language in the
18 public records act to clarify how modern transportation data can
19 be collected and used while simultaneously protecting citizens'
20 rights to privacy, the ability of businesses to protect
21 proprietary business information from release to competitors,
22 and the need for transparency of the information being used for
23 public decisions.

24 (11) The legislature intends that exemptions to the public
25 records act provided in this act will enable the state's public
26 agencies and governmental jurisdictions to obtain and use a
27 variety of data, often collected by the private sector, that
28 describe the movement of individuals or vehicles, without being
29 required to release detailed data with information that could
30 compromise either the privacy of individuals or the proprietary
31 business information of companies.

32 **Sec. 2.** RCW 42.56.330 and 2017 c 333 s 6 are each amended to
33 read as follows:

34 The following information relating to public utilities and
35 transportation is exempt from disclosure under this chapter:

1 (1) Records filed with the utilities and transportation
2 commission or attorney general under
3 RCW 80.04.095 or 81.77.210 that a court has determined are
4 confidential under RCW 80.04.095 or 81.77.210;

5 (2) The addresses, telephone numbers, electronic contact
6 information, and customer-specific utility usage and billing
7 information in increments less than a billing cycle of the
8 customers of a public utility contained in the records or lists
9 held by the public utility of which they are customers, except
10 that this information may be released to the division of child
11 support or the agency or firm providing child support
12 enforcement for another state under Title IV-D of the federal
13 social security act, for the establishment, enforcement, or
14 modification of a support order;

15 (3) The names, residential addresses, residential telephone
16 numbers, and other individually identifiable records held by an
17 agency in relation to a vanpool, carpool, or other ride-sharing
18 program or service. Participants' names, general locations, and
19 point of contact may be disclosed to other persons who apply for
20 ride-matching services and who need that information in order to
21 identify potential riders or drivers with whom to share rides;

22 (4) Data collected, owned, used, or retained by any agency that
23 includes an individual's name, account information or other
24 financial information as defined in RCW 9.35.005, location,
25 travel history, receipt of goods, or transportation
26 transactions. Such data includes without limitation (i)
27 information uniquely identifiable to a device, (ii) Global
28 Positioning System (GPS) coordinates, (iii) media access control
29 (MAC) addresses, (iv) Bluetooth identifiers, (v) wireless (Wi-
30 Fi) networking data, or (vi) cellular network data.

31 (a) Such data may be disclosed if it is in aggregate form.

32 (b) Such data is not exempt from disclosure if it
33 identifies an agency vehicle or agency employee acting within
34 the scope of employment, unless exempt under RCW 42.56.230(7),
35 RCW 42.56.250(9), RCW 42.56.240(13), or other law.

1 (c) The exemption in this paragraph (4) does not prevent
2 the disclosure of reports or studies based in whole or in part
3 on such data so long as exempted data is in aggregate form or is
4 removed or redacted from the disclosed record.

5
6 As used in this paragraph (4):

7 "Transportation Transaction" means the use of an online
8 platform, cell phone or other mobile communications application
9 to locate, reserve, or transmit information relating to:

10 (i) the hailing or use of a commercial transportation
11 service that uses a digital network or software application
12 to connect passengers to drivers,

13 (ii) the use of public transit,

14 (iii) the rental of a self-operated vehicle including but
15 not limited to a motor vehicle, scooter, or bicycle; or

16 (iv) the payment of tolls, fees, or road user charges.

17 "Aggregate form" means a compilation of data, such as reports,
18 patterns, totals, aggregate statistics, or other combinations of
19 data, that an agency reasonably concludes does not identify the
20 name, account information, location, travel history, receipt of
21 goods, or transportation transactions of an individual person or
22 device.

23
24 By way of example: location data are considered "aggregate" if
25 they are released at the five-digit zip code, census block
26 group, or higher level of abstraction; Global Positioning System
27 (GPS) data, addresses, or other location information that locate
28 an individual or device with more specificity than a five-digit
29 zip code or census block group are not sufficiently aggregate
30 for public disclosure; data indicating time of day are
31 considered "aggregate" if they are released in increments of 15
32 minutes or greater.

33

1 Records that contain data unique to fewer than [eleven]
2 individuals or devices are considered to be in aggregate form if
3 the statistical information generated by those data does not
4 disclose the sample size but instead identifies the sample size
5 as "less than [eleven]."

7 "Account information" means username, email address, social
8 media profile, password, security code, driver's license number,
9 or financial information.

10 ((+4)) (5) The personally identifying information of
11 current or former participants or applicants in a paratransit or
12 other transit service operated for the benefit of persons with
13 disabilities or elderly persons;

14 ((+5)) (6) The personally identifying information of persons
15 who acquire and use transit passes or other fare payment media
16 including, but not limited to, stored value smart cards and
17 magnetic strip cards, transportation accounts, or other payment
18 systems, except that an agency may disclose personally
19 identifying information to a person, employer, educational
20 institution, or other entity that is responsible, in whole or in
21 part, for payment of the cost of acquiring or using a transit
22 pass or other fare payment media for the purpose of preventing
23 fraud. As used in this subsection, "personally identifying
24 information" includes acquisition or use information pertaining
25 to a specific, individual transit pass or fare payment media.

26 ▪ (a) Information regarding the acquisition or use of transit
27 passes or fare payment media may be disclosed in aggregate
28 form if the data does not contain any personally
29 identifying information.

30 ▪ (b) Personally identifying information may be released to
31 law enforcement agencies if the request is accompanied by a
32 court order;

33

34 ((+6)) (7) Any information obtained by governmental agencies
35 that is collected by the use of a motor carrier intelligent
36 transportation system or any comparable information equipment

1 attached to a truck, tractor, or trailer; however, the
2 information may be given to other governmental agencies or the
3 owners of the truck, tractor, or trailer from which the
4 information is obtained. As used in this subsection, "motor
5 carrier" has the same definition as provided in RCW 81.80.010;
6

7 ~~((+7))~~ (8) The personally identifying information of persons
8 who acquire and use transponders or other technology to
9 facilitate payment of tolls. This information may be disclosed
10 in aggregate form as long as the data does not contain any
11 personally identifying information. For these purposes aggregate
12 data may include the census tract of the account holder as long
13 as any individual personally identifying information is not
14 released. Personally identifying information may be released to
15 law enforcement agencies only for toll enforcement purposes.
16 Personally identifying information may be released to law
17 enforcement agencies for other purposes only if the request is
18 accompanied by a court order;
19

20 ~~((+8))~~ (9) The personally identifying information of persons
21 who acquire and use a driver's license or identicard that
22 includes a radio frequency identification chip or similar
23 technology to facilitate border crossing. This information may
24 be disclosed in aggregate form as long as the data does not
25 contain any personally identifying information. Personally
26 identifying information may be released to law enforcement
27 agencies only for United States customs and border protection
28 enforcement purposes. Personally identifying information may be
29 released to law enforcement agencies for other purposes only if
30 the request is accompanied by a court order; and
31

32 ~~((+9))~~ (10) Personally identifying information included in
33 safety complaints submitted under chapter 81.61 RCW.