Office of Privacy and Data Protection Performance Report

Office of Privacy and Data Protection
Dec. 1, 2020

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Table of Contents

Report Requirement

The Office of Privacy and Data Protection is required to prepare and submit this performance report to the legislature every four years under RCW 43.105.369(5). The report must include performance measures set in the RCW. These performance measures must include, but are not limited to, the following:

(a) The number of state agencies and employees who have participated in the annual privacy training;

(b) A report on the extent of the office of privacy and data protection's coordination with international and national experts in the fields of data privacy, data protection, and access equity;

(c) A report on the implementation of data protection measures by state agencies attributable in whole or in part to the office of privacy and data protection's coordination of efforts; and

(d) A report on consumer education efforts, including but not limited to the number of consumers educated through public outreach efforts, as indicated by how frequently educational documents were accessed, the office of privacy and data protection's participation in outreach events, and inquiries received back from consumers via telephone or other media.

Letter from the state Chief Privacy Officer

The Office of Privacy and Data Protection (OPDP) is committed to issues of data privacy, data protection and access equity. Since my appointment as state Chief Privacy Officer in January, we have worked hard to maintain and strengthen the state's role as a responsible custodian of personal information Washingtonians entrust to agencies and programs.

OPDP serves as a resource for state and local agencies, the Legislature and the Governor's Office on privacy issues. This has been especially critical during 2020 as society has come to rely on digital technology in new and unexpected ways during the COVID-19 pandemic.


Katy Ruckle, Chief Privacy Officer
Washington State

Due to this shift, recent initiatives have included connecting with a broader community of stakeholders including the Washington State Office of Cybersecurity and the IT security professionals who keep our systems and networks safe. Close collaboration between OPDP and the Office of Cybersecurity is essential to the data protection efforts of our state.

Other initiatives include holding monthly webinars on hot topics of privacy and data protection including COVID-19 contact tracing, data breach assessment, de-identification of records and the Public Records Act. We also completed the 2020 Privacy Assessment Survey of state agencies as required by law. Agencies continue to rate privacy as a high priority.

While I am proud of the work we've accomplished, there is still room for improvement as we seek to increase privacy program maturity across state government. To this end, OPDP has spent a significant amount of time drafting and finalizing the Washington State Agency Privacy Principles. Research of international guidelines, input from stakeholder agencies and outside experts helped shape these principles for Washington. We plan to use the principles as a foundation for building strong and lasting data governance frameworks for state agencies moving forward.

I firmly believe the state can play an important role in educating local government and the broader Washington community about measures that can help protect information and handle sensitive data responsibly. I look forward to continuing these efforts statewide.

Katy Ruckle

Katy Ruckle
Chief Privacy Officer

Privacy and OPDP background

Information privacy is an area of increasing concern for both Washington residents and public agencies.

For residents, concerns include the proliferation of data collection, aggregation by private industry and the constant news of data breaches. They also want improved reporting and visibility into data practices. A 2019 Pew Research study[1] found 81% of Americans believe they have little or no control over the data companies collect and that the potential risks of collection outweigh the benefits.

Government agencies themselves also maintain a significant amount of sensitive information needed to provide services and perform essential government functions. The same Pew study revealed a similar lack of trust in how the government handles personal information:

- 84% believe they have little or no control over what data the government collects.
- 66% believe the potential risks of collection outweigh the benefits.
- 78% have little or no understanding of what the government does with their information.

Those concerns are amplified by data breaches or inappropriate state practices and the public's distrust can interfere with the state's ability to perform important functions that benefit residents. It is vital that agencies continually strive to be trusted stewards of sensitive personal information.

With this backdrop the Legislature formally created the Office of Privacy and Data Protection (OPDP) in 2016. The primary purpose of OPDP is to be a central point of contact for state agencies on privacy and data protection matters. Essential OPDP functions include conducting privacy reviews and trainings, articulating privacy principles and best practices, and coordinating in the review of major state projects that involve personal information. Other key functions include disseminating best practices for local governments and performing consumer education.

Two people are tasked with performing these functions. Katy Ruckle, the state Chief Privacy Officer, began on January 1, 2020. She was joined by a new Privacy and Open Data Manager during the 2020 legislative session.

[1] https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Recent initiatives

Recent OPDP efforts have focused on expanding the volume of available resources on privacy and increasing engagement with public agencies. Examples of key initiatives this year include:

- Expanding and rebranding the existing Privacy Working Group into a new State Agency Privacy Forum (SAPF). The SAPF, which meets quarterly, is open to any agency that wants to participate and includes privacy, data sharing and cybersecurity experts.

- Hosting privacy webinars each month there is not a quarterly SAPF meeting. Topics have included data breach notification, facial recognition, contact tracing, de-identification, the intersection of privacy and the Public Records Act, and the Keep Washington Working Act. These webinars are recorded and available on the OPDP's webpage.

- Creating and distributing draft Washington State Agency Privacy Principles to state agencies during the summer, with the final version published in November 2020. The principles will help establish a common understanding to use when discussing, promoting and implementing privacy practices as a priority among state agencies.

- Launching a new OPDP website and Privacy Points, a monthly blog/newsletter, to help improve the distribution of privacy information and give additional access to OPDP trainings and presentations.

- Revamping the annual privacy assessment survey to gather additional information that will help determine the needs and maturity of privacy programs across the spectrum of state government.

- Developing a breach assessment form template that helps agencies determine if an incident is a breach that requires notification under Washington's breach notification law. This tool is also useful to local governments.

- Representing OPDP on several committees working on important initiatives in the state including the Bluetooth Exposure Notification Advisory Committee, Systems Technology and Data Security Subcommittee for the Washington State Autonomous Vehicle Workgroup, Washington All-Payer Claims Database Data Release Advisory Committee (DRAC), and the Open Data Advisory Group.

- In partnership with the Office of Cybersecurity, creating resources for safely using Wi-Fi and video conferencing during the pandemic. In addition, to increase accessibility, OPDP's *Tips for* safely *using public Wi-Fi* publication was translated into 35 languages spoken by communities across Washington.

Core Office of Privacy and Data Protection functions

OPDP serves as a central point of contact on privacy and data protection matters. RCW 43.105.369 includes seven duties for the OPDP:

State agency support:

1. Conduct an annual privacy review.
2. Conduct an annual training for agencies and employees.
3. Articulate privacy principles and best practices.
4. Coordinate data protection in cooperation with WaTech.
5. Participate in the review of major state agency projects involving personality identifiable information.

Local government support:

6. Develop and promote best practices, including training.

Consumer support:

7. Educate consumers about the use of personal information and measures to protect information.

State Agency Support

Privacy Review

The OPDP conducts an annual privacy assessment survey of state agencies. The number of agencies responding, the importance of privacy, and the maturity of privacy programs across state agencies has steadily increased over time. Specific details about the privacy assessment survey findings are included later in this report and the full report is posted on our website at https://watech.wa.gov/privacy/newsinformation.

Training

Training and education has been OPDP's focus since its inception. The office's staff has presented four times a month, on average, since 2017 to a variety of audiences.

Until the COVID-19 pandemic hit in the spring of 2020, most OPDP presentations and trainings took place with in-person audiences. Beginning in April 2020, the office shifted to a virtual model that allowed us to increase outreach to public agencies.

The office first expanded and rebranded the existing Privacy Working Group into a new State Agency Privacy Forum (SAPF). The SAPF, which meets quarterly, is open to any agency that wants to participate and includes privacy, data sharing, agency CIOS, and cybersecurity experts. This step was taken to accommodate the different ways that agencies staff privacy.

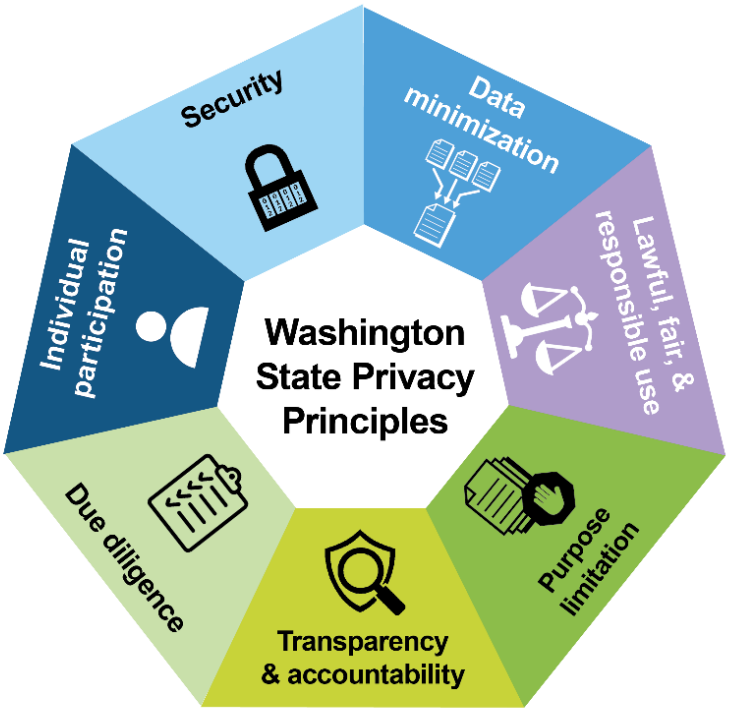
The OPDP also began hosting privacy webinars each month there is not a quarterly state agency privacy forum. Topics so far include:

- Washington's Data Breach Notification Law for State and Local Government.
- Washington's Approach to Regulating Facial Recognition.
- Contact Tracing in Washington State.
- Decoding De-identification for Public Agencies.
- Privacy and the Public Records Act.
- Keep Washington Working Act.

These sessions are attended, on average, by approximately 100 people across the state enterprise and are also archived and posted on office's website where they receive additional views by state and local government employees. Increased promotion of OPDP's work and an improved website presence has enabled the office to reach more state and local government audiences.

For example, the office was contacted in September by a county information security officer who viewed the data breach notification presentation on the OPDP website. He provided positive comments and asked for additional resources which we were able to provide. Several agencies also indicated in their responses to the annual privacy assessment that they appreciate the frequency of presentations and want them to keep coming. OPDP's goal is to increase outreach and training across the state and local government spectrum.

Privacy Principles



The foundation for modern privacy principles was formed decades ago. Since then, variations have been explicitly or implicitly included in virtually all significant privacy laws. They are in the Health Insurance Portability and Accountability Act (HIPAA) rules, the California Consumer Privacy Act and in Europe's General Data Protection Regulation. They are also recognized in standards for data privacy framework set by the Organization for Economic Co-operation and Development, the United Nations and several other international and national agencies including the Federal Trade Commission.

Although each of these variations has significant overlap, there is not a specific version uniformly recognized as authoritative. After extensive research and review, OPDP drafted the Washington State Agency Privacy Principles and distributed them to agencies for comment in July 2020. After consulting with agencies and incorporating stakeholder feedback, the principles were finalized in October 2020.

The finalized Washington State Agency Privacy Principles are:

- Lawful, fair, and responsible use.
- Data minimization.
- Purpose limitation.
- Transparency & accountability.
- Due diligence.
- Individual participation.
- Security.

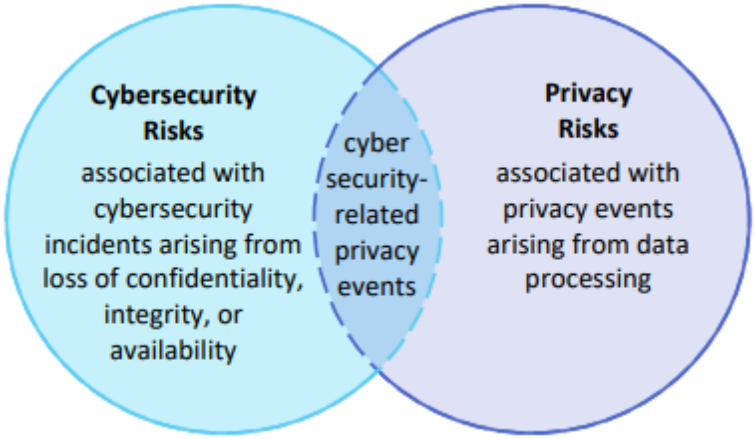
These principles are intended to be a high-level guide for agencies to follow when handling personal information about Washington residents. They foster best practices for agencies to collect, use and disclose personal information responsibly and in a fair and transparent way. Each principle is defined with a description of implementation. The principles are intended to be scalable and flexible depending on the agency and the type of information and laws that may apply to the data.

The principles also serve as a common language and framework for discussing privacy that OPDP can use when developing and distributing resources. Agencies can also use them internally to discuss and promote privacy. Adoption of the privacy principles by state agencies can build a stronger data protection framework and help establish public trust.

A copy of the finalized principles is included as an attachment to this report on page 17.

Coordinate data protection with WaTech

The Office of Data and Privacy Protection has also worked to align its initiatives with WaTech's state Office of Cybersecurity. Security is one of the Washington State Agency Privacy Principles because privacy practitioners know that without security there cannot be privacy. The National Institute of Science and Technology depicts the relationship of privacy and cybersecurity through this Venn diagram.



Our joint efforts with OCS have included OPDP's participation in the Chief Information Security Officers Council meetings, including cybersecurity and IT personnel in the State Agency Privacy Forum and other trainings, and the inclusion of privacy impact assessments as a part of the OCS Operational Plan. These privacy impact assessments will ensure privacy impacts are appropriately evaluated by agencies and incorporated as part of WaTech's review of major state agency projects involving personally identifiable information.

OPDP is also integrating its efforts with the Office of the Chief Information Officer. For example, the annual privacy assessment is part of the OCIO annual certification process for state agencies. This creates additional accountability for agencies to complete the assessment and avoids duplicative efforts. OPDP also participates with the OCIO team that reviews and scores decision packages that involve significant information technology investments. OCIO's review

helps ensure alignment with the Washington State Enterprise Technology Strategy, and OPDP's involvement ensures privacy impacts are considered.

Develop and promote best practices for local government

OPDP this year presented to both the Association of Washington Cities (AWC) and the Association of County and City Information Systems (ACCIS) on the state's updated data breach notification law. In addition, the office has been building relationships and offering assistance when contacted directly by county and city privacy professionals.

Specifically, the State and Local Government Breach Assessment Form is a tool intended to be used by any public entity in Washington that has experienced a potential breach incident. The form is created to align with Washington state's data breach notification law (RCW 42.56.590). Both state and local agencies can use the form as a tool to brand or adapt to their needs. The form was created be editable and flexible for agency use, but also include all of the elements required by law for a data breach assessment.

Most resources developed for state agencies are also applicable for local agencies. OPDP's efforts to record and post trainings online makes them available for everyone. The office expects to increase local government participation as its visibility grows through OPDP's Privacy Community listserv.

Consumer support

OPDP's first few years concentrated on consumer privacy issues. Early on the office created a consumer *Privacy Guide for Washington Citizens*, which was distributed to libraries, senior centers and other venues. OPDP also leveraged resources offered by the federal government and distributed privacy and digital protection guides from the Federal Trade Commission while partnering with other similar outreach by state agencies, such as the Department of Financial Institutions.

In response to the Coronavirus, and with the coordinated launch of hundreds of drive-in WiFi hotspots across Washington, OPDP created *Tips for safely using public Wi-Fi.* The information was translated into 35 languages spoken by communities across Washington. Our office, in conjunction with OCS, also released instructions about video conferencing best practices.

In June 2020, OPDP launched an updated website to offer news and information, consumer resources, government and agency resources and background on the Office of Privacy and Data Protection. In addition, the office set up a subscription listserv that anyone can use to sign up for alerts and updates from the office. This includes the Privacy Points blog issued monthly about tips, initiatives, and topical privacy developments our office is monitoring.

When possible, OPDP uses relationships to leverage its limited resources and meet consumers where they are. For example, OPDP has an open data partnership with the Washington State Library that helps OPDP distribute privacy resources to librarians around the state. OPDP has also participated in presentations with librarian professional associations to increase privacy awareness. Because people use libraries to seek information on a wide range of topics, including consumer protection and privacy, using this "teach the teacher" model has the potential to reach far more people than OPDP could reach on its own.

Privacy Assessment Survey findings

RCW 43.105.369 requires OPDP to conduct an annual privacy review of agency practices. The results help OPDP measure privacy maturity across state agencies and develop resources and trainings where they are most needed. The goal is to establish an understanding of current practices, not to measure compliance with specific laws or a specific set of standards. Agency functions and privacy requirements vary. What is a best practice for one agency may not apply to another.

Since the first assessment in 2016, the number of agencies that respond has steadily grown. The survey is sent to 88 agencies and 74 responded this year, more than ever before. In 2019, 65 agencies responded, and 58 responded in 2016.

This year, 61 agencies reported they maintain personal information and indicated that privacy is a significant priority. Two-thirds reported that the importance of strong privacy controls had increased over the last biennium. No agencies reported that privacy has become less important.

Agency recognition of the importance of privacy is well founded given public attitudes towards the government's use of data, and the types of personal information agencies maintain. Agencies often collect information that goes far beyond names and contact information. For example, this year 48 agencies reported collecting social security numbers, 37 collect demographics information, 35 collect medical information and 22 collect immigration or citizenship information.

Responses confirm agencies are taking steps to protect personal information. Twenty-three agencies, 38% of those responding, reported having a specific person designated to handle policy and handle privacy questions. For nine of those agencies the designated person's primary function is privacy and related functions. Last year, just 13 agencies reported having a designated privacy officer.

Forty-five agencies have formal internal privacy policies and 42 agencies have completed or are in the process of completing a data map or inventory.

Even with this progress, the assessment revealed opportunities for improvement by agencies and OPDP. As awareness and concern about privacy continues to increase, many agencies are looking to improve their privacy practices. The level of maturity varies. Some are developing practices for the first time while others are turning privacy policies into privacy programs or are expanding existing privacy programs.

All agencies are looking for guidance and assistance. Dedicating resources that allow the OPDP to conduct additional outreach and create additional resources will fill an identified gap for WaTech customers and help ensure appropriate best practices to protect Washington residents' information.

For specific conclusions and recommendations, please see the *2020 Privacy Assessment Report* posted on our website at https://watech.wa.gov/privacy/newsinformation.

Performance measures

By its authorizing statute, the Office of Privacy and Data Protection must establish performance measures. In its 2017 report to the Legislature, the OPDP proposed six performance measures related to:

- Public agency training.
- Consumer outreach.
- State coverage of consumer outreach.
- Adoption of the privacy modeling tool.
- Open data.
- Broadband access.

Theme	Training	Outreach	Coverage	Privacy Modeling	Open Data	Broadband
Theory	With training, agency staff can improve the management of citizens' data	Citizen awareness will increase as more people and communities are exposed to in person and online outreach	Statewide awareness requires statewide appearances in trusted venues	Tools and policies developed by tech and legal thought leaders can spot privacy issues before they become liabilities or attractive targets	Affirmative publication of open data within existing resources requires planning at the agency level and statewide coordination	Broadband is local; communities that plan collaboratively for broadband stand a better chance of landing resources or seeing new deployment
Measure	Number of government employees trained	Impressions from events and publications	Number of communities where staff have presented	Utilization of the tool	Agencies planning for Open Data	Map of communities planning for broadband
Method	Sum of recorded attendance at OPDP training events	Sum of attendees at presentation events, plus sum of website visits, plus sum of estimated readers of earned media	Map of training, research or outreach event locations	Number of times the modeling tool is used (hits on results page)	Number of agencies with a published Open Data plan	Number of engagements with NTIA CCI tool, plus number of comprehensive plans addressing broadband, plus number of grant applications for federal funds from WA companies/ communities
Frequency	Recorded monthly	Recorded monthly	Recorded monthly	Recorded monthly	Recorded quarterly	Recorded annually
Period	Reported annually	Reported annually	Reported annually	Reported monthly	Reported annually	Reported every 4 years
Type	Activity	Outcome	Outcome	Activity	Output	Output
+Baseline	780	70000	6	100	20	3
Target	1425	85000	20	1000	30	6
Change	83%	21%	233%	900%	50%	100%

+Baseline numbers were set in 2017 based on 2016 data.

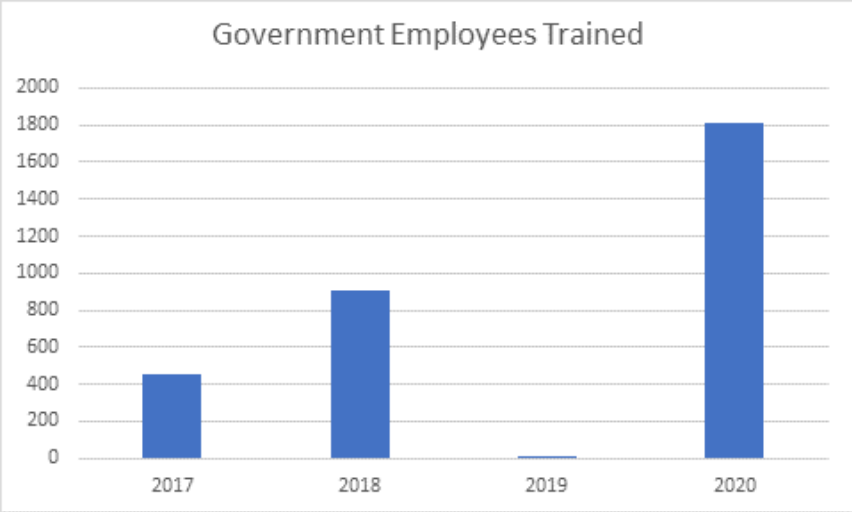
Of the six measures described in the chart above, the OPDP is unable to report on adoption of the privacy modeling tool and broadband access.

The privacy modeling tool was created based on grant funds. When the grant ran out, the tool was decommissioned because there were not resources to keep the application updated, making it a security vulnerability.

Broadband access was an optional piece of the OPDP's work based on existing resources that became redundant with the creation of a centralized state broadband office. While OPDP still has a strong commitment to digital equity and increased broadband access, our coordination with the Department of Commerce is now to support its efforts.

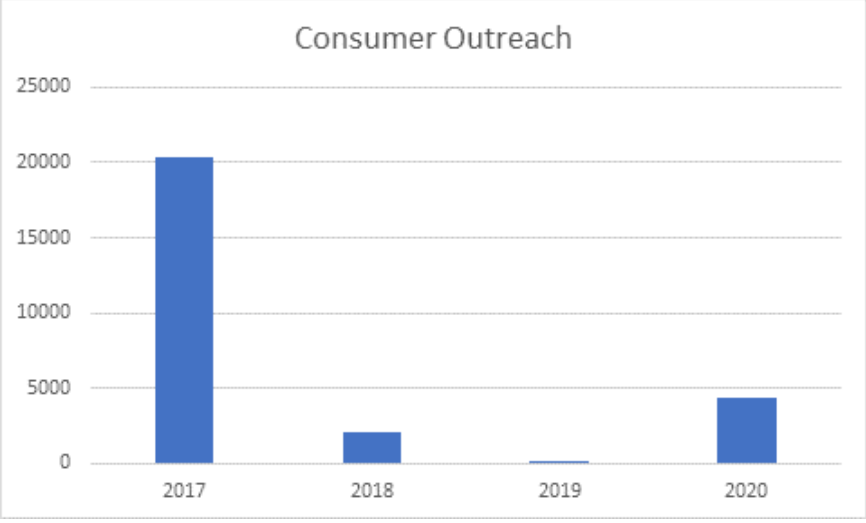
Based on the four remaining measures that OPDP can report on, the data reflects the following:

Training



Training of government employees has been our focus this year and our numbers reflect that. The office is proud of what was accomplished in this metric given the challenges of the pandemic. OPDP worked hard creating content and collaborating with others to present on timely and relevant privacy issues for government employees.

Outreach



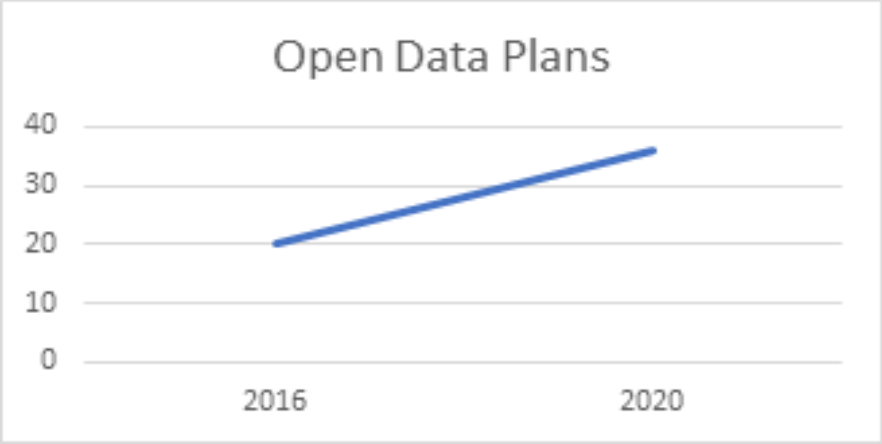
Consumer outreach has been a challenge. Given OPDP's limited resources, and the growing need for outreach to state and local government, significant in-person contact with residents has not been feasible. Past comparisons are also problematic because metrics used in previous OPDP reports combined in-person contacts with webpage hits on a legacy website that changed to a new platform this year. Previous numbers cannot be directly compared to today's efforts. OPDP will start from a new baseline this year.

Coverage

2017	2018	2019	2020
Olympia	Olympia	Olympia	Olympia
Seattle	Everett	Seattle	Virtual
Spokane	Bellevue	Pullman	
Clarkston	Richland		
Lacey	Anacortes		
Burien	Pullman		
Kirkland	Tumwater		
Port Hadlock	Seattle		
Vashon Island	Bremerton		
Tumwater			
Lake Forest Park			
11	**9**	**3**	**2**

This metric set in 2016 was based on ability to travel throughout the state to reach a broad variety of communities. Unfortunately, this was not possible in 2020 due to the pandemic. OPDP proposes revising this metric. It is unlikely, even after the COVID-19 crisis has passed, that travel for business will be as prevalent as it once was.

Open Data



Open data has expanded in the state since 2016 and 36 agencies now have open data plans. There are additional agencies that publish open data but do not have a formal plan. OPDP has taken steps, such as adding open data to the OCIO annual certification and entering a partnership with the Washington State Library, that make the outlook for additional growth promising.

Given the difficulty of following the metrics set in 2016 - which are not feasible within existing resources or match current initiatives and priorities - OPDP proposes going forward with the metrics in its authorizing statute, RCW 43.105.369(5), and will continue to develop additional metrics that better align with current priorities.

Priorities and initiatives

Based on the Privacy Assessment Survey results and building off of the momentum OPDP has created in the past year around privacy, we are working to launch new privacy initiatives around targeted outreach to state agencies. This will include supporting more mature privacy programs built on the foundation of the Washington State Agency Privacy Principles and incorporating the use of privacy impact assessments.

Specific initiatives include:

- Creating a privacy framework, including recommended policies and processes, to implement Washington State Agency Privacy Principles across all state agencies and to support the creation of individual agency privacy programs.
- Develop a tool and associated processes and procedures to perform privacy impact assessments on major state agency IT projects that involve personally identifiable information.
- Develop generally applicable training modules that can be used by all agencies.

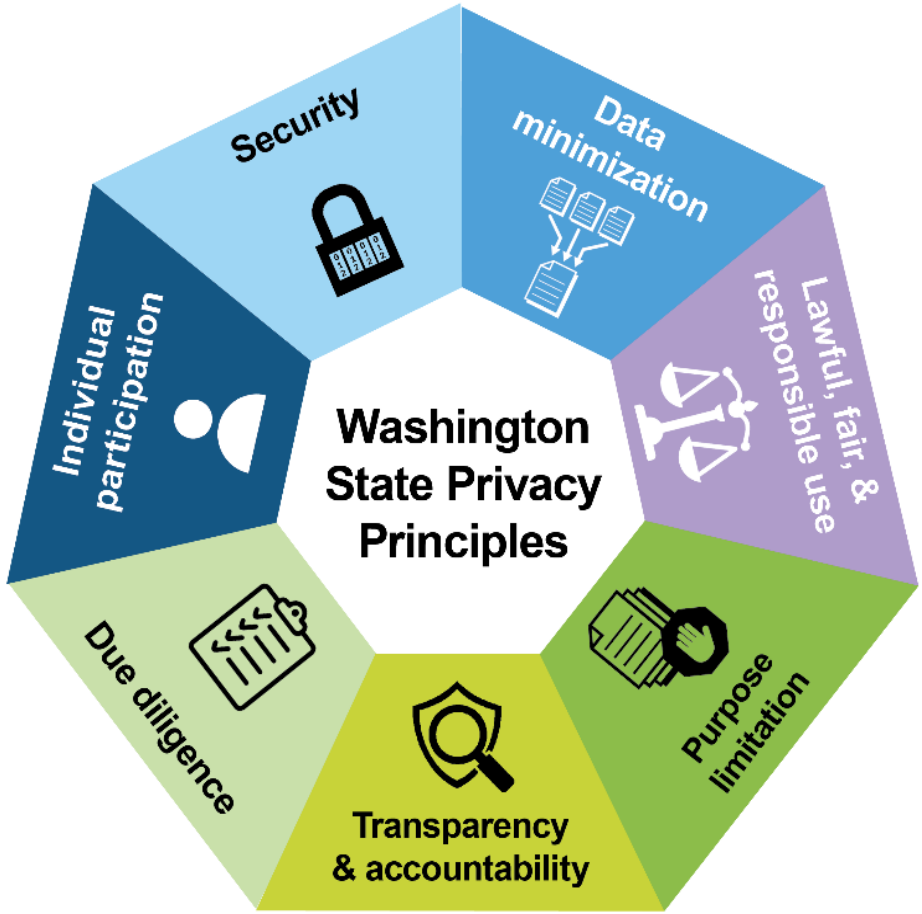
Strategic data governance is central to state agencies. It is critical to build trust in government now, given the state's increasing shift to digital solutions that hold sensitive personal information. Without trust in the government to handle data responsibly, important government activities like public health cannot be effective. The responsible use of data drives innovation and yields broad societal benefits. The reverse is also true. The unregulated and unauthorized use and disclosure of personal information and the resulting loss of privacy can have devastating impacts on residents. Negative consequences from mishandling personal information range from financial fraud, identity theft, and unnecessary costs to personal time and finances, to the destruction of property, harassment, reputational damage, emotional distress, and even physical harm.

Further, the COVID-19 pandemic has surfaced additional privacy issues related to the handling of citizen data and the importance of data privacy. As such, OPDP seeks to increase the adoption of privacy best practices across agencies. Federal and state legislation regarding compliance with sound privacy principles is being considered now and state agencies will receive more scrutiny on data management practices and protection of Washington resident's personally identifiable information. Continued investment in privacy and data protection will ensure the state is better prepared to handle privacy issues in the near term and build trust with the public in the years to come.

Attachment 1: Washington State Agency Privacy Principles

Purpose Statement

The government performs a variety of functions that require personal information. Public agencies have an obligation to handle personal information about Washington residents responsibly and in a fair and transparent way. The purpose of this document is to articulate fundamental privacy principles to guide agency practices and establish public trust. *See* RCW 43.105.369(3)(c).



PRIVACY PRINCIPLES		
Principle		**Implementation**
LAWFUL, FAIR, AND RESPONSIBLE USE	Collection, use, and disclosure is: • Based on legal authority; • Not deceptive; • Not discriminatory or harmful; and • Relevant and reasonably necessary for legitimate purposes.	• Only collect, use, and disclose information with appropriate legal authority. • Collect, use, and disclose information fairly, meaning at a minimum that processing is not deceptive or unduly harmful. • Collect, use, and disclose information responsibly and ethically. This includes taking steps to ensure information gathered is accurate and correcting information that is not. • Collecting, using and disclosing information in a lawful, fair and responsible way includes considering stricter standards when handling information about vulnerable populations and persons at risk. It also includes using stricter standards for particularly sensitive information. Potential impacts should be evaluated holistically. Information that does not appear especially sensitive on its own can become highly sensitive when combined with other available information. It can also become highly sensitive when viewed in context, which may require considering cultural, geographic, religious or political circumstances.
DATA MINIMIZATION	The minimum amount of information is collected, used, or disclosed to accomplish the stated purpose for collecting the information.	• Collect only the minimum amount of information needed to accomplish a specific purpose. • Minimize data use and disclosure by only allowing access to the minimum amount of information by the minimum number of people or organizations to accomplish a specific purpose. This includes utilizing de-identified or anonymous information when possible. Retain information only for the length of time that is necessary for its original purpose and applicable retention requirements.
PURPOSE LIMITATION	The reasons for gathering information are identified before it is collected. Use and disclosure is limited to what is reasonably necessary in relation to the specific reasons the information was collected.	Specifically state the reasons for collecting information. Unless a person provides consent, the information should not be used or disclosed for purposes that are not reasonably necessary to, or compatible with, the original purpose for collecting the information. Examples of compatible purposes include public archiving, research, or disclosures required by law.

TRANSPARENCY & ACCOUNTABILITY	Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with and under what circumstances. Accountability means being responsible for following data privacy laws and principles.	• Provide notice that is clear, honest and open about what information is collected, how it is used, and who it is shared with. When information is inappropriately used or disclosed, give timely notice to affected individuals. • Ensure accountability for adherence to these principles, any applicable privacy laws, and the public's expectations for the appropriate use of personal information. Accountability includes creating and maintaining policies and other records to demonstrate compliance and appropriate information handling. It also includes processes for monitoring or auditing, receiving and responding to complaints, and redress for harmed individuals.
DUE DILIGENCE	Taking reasonable steps and exercising care before and after entering into an agreement or arrangement with a third party that includes sharing personal information.	Exercise due diligence when sharing information with third parties. Appropriate due diligence will vary based on the circumstances, but may include: • Ensuring authority for the recipient to receive the information. • Evaluating whether sharing is consistent with the original purpose of collecting the information. • Requiring the third party to adhere to the same data use and security standards as the agency, including agency policies, these principles and applicable privacy laws. • Verifying and monitoring the third party's security and privacy practices.
INDIVIDUAL PARTICIPATION	Give people control of their information when possible.	Involve people in the collection and management of their personal information whenever practicable and consistent with the government functions being performed. Individual participation may include accessible processes to: • Provide, revoke or manage consent. • Opt-out or restrict collection or use. • Access information. • Request corrections to inaccurate information. • Learn who information has been shared with. • Timely response to requests for information.
SECURITY	Appropriate administrative, technical, and physical security practices to protect the confidentiality, integrity, availability and control of personal information.	Establish, implement and maintain reasonable security controls. Cybersecurity and non-technical controls must be appropriate to the amount and type of personal information being protected. Determining which security practices are reasonable includes considering what technology is available, the cost of implementation and assessment of risk.