WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Washington State
Office of Privacy and Data Protection

WACO Presentation
May 9, 2022

Background – path to privacy

- Admitted to WSBA 2005
- Started with state in 2006
- Contracts/procurement
- Healthcare
  - Dept of Social and Health Services
  - Largest state agency – 17,000 employees
  - Three hospitals
  - Implemented privacy program at DSHS to comply with HIPAA

Office of Privacy and Data Protection (OPDP)

- Executive Order 16-01
- RCW 43.105.369
- OPDP is in the Office of the Chief Information Officer
- State Office of Cybersecurity is also appointed by the Chief Information Officer

O P D P

OPDP Duties in Law

- Serve as a central point-of-contact for state agencies on policy matters involving data privacy and data protection
- Serve as a resource to local governments and the public on data privacy and protection concerns
- Conduct an annual state privacy review
- Conduct an annual privacy training for state agencies and employees
- Articulate privacy principles and best practices
- Coordinate data protection in cooperation with state agencies
- Review of major state agency projects involving PII
- Promote best practices for the collection and storage of PII
- Educate consumers about the use of PII on mobile and digital networks
- Legislative Reports on Metrics

O P D P

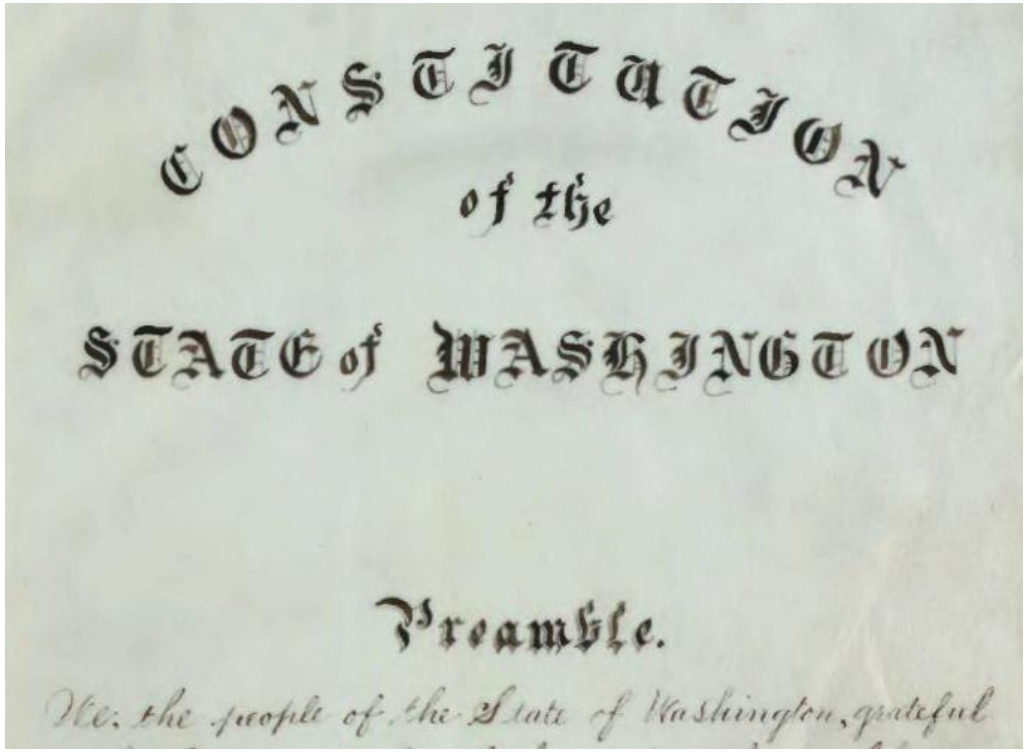
OPDP Duties in Law

- Serve as a central point-of-contact for state agencies on policy matters involving data privacy and data protection
- Serve as a resource to local governments and the public on data privacy and protection concerns
- Conduct an annual state privacy review
- Conduct an annual privacy training for state agencies and employees
- Articulate privacy principles and best practices
- Coordinate data protection in cooperation with state agencies
- Review of major state agency projects involving PII
- Promote best practices for the collection and storage of PII
- Educate consumers about the use of PII on mobile and digital networks
- Legislative Reports on Metrics

OPDP

Why Privacy Principles?

Privacy is important.



What is Privacy?

Communications Privacy

Territorial Privacy

Bodily Privacy

Information Privacy

OPDP

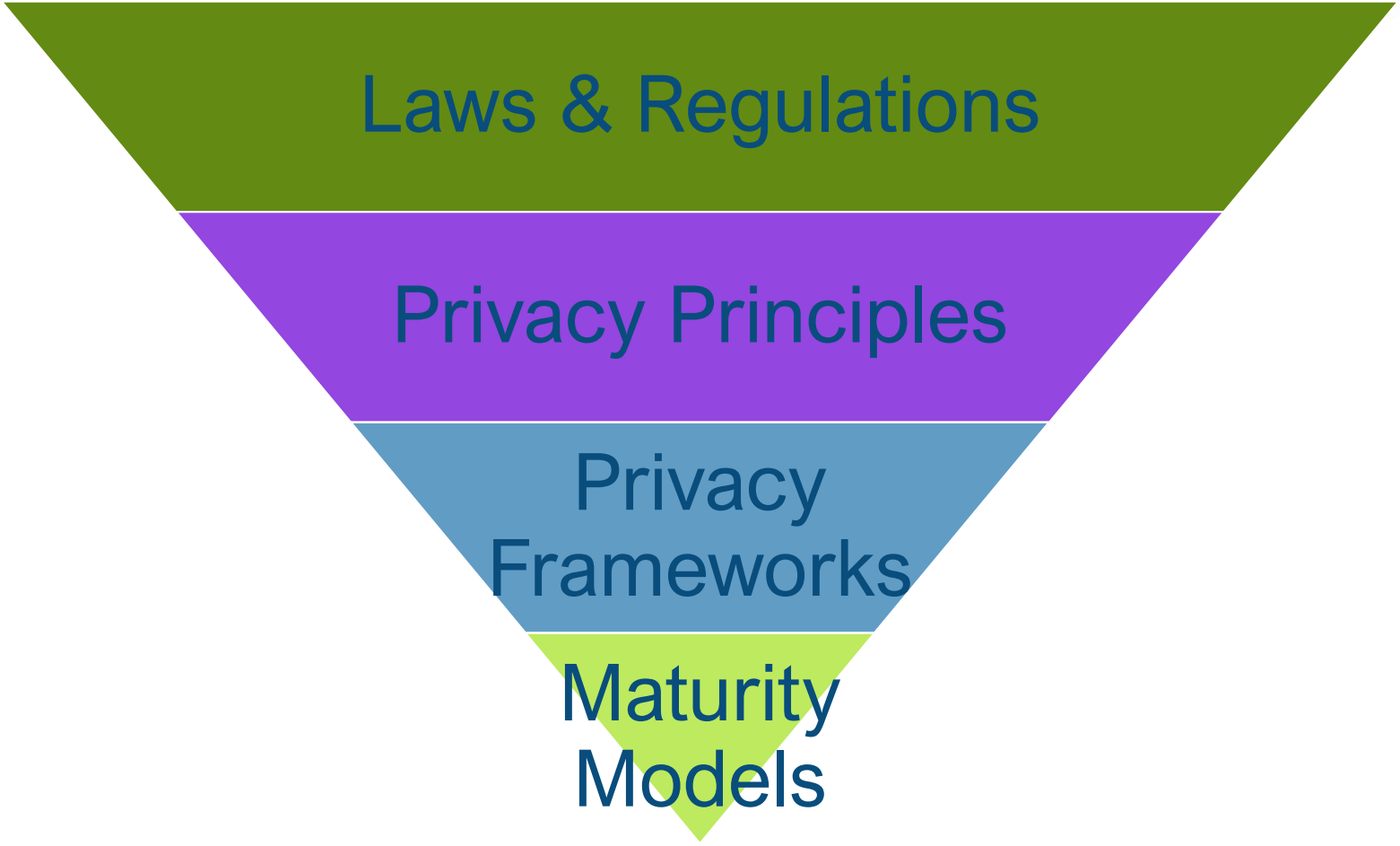
What is Privacy?

Communications Privacy

Territorial Privacy

Bodily Privacy

Information Privacy

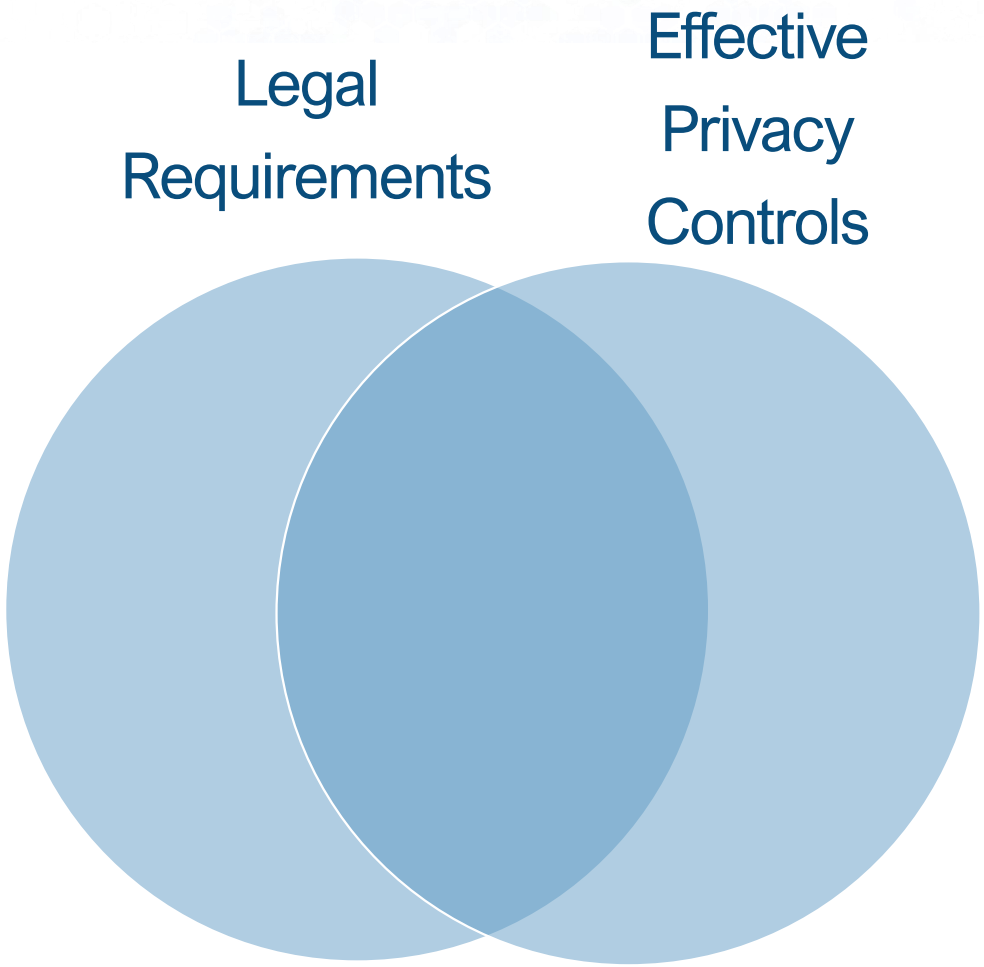


Effective Privacy and Data Protection

Laws and Regulations

Gaps may exist where laws:

- Do not establish strong enough protections to meet people's expectations
- Contemplate changes in technology and business practices
- Account for an organization's specific mission or cultural context



Privacy Principles Background

Inclusion in Privacy Laws

- Privacy Act of 1974
- General Data Protection Regulation (GDPR)
- Fair Credit Reporting Act (FCRA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Children's Online Privacy Protection Act (COPPA)
- California Consumer Protection Act (CCPA)

What's an organization to do?

- No complete consensus on principles
- No alignment between laws
- No wide applicability to all entities

Primary OPDP Functions

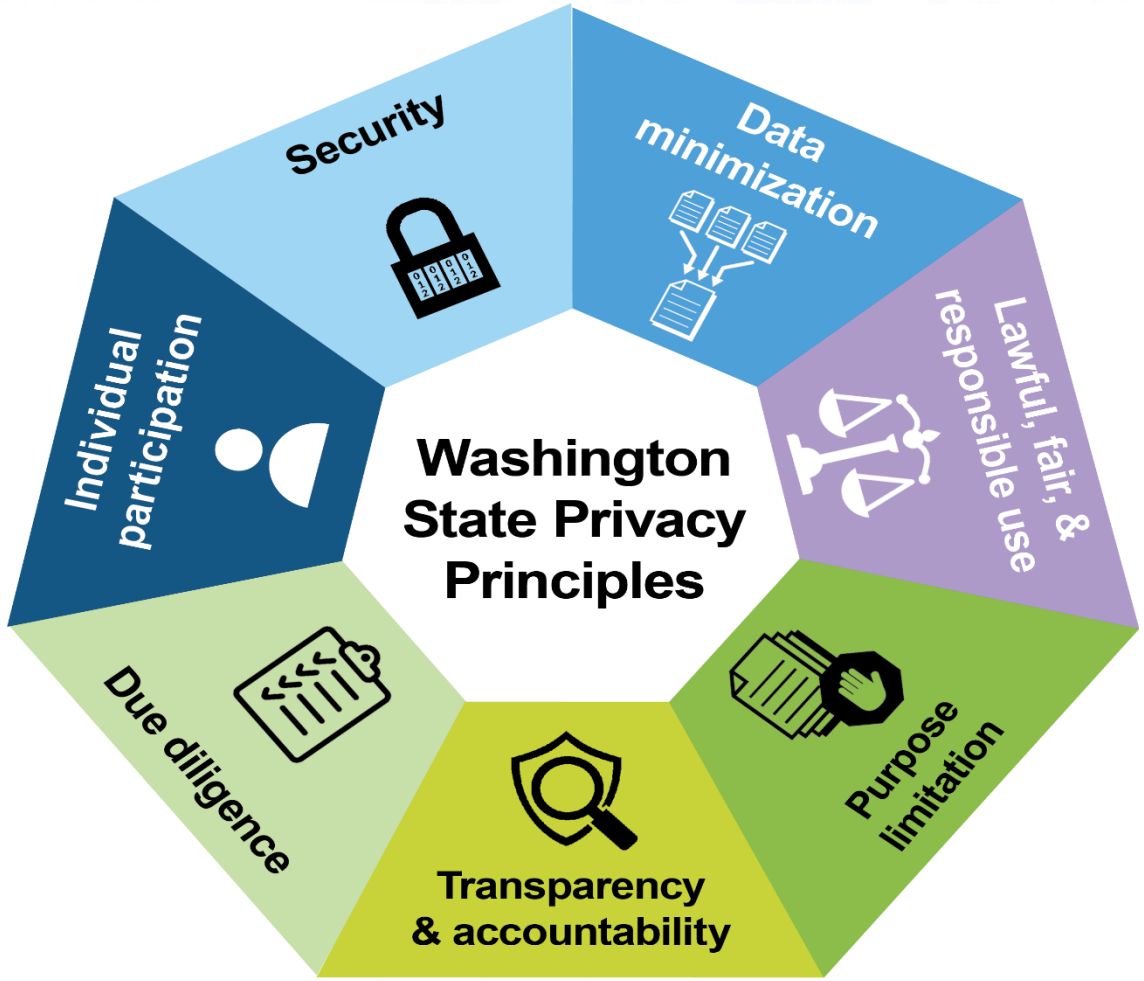
"The primary duties of the office of privacy and data protection with respect to state agencies are:

. . . .

(c) To articulate privacy principles and best practices. . ."

RCW 43.105.369(3).

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



Principles and Risk Management

❖ LAWFUL, FAIR, AND RESPONSIBLE USE

Collection and use is:

- Based on legal authority;
- Not deceptive;
- Not discriminatory or harmful; and
- Relevant and reasonably necessary for legitimate purposes

LAWFUL, FAIR, AND RESPONSIBLE USE

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Implementation

- Only collect and use information with appropriate legal authority.
- Collect and use information fairly, meaning at a minimum that processing is not deceptive or unduly harmful.
- Collect and use information responsibly and ethically. This includes taking steps to ensure information gathered is accurate and correcting information that is not.
- Collecting and using 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.

Risk mitigation

- Ensures collection, use, and disclosure of sensitive data is based on legal authority – e.g. evaluate what laws allow you to collect, use and share information. This means find the law and cite it.
- Think about data that can be used discriminatorily. E.g. Geolocation data on its own may not seem sensitive but when paired with other data can be very sensitive/population based (religious communities) (needle exchanges)
- Provides guidance making ethical decisions to navigate risk in gray, unregulated areas like AI, automated decision making

❖ DATA MINIMIZATION

The minimum amount of information is collected, used, or shared to accomplish the stated purpose for collecting the information.

DATA MINIMIZATION

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Implementation

- 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.

Risk Mitigation

- Less data means less risk
  - How so?
    - Less to breach
    - Less to hack/ransomware
    - Less to protect
    - Less to search and produce for public records
    - Less data collection can translate to better data quality and integrity

❖ 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.

PURPOSE LIMITATION

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Implementation

- Specifically state the reasons for collecting information.
- Unless a person provides consent, the information should not be used or shared 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.

Risk Mitigation

- Forces you to be deliberate and think about what you are collecting
- Avoids data scope creep
- Avoids over collection of data
- Accountability
- Reduces liability - legitimacy
- Privacy by design/privacy by default principles

❖ TRANSPARENCY & ACCOUNTABILITY

- Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with under what circumstances.
- Accountability means being responsible and answerable for following data privacy laws and principles.

TRANSPARENCY & ACCOUNTABILITY

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Implementation

- 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.

Risk Mitigation

- "Sunshine is the best disinfectant" ☺
- Transparency also includes "plain language." Being clear about your intentions with data lessens the risk of confusion, deception, complaints.
- Accountability holds entities and employees to the standards set forth in transparent data policies. Everyone more likely to follow clear processes and procedures.
- Sets clear expectations for organizations, staff, public.

❖ 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.

Implementation

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 data use and security practices

Risk Mitigation

- Requires research/thoughtfulness before handing over data to third parties (this includes those in authority)
- Good contracts! (examples: indemnification, insurance, cybersecurity, limited lability, governing law, termination, warranty, pass through data security requirements, secure destruction of data, etc.)
- Monitor/audit – System and Organization Controls (SOC)
- Reputation/reviews

❖ INDIVIDUAL PARTICIPATION

Give people control of their information when possible.

INDIVIDUAL PARTICIPATION

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Implementation

- 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 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

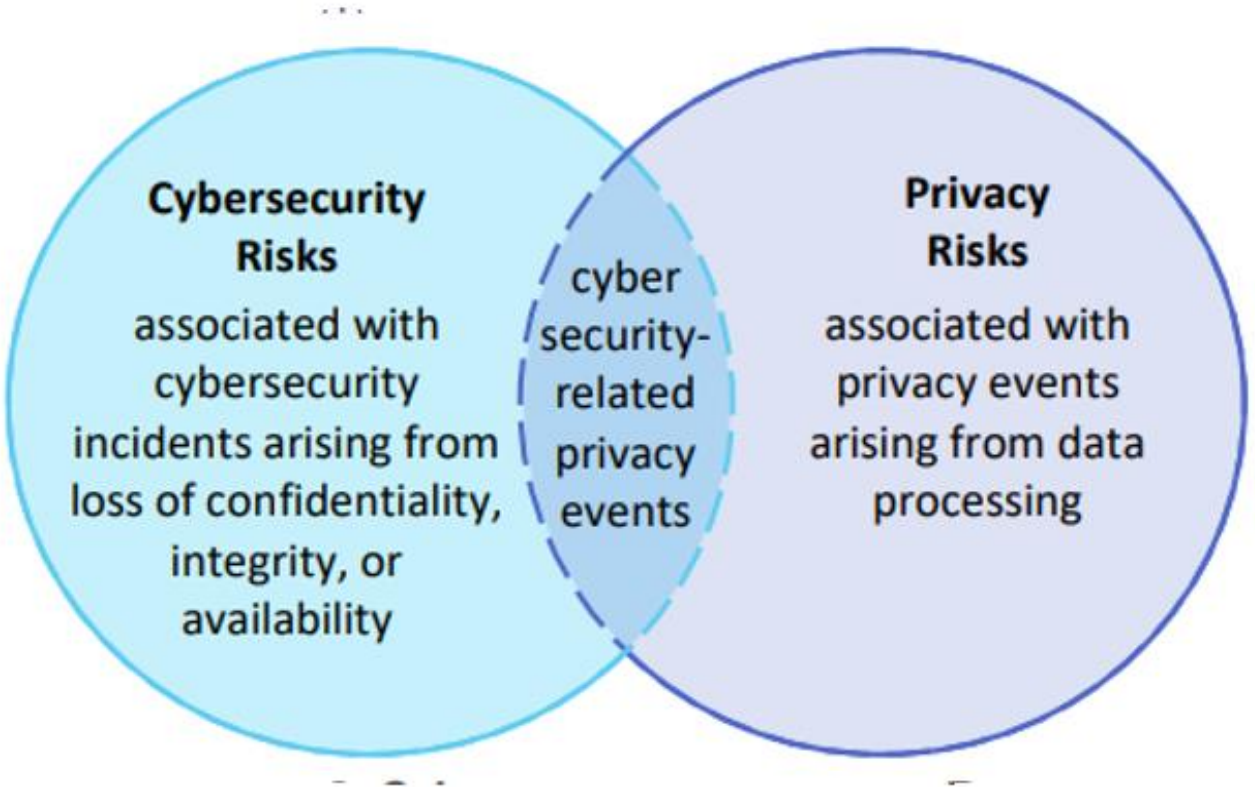
Risk Mitigation

- Creates records of informed consent and authorization
- Allows individuals some control over their data
- Provides direction to those handling data – e.g. clear restrictions or sharing allowances
- Ensures more accurate, high-quality data (which reduces business risk of bad decisions based on bad data)
- Revocation processes – "as easy to revoke as it is to consent"

❖ SECURITY

Appropriate administrative, technical, and physical security practices to protect the confidentiality, integrity, and accessibility of personal information.

Cybersecurity Relationship to Privacy



Implementation

- 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.

Risk Mitigation

- "Make the secure thing the easy thing"
- Secure data is protected data
- Protect against data breaches
  - Network infiltration; exfiltration of data
- Protect against ransomware
- Identify, detect, address vulnerabilities
- Internet/endpoint/cloud/application security

Just ask yourself does the adoption of _____ [fill in the blank privacy principle] reduce risk?

- Does the adoption of lawful, fair, and responsible data management reduce risk?
- Does the adoption of data minimization practices reduce risk?
- Does the adoption of transparent and accountable data management reduce risk?
- Does due diligence in selection of who and how you share your data with third parties reduce risk?
- Does allowing for individual participation in the data collection, use, and sharing process reduce risk?
- Does robust security for systems holding sensitive information reduce risk?

OPDP

Building a Privacy Program

Privacy Program Development

Identify roles within your organization that are central to data management.

- Legal
- Risk
- IT
- Security
- Records (retention, management, public)
- Compliance
- Others?

Ask?

Does your agency have an identified privacy officer?

- ❑Yes
- ❑No
- ❑Partial

Does your agency have an incident response plan?

- ❑Yes
- ❑No
- ❑Under development

Privacy is Interdisciplinary

- Look at your [data] incident response plan
- Current data handling policies
  - Who would you report a data incident to?
  - Within how much time? A day? A week?
- Training on data handling and confidentiality
- Nondisclosure Agreements
- Privacy Principles

Program Development

- Look at the positions you already have
- Look at the policies you already have
- Identify what information you need to protect
- Build a community within those resources
  - Regular meetings
  - Regular trainings
  - Build the culture
  - Build the expertise
- Use Foundational Principles

Conduct Training

Privacy Training and Communications

- Recorded webinars that provide more detail on specific privacy topics
  - Data Breach Law in Washington
  - Regulating Facial Recognition in Washington
  - Decoding Deidentification
  - Keep WA Working Act
  - Reducing Risk with Data Classification
  - SB 5432 Implementation
  - Privacy Impact Assessments
  - Privacy Notices

Legislative Work

Legislative Work

- Testify in legislative committees
- Participate in bill drafting
- Meet with Governor's office and elected officials on privacy legislation
- Track and update state agencies and Technology Services Board on bills relevant to privacy

OPDP

2022 Privacy Legislation

Last session we tracked 43 bills:

- **Privacy Rights and Protection bills**
- **Public Records bills**
- **AI and Facial Recognition**
- **State agency impact bills**
- **Misc: Broadband/Equity data/health sys transparency**

ESSB 5432 – Concerning cybersecurity and data sharing in Washington state government

- Data governance report
- Data sharing agreements
- OCS creation in statute
- Catalog of services
- Incident response
- Independent security assessment

Section 4 – Cybersecurity, Privacy and Data Sharing Agreements Best Practices Report

- Report Highlights - A two-page summary of the Privacy and Cybersecurity Best Practices key findings and recommendations.
- Privacy and Cybersecurity Best Practices Report – Full report from the collaboration of the Office of Cybersecurity, Office of Privacy and Data Protection, and the Attorney General's Office.
- Data Sharing Agreement Implementation Guide – Guidance intended to help agencies successfully implement appropriate data sharing agreements (DSAs) to protect confidential information

https://watech.wa.gov/Privacy

O P D P

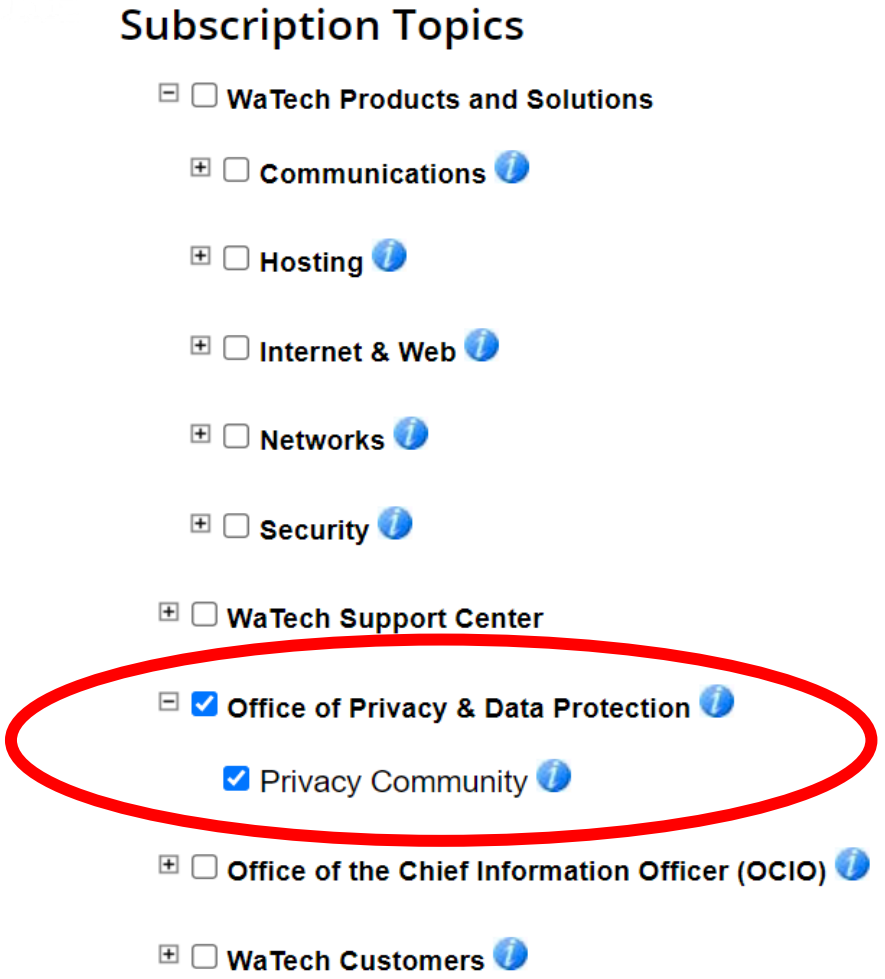
Privacy Training and Communications

Privacy Points – Monthly blog on events, initiatives, legislative updates, and other current privacy topics

Privacy.wa.gov

Subscribe for alerts & updates

How to subscribe



Thank you!

privacy@watech.wa.gov