OREGON SUNSHINE COMMITTEE

Standing Subcommittee for All Things

October 3, 2019

Reference materials attached:

1. Summary of phone conference between Eileen Eakins and Kathryn Helms, Chief Data Officer, State of Oregon;

2. Public Records Requests – Bulk Data talking points, from Ben Tate, Director, Oregon Longitudinal Data Collaborative, Office of Research and Data, Higher Education Coordinating Commission;

3. Summary of Oregon laws relating to private sector use/disclosure of personal information, from Department of Justice staff.

LAW OFFICES OF EILEEN EAKINS, LLC

ASSISTING LOCAL GOVERNMENTS SINCE 2006.

SUMMARY OF PHONE CONFERENCE[1]

With
Kathryn Darnall Helms
Chief Data Officer
State of Oregon – Office of the State CIO

October 2, 2019

Because Ms. Helms is unable to attend the meeting of the standing subcommittee of the Oregon Sunshine Committee scheduled for October 3, 2019, I spoke to her by telephone for about 30 minutes on October 1 about specific challenges posed or strategies used to respond to bulk data requests at the state level.

Ms. Helms explained that, like the Public Records Advocate position, the position of Chief Data Officer is relatively new (less than a year as of the date of this memo), and that processes at the state level are primarily ad hoc in nature due to the complexity of Oregon's Public Records Law.

The scope of work for Chief Data Officer position encompasses data governance and consistency among state agencies in facilitating the publication of open data. Key to this process are electronic storage methods that allow non-exempt data to be easily and efficiently located according to specific parameters set by the requester, and making level-one data dictionaries publicly available so requesters can locate data on their own and tailor their requests more narrowly to help limit high fees from requesting large amounts of data they may not need.

Specific challenges include:

- Cybersecurity and privacy risks posed by expanding public access to data
- Addressing or resolving questions about whether such things as data dictionaries are proprietary intellectual property

---

[1] AUTHOR'S NOTE: Kathryn Helms reviewed and approved this information on October 2, 2019, with the following clarifying note in her reply email:

I want to clarify that my position comes with a mandate to advocate for Open Data, which can be prioritized based upon public records requests, but I do not have any direct involvement in the public records process, so I can guide agencies but I may not always have a direct connection to how they're managing public records requests specifically.

4248 SW GALEWOOD STREET • LAKE OSWEGO, OREGON • 97035
PHONE: 503.607.0517 • EILEEN@EAKINSLLC.COM

- How to mandate that future purchases of electronic storage equipment for public agencies be made with dissemination of information in mind

We discussed the potential role of end-user agreements requiring the requester to use the data for specific approved purposes in exchange for greater access. Ms. Helms explained that the state already uses a variant of this agreement in the form of negotiated data-sharing contracts with certain research institutions. She acknowledged that use of this type of agreement could be expanded for certain specified parties, but that "you can't legislate intent" so the widespread use of such agreements probably isn't practical, at least without clear legislative direction.

When asked if there were specific areas that that would aid her work, she proposed the following:

- Clear guidance on when and how to apply the public interest balancing test
- Development of specific criteria for storage and transmission methods, particularly as they apply to bulk data requests
- Consolidation of the many exemptions in the Public Records Act into as few as possible so state agencies can more easily navigate which data may be publishable

Respectfully submitted,

Eileen G. Eakins
Subcommittee Chair

SUBMITTED BY:

Ben Tate (he/him/his)
Director, Oregon Longitudinal Data Collaborative
Office of Research and Data
HIGHER EDUCATION COORDINATING COMMISSION
www.oregon.gov/highered
Office 503-378-2764 | Cell 971-273-3837

October 2, 2019

Public Records Requests – Bulk Data

Overview – Below is the process I use when evaluating a public records request, especially one that encompasses a large amount of data. I lay out the key questions I use to determine what data can be shared, how difficult (technically) it is to fulfill the request, and to ensure that I understand the scope and timeline of the request.

Question 1 – How can we legally fulfill this request?

- Consideration 1 – What do existing data privacy laws (both state and federal) allow? Are specific data elements prohibited from being disclosed? Is there a specific situation that prohibits data form being shared (active legal case, etc.)?
- Consideration 2 – Overlap of existing laws – Often data being request is subject to multiple laws. Are there special considerations given for when this overlap of regulations occurs? Are there special circumstances that prohibit the combination of data where it wouldn't apply to data individually (would disclosing combined data allow identification of identities that would otherwise be protected?)
- Consideration 3 – Who owns the data being requested? Often data sharing agreements exist between agencies that allow data from Agency A to be stored in the system for Agency B. However, this data is not owned by Agency B and often cannot be directly disclosed.

Question 2 – How can we technically fulfill this request?

- Consideration 1 – Was the data system built with large data export functionality? From a technical perspective, is the exported data format difficult for modern systems to read? From a readability perspective, will the data be exported in a way that is usable?
- Consideration 2 – How far back does the request go? Are older records (especially those for closed files) housed within the data system or within an archived system? Does retrieving those records require a rebuild of an older system or an older version of the system? Was the data system upgraded recently? Was the data migrated to the new system or was it archived? Are scanned document involved that need to be manually reviewed?
- Consideration 3 – How many data fields are being requested? How many different applications or data tables within a single application are involved? Is there a key field linking these data

tables to allow the data to be exported in a way that maintains linkage across the tables? If the data comes from multiple systems is it possible to link the data in a meaningful way?

- Consideration 4 – Was the data system designed in a way to separate out confidential data or data that may need to be redacted? Or is it co-mingled with releasable data? (If the system design or business use of the system doesn't explicitly call out sensitive data to be recorded separately, it could require manual review and redaction by staff before disclosure.)
- Consideration 5 – Has the use of the data fields changed over time? Do the changes in business rules change the data being stored in the system? Is there documentation to help requestors understand the changes in data over time?

Question 3 – How can we fulfill this request in a timely manner?

- Consideration 1 – What is the scope of the request? Is the requestor open to considering alternations to scope based on the answers to technical questions above? Is a public data dictionary for the system available to allow the requestor to see what is available? How tight are the search criteria? If the initial data pull is too broad, can the search be refined?
- Consideration 2 – What is the timeline for the request? Is there a hard deadline? Does all the data need to be delivered at once or can there be incremental deliveries?
- Consideration 3 – What format does the data need to be delivered in? Can the default from the system be used or does that data need to converted into a separate format?

Use of Personal Information by Private Entities

Question Presented: Whether Oregon law places limits on what private entities can do with personal information (not including specialized data such as medical information, education records, and financial account information).

Short Answer: Oregon law imposes few restrictions on the disclosure of personal information by private actors. Although there are laws designed to protect such information from "unauthorized access" by third parties (e.g., ORS 646A.622), private entities are generally free to designate how personal information may be used and who is "authorized" to receive such information. Such matters are generally governed by the terms of consumer agreements or through an entity's user agreements or terms of use. Under ORS 646.607(12) it is an unlawful trade practice for a private entity to use such information in a manner materially inconsistent with its stated terms. Violations are subject to civil penalties of up to $25,000 per violation. The Oregon Consumer Information Protection Act also requires entities to notify consumers and the Attorney General of certain breaches of security (defined as unauthorized acquisition of computerized data), and authorizes civil penalties of up to $1,000 for failure to report.

Key Provisions of Oregon Consumer Information Protection Act (ORS 646A.600 to 646A.628):

1. 646A.602(11) defines "personal information"

2. 646A.604 provides notice of breach requirements, methods and contents of notification

3. 646A.606 to 646A.618 relate to security freezes on consumer reports in response to a data breach

4. 646A.622 requires covered entities to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information.

646A.602(11) **Definition of "personal information"**:

(a) A consumer's first name or first initial and last name in combination with any one or more of the following data elements:

(A) A consumer's Social Security number;
(B) A consumer's driver license number or state identification card number issued by the Department of Transportation;
(C) A consumer's passport number or other identification number issued by the United States;
(D) A consumer's financial account number, credit card number 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;
(E) Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction;
(F) A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or
(G) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.

(b) Any of the data elements or any combination of the data elements described in paragraph (a) of this subsection without the consumer's first name or first initial and last name if:

(A) Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and
(B) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

Additional Resources:

Congressional Research Service on federal data protection laws:
https://fas.org/sgp/crs/misc/R45631.pdf

Summary of State Data Breach Laws:
https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf

AG Notice on Data Breach Notification Requirements: https://www.doj.state.or.us/wp-content/uploads/2017/10/oregon_data_breach_reporting.pdf