WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Privacy Notices

Office of Privacy and Data Protection
April 28, 2022

Overview of Today's Webinar

- Privacy Notices importance and relevance (laws, legislation, required)
- What is the difference between a Privacy Notice and Privacy Policy?
- Privacy Notices relationship to Privacy Principles
- What should be included in a Privacy Notice?
- Privacy Notice Debate
- Privacy Notice Reminders

Privacy Notices importance and relevance

Recent Legislation

- Bills requiring privacy notices for state agencies
  - HB 1127 - Protecting the privacy and security of COVID-19 health data
  - HB 1552 - Concerning personal data collected by state agencies.
- People's Privacy Act – required Commerce to do model privacy policies
  - HB 1433
  - "Within six months of enactment, the Washington state department of commerce shall establish a standardized short-form privacy notice…"
- Consumer data privacy bills –
  - SB 5062

    "Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes…"

Recent Legislation

HB 1127 (2021) (vetoed) Protecting the privacy and security of COVID-19 health data collected by entities other than public health agencies, health care providers, and health care facilities.

A covered organization shall provide to an individual a privacy policy that describes, at a minimum:

(i) The covered organization's data retention and data security policies and practices for COVID-19 health data;

(ii) How and for what purposes the covered organization collects, uses, and discloses COVID-19 health data

(iii) The recipients to whom the covered organization discloses COVID-19 health data and the purpose of disclosure for each recipient; and

(iv) How an individual may exercise their rights under this chapter.

Recent Legislation

HB 1552 - Concerning personal data collected by state agencies

(1) A state agency must be transparent and accountable for its processing of personal data by making available to state residents and property owners a **privacy notice** that includes:

- The categories of personal data collected by the state agency;
- The categories of personal data that the state agency shares with 3rd parties and purposes for which that data is shared;
- The categories of 3rd parties, if any, with whom the state agency shares personal data.
- "Processing" means collection, storage, alteration, retrieval, use, disclosure, or dissemination.

HB 1552 (2021 & 2022)

WaTech Washington Technology Solutions
Washington's Consolidated Technology Services Agency

NEW SECTION. **Sec. 3.** A new section is added to chapter 43.105 RCW to read as follows:

(1) A state agency must be transparent and accountable for its processing of personal data by making available to state residents and property owners a privacy notice that includes:

(a) The categories of personal data collected by the state agency;

(b) The categories of personal data that the state agency shares with third parties, if any, and the purposes for which that data is shared; and

(c) The categories of third parties, if any, with whom the state agency shares personal data.

(2) As used in this section:

(a) "Personal data" has the same meaning as defined in section 2 of this act.

(b) "Processing" means any operation or set of operations that is performed on personal data or sets of personal data, such as collection, storage, alteration, retrieval, use, disclosure, or dissemination.

OPDP

Sectoral Privacy Laws

HIPAA - Health Insurance Portability and Accountability Act (Health care)

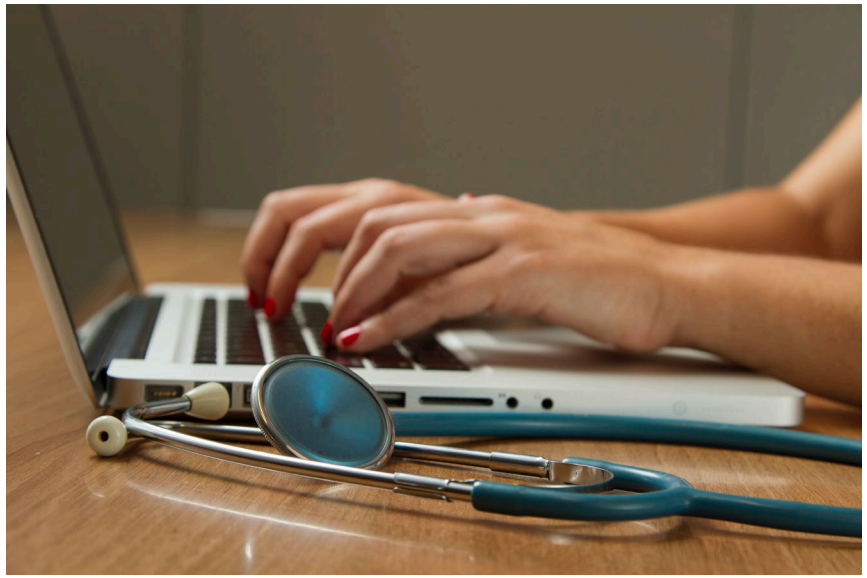
GLBA – Gramm-Leach-Bliley Act (Financial)

FERPA – Family Educational Rights and Privacy Act (Education)

HIPAA Notice of Privacy Practices

Notice must describe in plain language:

- The organization's legal requirements to maintain confidentiality and provide notice of breaches
- Uses and disclosures allowed without written authorization
- Uses and disclosures that require written authorization
- How to exercise individual participation rights
- How to file a complaint
- Who to contact for more information



GLBA Privacy Notice

- Categories of information collected
- Categories of information disclosed
- Categories of affiliates and nonaffiliated third parties to whom the institution may disclose information
- Policies and practices with respect to the treatment of former customers' information
- Categories of information disclosed to nonaffiliated third parties that perform services for the institution or functions on the institution's behalf and categories of third parties with whom the institution has contracted
- An explanation of the opt out right and methods for opting out
- Any opt out notices that the institution must provide under the Fair Credit Reporting Act
- Policies and practices for protecting the security and confidentiality of information
- A statement that the institution makes disclosures to other nonaffiliated third parties for everyday business purposes as permitted by law

FERPA – Annual Notification of Rights

- Right to inspect and review student's education records
- Right to request an amendment to the records
- Right to provide written consent before school disclosed PII
- Right to file a complaint with US Dept of Education (Student Privacy Policy Office)

Executive Order 16-01

JAY INSLEE
Governor

STATE OF WASHINGTON
OFFICE OF THE GOVERNOR
P.O. Box 40002 • Olympia, Washington 98504-0002 • (360) 902-4111 • www.governor.wa.gov

EXECUTIVE ORDER 16-01

PRIVACY PROTECTION AND TRANSPARENCY IN STATE GOVERNMENT
"MODERNIZING STATE AGENCY PRIVACY PROTECTION"

5. Update Privacy Policies. State agencies shall continually review and update their privacy policies to match current information collection and retention procedures. The updated policies should be *prominently displayed on each agency's website home page* and on any other page where personal information is collected, and/or viewable.

What is the difference between a Privacy Notice and Privacy Policy?

Privacy Notice

- Comprehensive notice that explains how an agency collects, uses, shares and manages personal information.

Website Privacy Notice

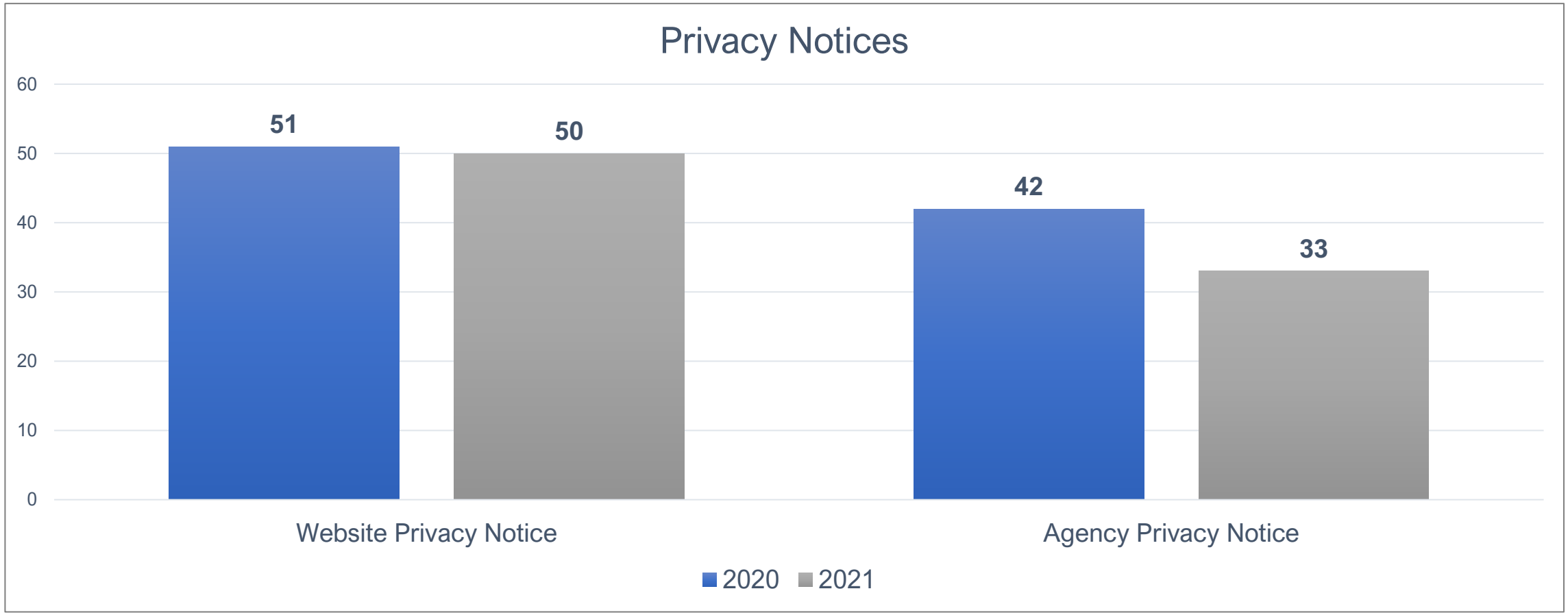
- Limited notice that explains what information is collected when you visit a website, and how that information is used, shared and managed.

Privacy Policy

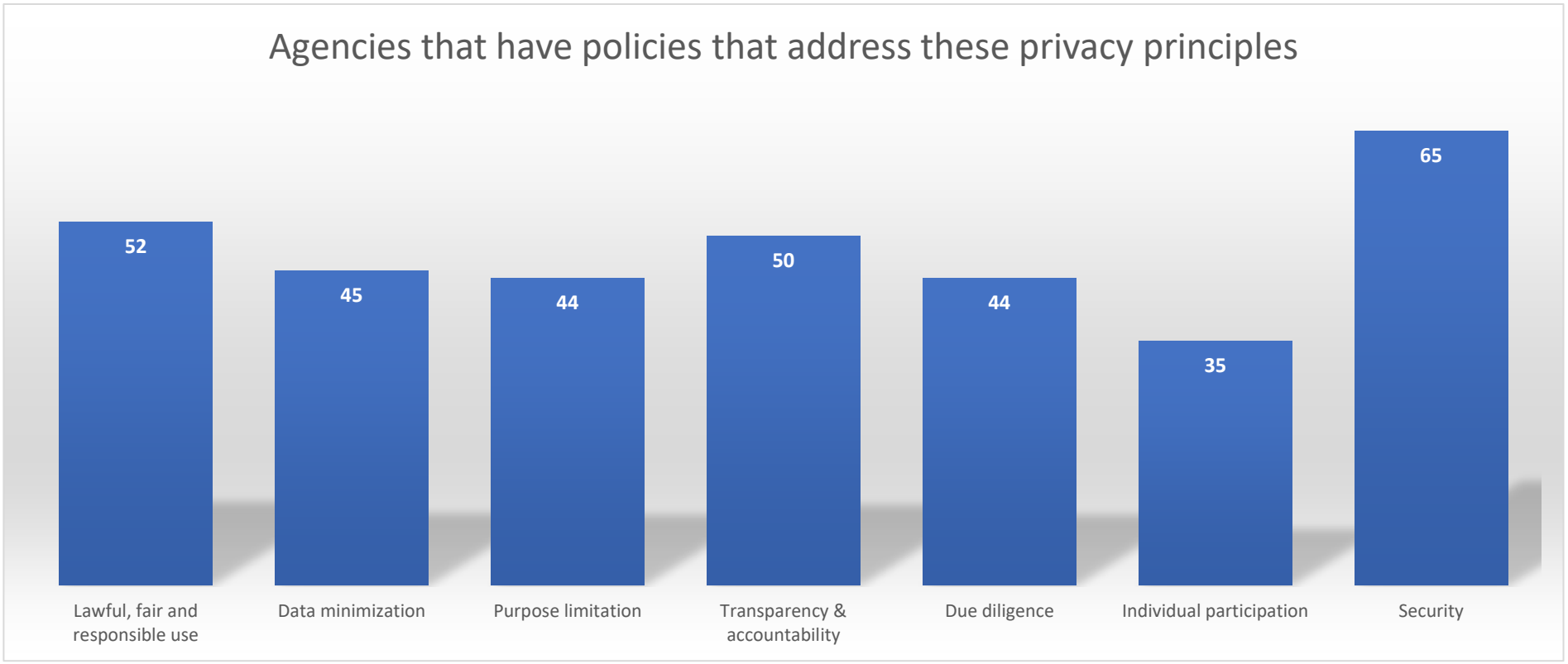
- Internal documentation of an agency's commitment to how it collects, uses, shares and manages personal information, and the associated standards and expectations for staff.

	Privacy Notice	Website Privacy Notice	Privacy Policy
Aliases	Privacy Statement, Privacy Policy, Notice of Privacy Practices	Cookie Notice, Security Notice, Privacy Notice, Privacy Statement, Privacy Policy	Privacy Plan, Privacy Code of Conduct, Privacy Practices
Associated principle	Transparency	Transparency	Accountability
Audience	External	External	Internal

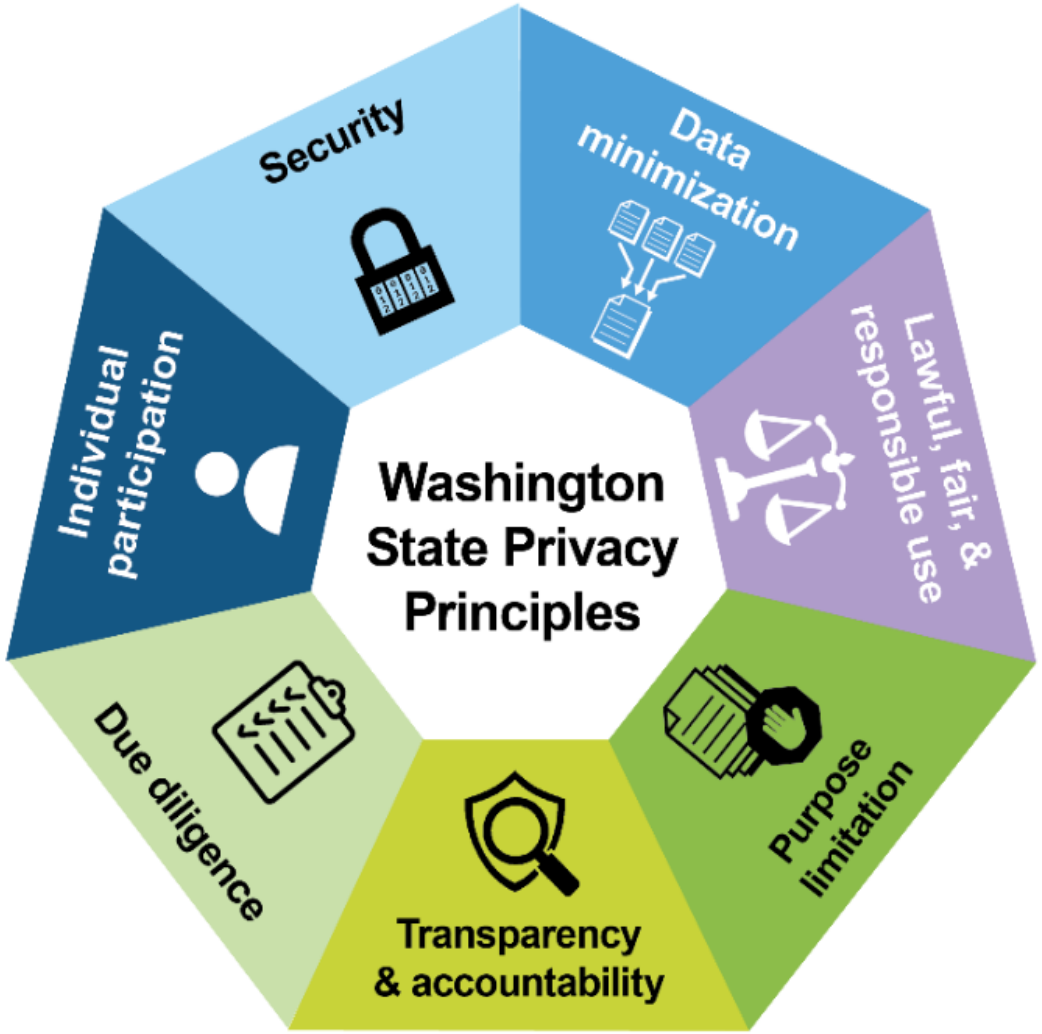
Transparency



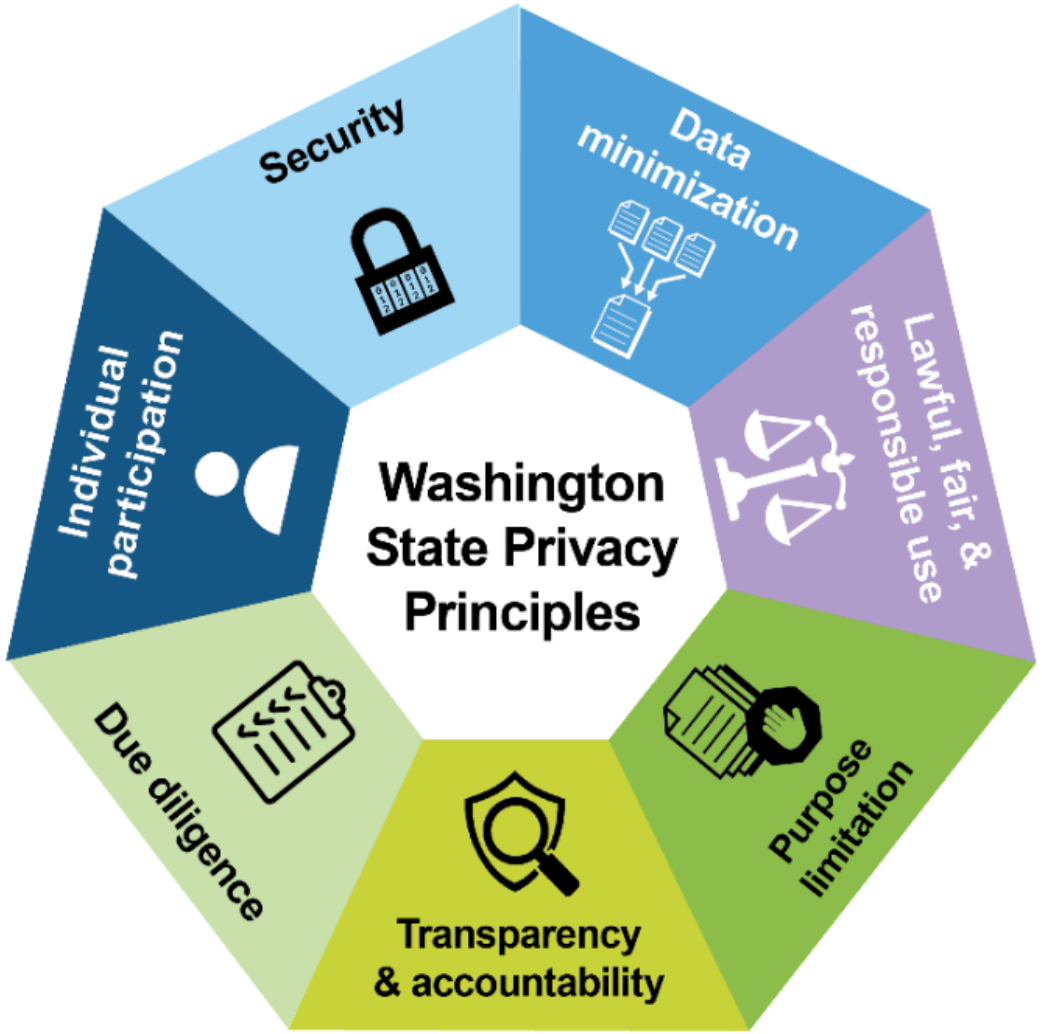
Privacy Policies



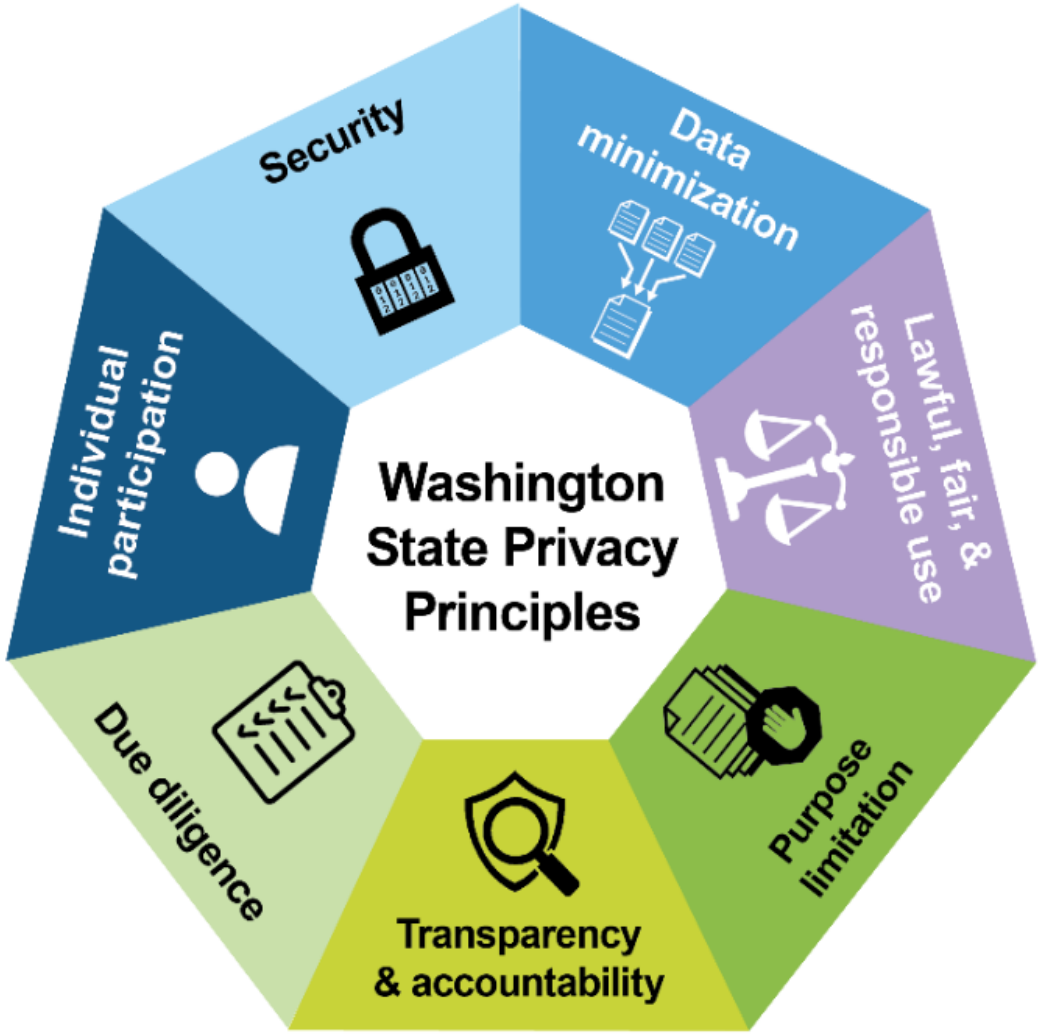
Privacy Notices relationship to Privacy Principles



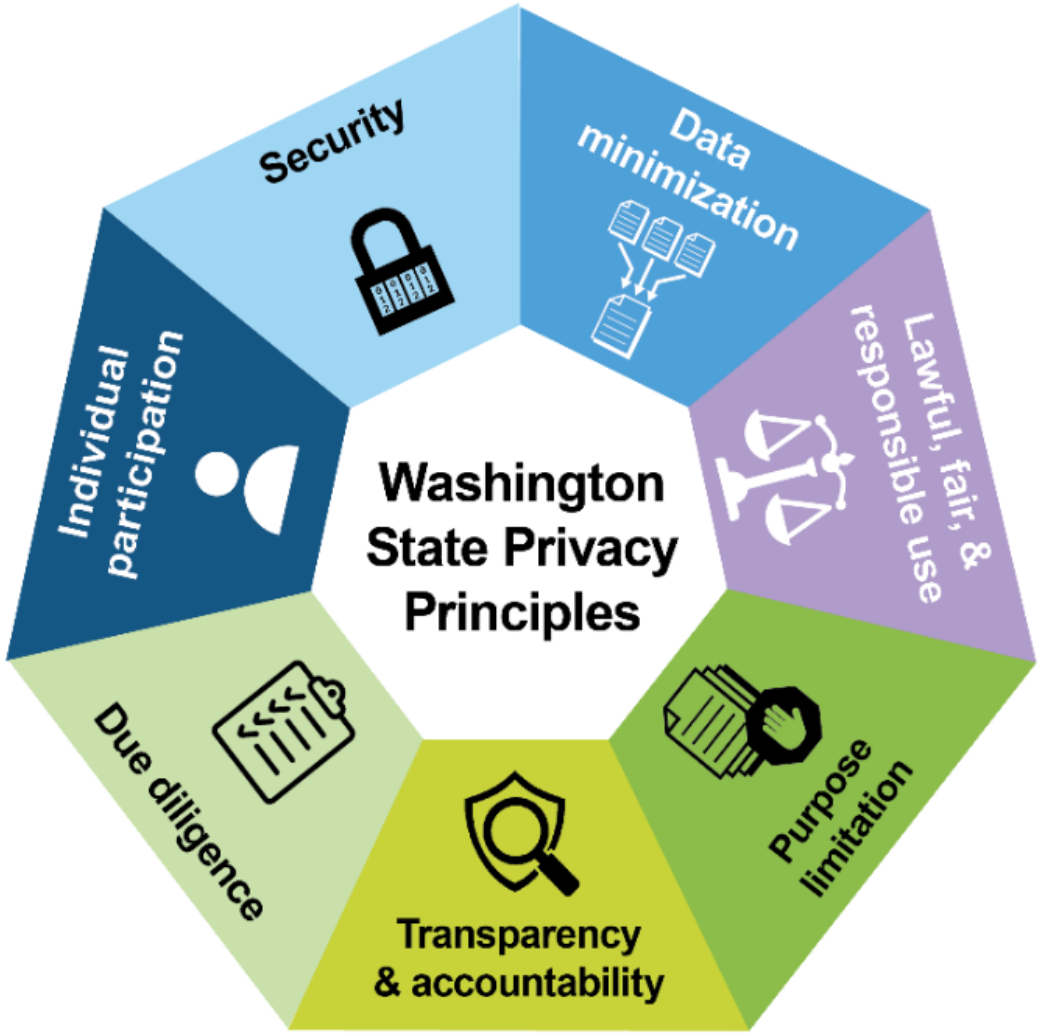
Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with under what circumstances.



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 disclosure, give timely notice to affected individuals.

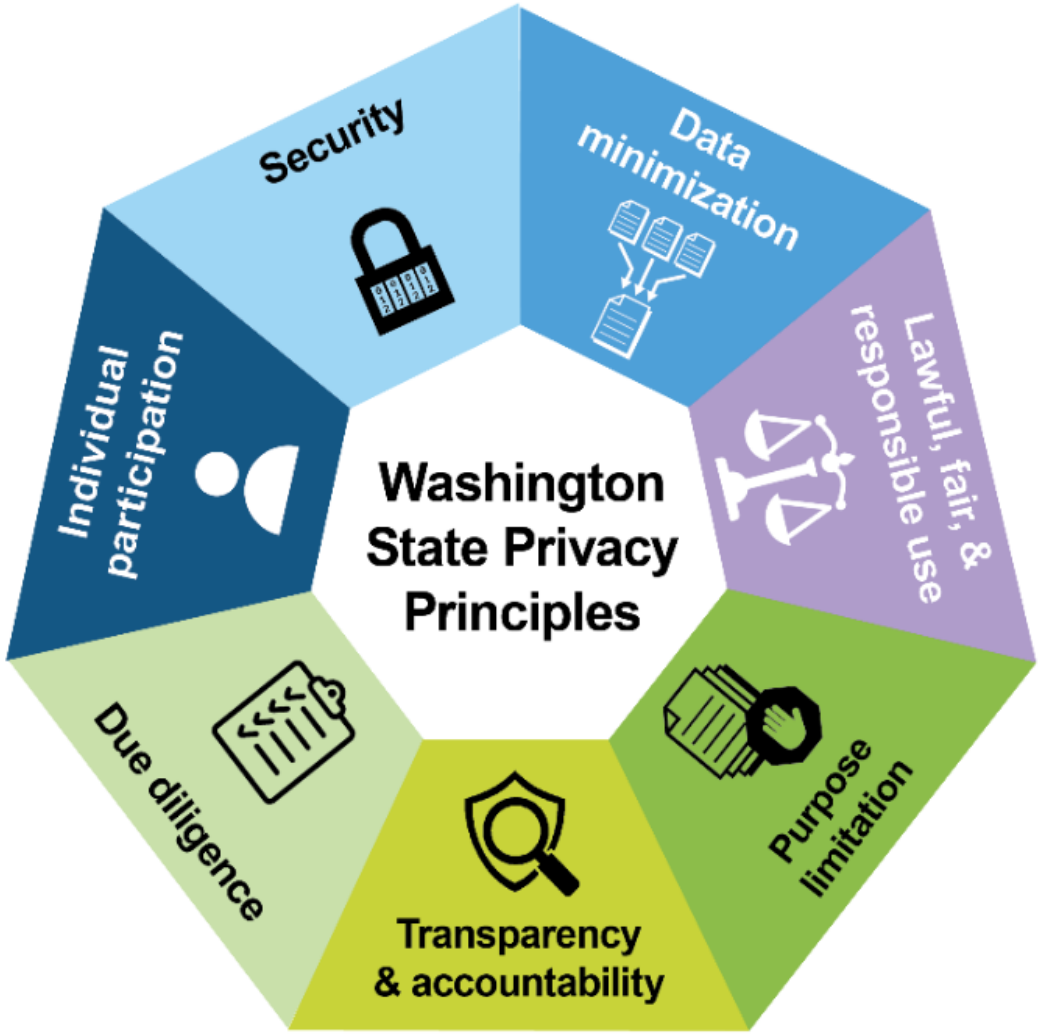


Accountability means being responsible and answerable for following data privacy laws and principles.

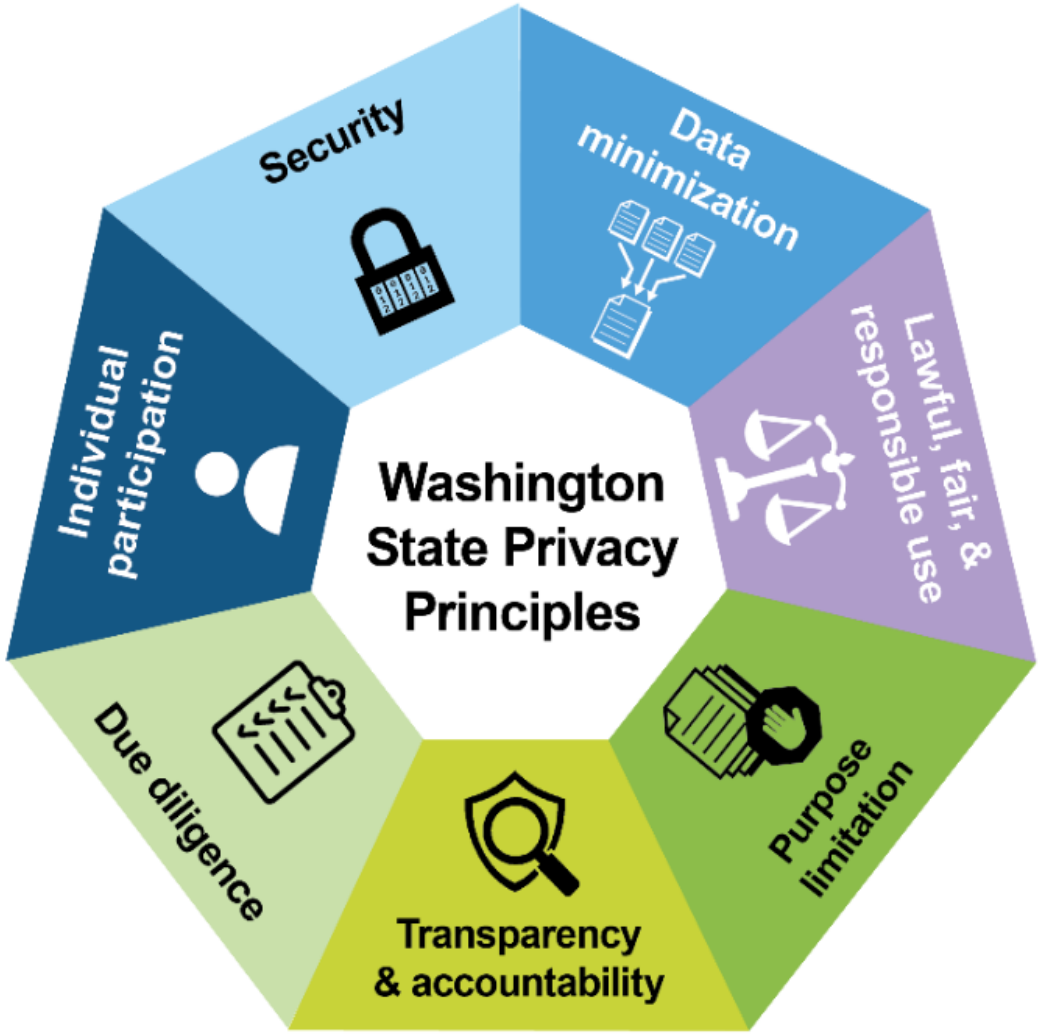


Implementation – Ensure accountability for adherence to these principles, any applicable privacy laws, and the public's expectations for the appropriate use of personal information.

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.



Individual Participation means giving people control of their information when possible.



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 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.

What should be included in a Privacy Notice?

Privacy Notice Elements

The point of a privacy notice is to be clear and transparent about your data collection and use practices. Each notice will depend on your organizations data use or applicable laws but consider including the following*:

- Name of organization
- Types or categories of personal data collected
- How personal data is used
- How personal data is shared
- Where personal data is used and stored
  - (e.g. out of the country)
- How long personal data is stored
- How personal data is protected
- An individual's rights re personal data use
- Contact information
- How to make a complaint (if applicable)
- Right to withdraw consent (if applicable)
- Effective date or last updated date

*list is not exhaustive

Model Templates

- HIPAA Model Privacy Notice Template from U.S. Health and Human Services Office of Civil Rights

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html

- FERPA Model Annual Notices from U.S. Department of Education

https://studentprivacy.ed.gov/annual-notices

- GLBA Model Privacy Form from U.S. Securities and Exchange Commission

https://www.sec.gov/rules/final/2009/34-61003_modelprivacyform.pdf

Other resources

- Very comprehensive checklists available on the U.K. Information Commissioner's Office

Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key...

ico.org.uk

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

When to provide it

☐ We provide individuals with privacy information at the time we collect their personal data from them.

If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

- ☐ within a reasonable period of obtaining the personal data and no later than one month;
- ☐ if we plan to communicate with the individual, at the latest, when the first communication takes place; or
- ☐ if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it

We provide the information in a way that is:

- ☐ concise;
- ☐ transparent;
- ☐ intelligible;
- ☐ easily accessible; and
- ☐ uses clear and plain language.

Changes to the information

☐ We regularly review and, where necessary, update our privacy information.

☐ If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

☐ We undertake an information audit to find out what personal data we hold and what we do with it.

☐ We put ourselves in the position of the people we're collecting information about.

☐ We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

- ☐ a layered approach;
- ☐ dashboards;
- ☐ just-in-time notices;
- ☐ icons; and
- ☐ mobile and smart device functionalities.

Recommended Best Practice

Layered Privacy Notices

•Very short privacy notices (Layer 1) – A very short statement that provides only the reason that personal data is being collected and a link or direction to more info.

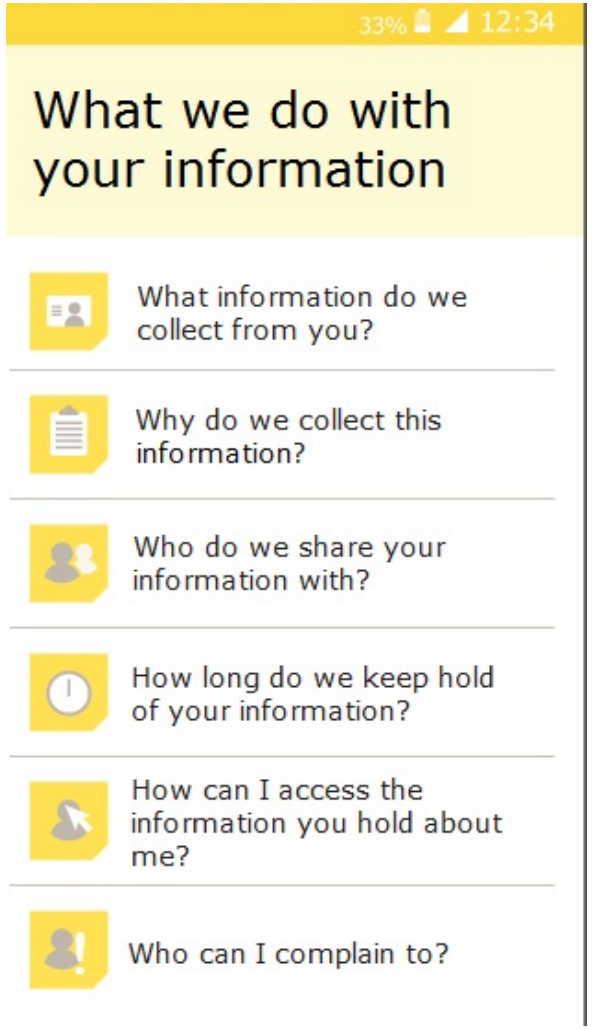
- This type of notice is used when space is very limited, such as on a data collection form. For example, on a web inquiry form you might include the following very short privacy statement: "We are collecting your email address and phone number in case we need to contact you about this matter. To read our full privacy notice, click here."

•A privacy notice summary or "highlights" (Layer 2) – A one page privacy notice that provides basic information about the personal data collected, the uses and sharing of the data, individual rights (such as choices and access options), and other important information and contact information.

•The complete privacy notice (Layer 3). Individuals always receive the complete notice when they want more information or when required by law.

Layered Privacy Notice Examples

Section	What can you find there?
How Twilio processes your personal information	Twilio collects personal information such as Customer Account Data directly from you — as a customer or a visitor — when you visit Twilio's website, request a product, service or access to an event, or when you contact a member of the Twilio team or sign up for a Twilio account to use our products and services. Twilio also indirectly collects the personal information of your end users called Customer Usage Data (e.g., communications metadata) and Customer Content (e.g., communications content).
Data about our customers	We process customer contact details such as your name, email, and phone number directly from you when you make a request, contact a member of our team, or sign-up for a Twilio account. Read this section to learn more about the types of data we collect about you, why we collect it, and how we store it.
Data about our customers' end users	We process your end users' communications-related data such as phone numbers, email addresses, friendly names that you create for your end users. We also process the content of communications sent by you or your end users to provide services to you and to carry out necessary functions of our business as a communications service provider. Please read this section to learn more about the types of data we collect about your end users, why we collect it, and how we store it.



NIST Privacy Framework

Function	Category	Subcategory
COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P)**: Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1**: Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risk are established and in place.
		CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.
	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1**: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.

NIST 800-53, rev.5

PT-5 Privacy Notice

Control: Provide notice to individuals about the processing of personally identifiable information that:

a. Is available to individuals upon first interacting with an organization, and subsequently at [Assignment: organization-defined frequency];
b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;
c. Identifies the authority that authorizes the processing of personally identifiable information;
d. Identifies the purposes for which personally identifiable information is to be processed; and
e. Includes [Assignment: organization-defined information].

Privacy Notice Debate

Privacy notices over time

1998	2001	Today
< 5% of websites have privacy notices	Virtually all prominent websites have notices	Virtually all organizations have privacy notices, for online and offline activities

What happened?

Fair Information Practice Principles

The internet

Banner ads

Targeted searches

Pay for placement and pay-per-click

Targeted ads

What happened?

Fair Information Practice Principles

The internet

Banner ads

Targeted searches

Pay for placement and pay-per-click

Targeted ads

Notice and consent / notice and choice

Step 1 – Organization provides notice of data collection, use and sharing

Step 2 – Individual consents or chooses to agree

Is there really choice?

Is there really consent?

Is it really enforceable?

Ripped from the Headlines

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Why Your Inbox Is Crammed Full of Privacy Policies

Data Protection and Privacy: Is the consent model broken?

Online privacy notices don't work.

April 15, 2022

FTC Chair Signals Crackdown on Confusing Privacy Policies

Khan Faults Company Privacy Policies

April 12, 2022, 3:16 AM

How "Notice and Consent" Fails to Protect Our Privacy

FTC position

"I'm concerned that the present market realities may render the notice and consent paradigm outdated and insufficient

....

[focusing on notice and consent ends up] side stepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place."

Alternatives?

Harm-based

Moving from deceptive to unfair

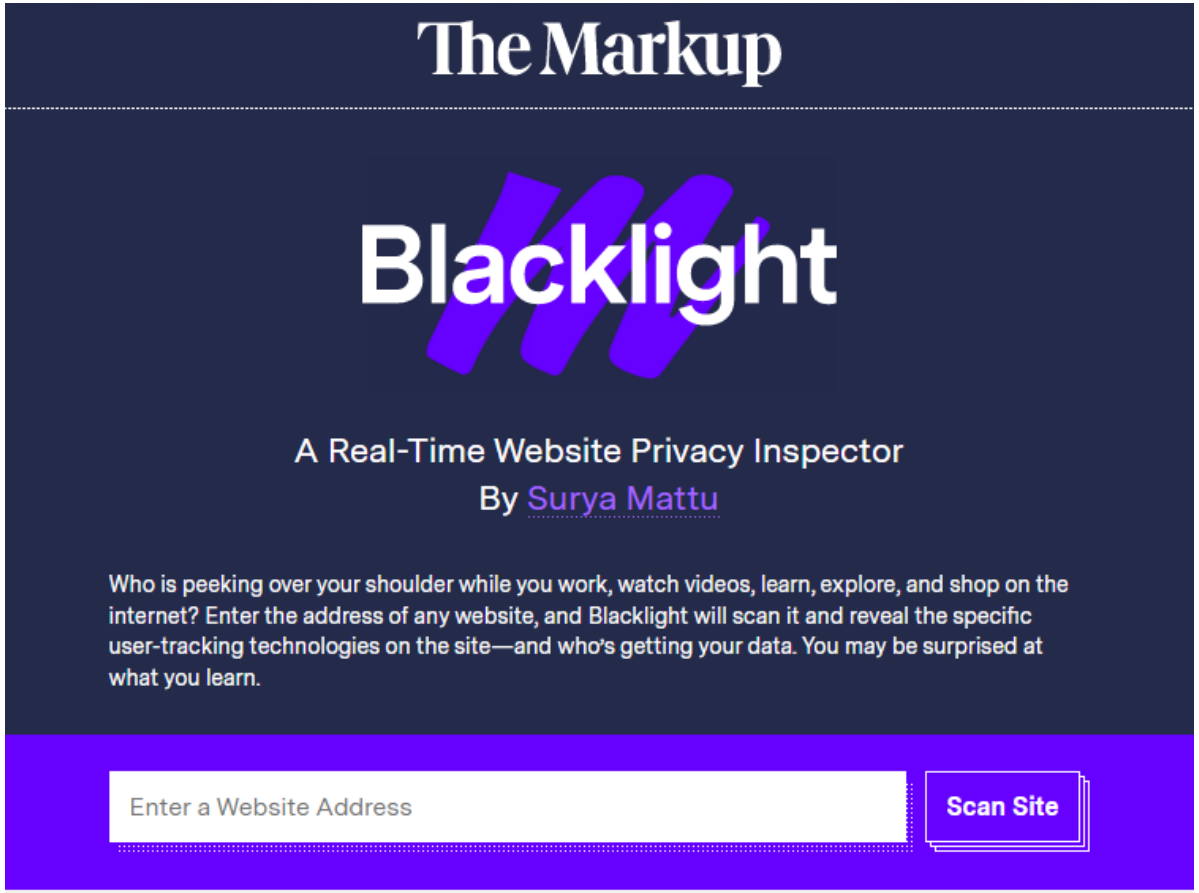
Setting baseline protections

Keep in Mind

Privacy Notices mean something…

- Review privacy notices periodically
- Update notices to reflect current data use practices
- Ensure teams know what is in the notices if they are responsible for data handling practices identified or explained in the notices
- Use plain language – avoid legalese
- Methods of delivery – (e.g. online, by mail)
- When – timing of delivery
- Organizations can be held accountable for not following their stated practices

“Real-Time Website Privacy Inspector”



https://themarkup.org/blacklight

Thank you

Questions?