Washington State Attorney General's Data Privacy Report

2026

Table of Contents

Letter from Attorney General Nick Brown

Dear Washingtonians,

Personal information has become one of the most valuable assets in the modern economy. This has led institutions to collect, retain, and share more information than necessary to provide their products and services. The harm produced by these incentives is increasingly apparent. Data breaches continue to expose sensitive information, while many Washingtonians report having little control over who holds their data or how their data is used. These harms affect our residents' personal safety, financial security, individual autonomy, and public trust in institutions.

With those challenges in mind, it is my honor to present the first-ever Washington State Attorney General's Data Privacy Report.

Washington has already taken important steps to protect personal information. I am proud of my office's work to enforce those protections and document emerging privacy risks. Through our annual Data Breach Report, we provide policymakers and the public with information about the scale and impact of breaches affecting Washington residents. In 2025, my office also conducted a statewide Data Privacy Survey to better understand Washingtonians' experiences, concerns, and priorities.

This first report of its kind from our office builds on those efforts by identifying gaps in protections for residents' personal information and proposing policies to strengthen protections, improve enforcement, and expand access to privacy and data-security resources.

Protecting privacy is an ongoing responsibility requiring collaboration among lawmakers, government agencies, businesses, advocates, researchers, and communities. I encourage everyone to use this report to help build a more transparent, accountable, secure, and consumer-centered approach to handling personal information across Washington.

Sincerely,

Nick Brown
Attorney General

Executive Summary

Key findings

This report identifies four recurring concerns in the modern data economy: overcollection and secondary use, weak consent requirements and deceptive design, the collection and sale of sensitive data, and limited consumer visibility into data broker practices. These practices can leave Washingtonians with little visibility into who holds their personal information, how it is being used, or how to regain control over it.

The resulting harms are evident across Washington. In 2025, the Attorney General's Office received reports of 209 data breaches affecting more than 8 million Washingtonians.[1] More than 80% of those breaches exposed Social Security numbers, increasing the risk of identity theft, financial fraud, and impersonation.[2] Personal information can also make scams more convincing,[3] enable stalking and harassment, expose visits to sensitive locations,[4] and influence the prices, discounts,[5] advertisements, or housing opportunities a person receives.[6]

Washington residents have expressed strong concern about these practices. A 2025 Attorney General's Office survey received more than 700 responses from residents in 26 counties.[7] 83% of respondents said they had little or no control over who could access their personal information, and 95% said there was no circumstance in which they would be comfortable providing personal information without informed consent.[8] 62% said it was difficult or very difficult to opt out of targeted advertising, and 65% said the same about requesting deletion of their information from an app or service.[9]

Washington has enacted targeted laws for consumer health data,[10] student data,[11] data breaches,[12, 13] biometric identifiers,[14] and government use of automated license plate reader systems,[15] among others. However, these protections apply unevenly. The same type of personal information may be subject to strict limits in one context but receive little comparable protection in another. More broadly, Washington does not have a generally applicable privacy framework establishing common standards for consent, data minimization, transparency, retention, and secondary use across sectors and institutions.

The following recommendations respond to these findings through policy, enforcement, and education approaches.

Recommendations at a glance

Policy – Strengthen Baseline Protections for Personal Data

1. *Require meaningful and informed consumer consent and prohibit deceptive design*
2. *Limit collection, use, and retention of personal information to what is necessary to provide a requested product or service*
3. *Strengthen protections for biometric and precise geolocation data*
4. *Require data brokers to register with the state and follow standard data privacy protections*

Enforcement – Strengthen Privacy Enforcement and Institutional Capacity

5. *Ensure privacy laws have clear, practical, and accountable enforcement mechanisms*
6. *Support state agencies in adopting privacy principles and building privacy capacity*

Education – Raise the Baseline of Digital Literacy in Washington

7. *Develop free and accessible resources that explain data privacy concepts and share tips to keep Washingtonians' data safe*
8. *Partner with business associations to develop educational resources to support small businesses with data security and compliance*

Background

The Data Economy

What is the data economy?

The **data economy** is an ecosystem in which personal information is collected, organized, analyzed, shared, or sold by a network of public and private institutions. In this report, "**institution**" refers broadly to businesses, government agencies, nonprofits, universities, and other entities. An institution that collects personal information may also be described as a "**data collector**."

Personal information is valuable because it can be used to make inferences about the people who use an institution's products, services, or programs.[16] By combining information from different sources, data collectors can infer a person's interests, routines, income range, health concerns, or likely behavior.[17] Those inferences may be used to build consumer profiles and audience segments that are sold or otherwise made available to advertisers and other customers.[18] For example, a person's browsing activity may be combined with demographic and behavioral information to place them into categories based on their age range, affluence, online activity, or family status, which can then be used to target advertisements across websites and apps.[19]

Why the data economy rewards more collection

Because personal information and the inferences drawn from it are valuable, **data collectors** have a strong incentive to collect more information, retain it longer, combine it with other data, and share it more widely.[20] Many websites, apps, and digital services rely at least partly on advertising or other data-driven business models.[21] Advertisers value detailed consumer profiles because they can use them to identify people who are more likely to respond to a particular ad.[22] **Data brokers** profit by combining information from data collectors, public records, social media, and other sources, then selling or licensing access to the resulting profiles and audience segments.[23]

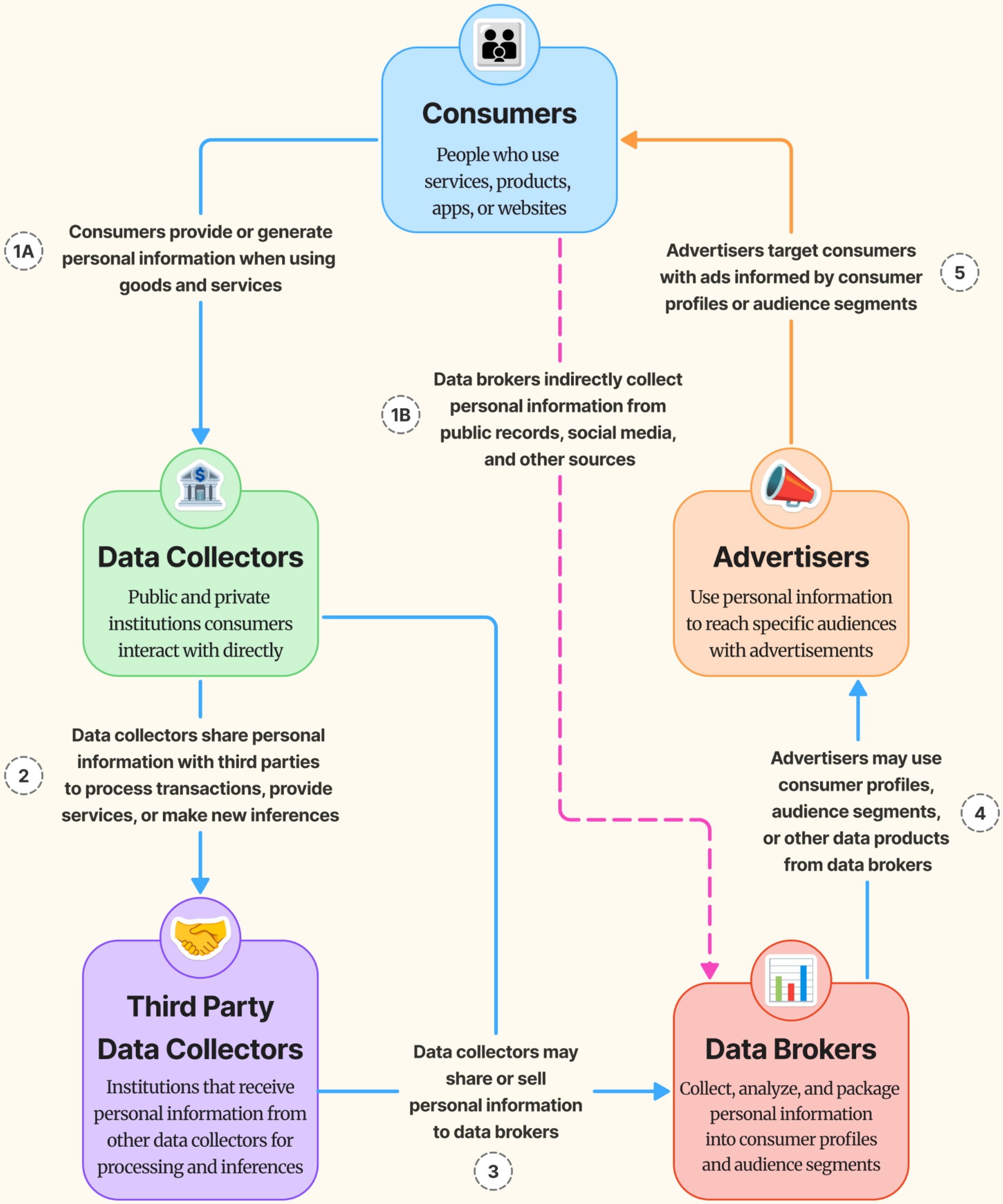
These connected incentives create pressure to collect and share increasingly detailed information about users, including information that may not be necessary to provide the product or service a person requested.[24] As that information is copied, combined, and shared, it can become far removed from the original interaction that generated it.[25] This makes it difficult for people to know who has their information, how it is being used, whether it is accurate, or how to regain control over it.[26]

The following diagram illustrates one simplified pathway personal information may follow through the data economy.

The Data Economy at a Glance

How personal information moves through a network of institutions

Personal information can move far beyond the first institution you directly interact with.



This diagram illustrates one simplified, potential pathway.
The path personal information takes through the data economy varies by service, business model, contract, and applicable law.

Concerning Data Collection Practices

The incentives that drive the data economy can encourage data collectors to collect, use, retain, and share personal information in ways that are difficult for people to understand or control. Although these practices operate in different ways, they share a common effect: they separate the collection and use of personal information from the expectations and choices of the people that information describes.

Overcollection and secondary use

Overcollection occurs when a data collector gathers more personal information than is reasonably necessary to provide a requested product or service. **Secondary use** occurs when personal information is used for a purpose unrelated to the interaction that generated it. For example, a user may provide a video game company with contact information to set up an online account. If the company later shares that information with a marketing agency to support targeted advertising, that would be a secondary use. The more personal information a data collector collects and retains, the more opportunities it has to repurpose that information. However, collecting and retaining more information also increases the potential harm if that information is breached, accessed without authorization, or otherwise misused.

Weak consent requirements and deceptive design

Important information about how personal information will be used, shared, or sold is often confusing,[27] bundled with unrelated terms,[28] or buried in privacy policies that people are unlikely to read or fully understand.[29]

Informed consent is a privacy concept that addresses this problem by setting a standard for how data collectors inform users about their intentions to use their personal information.[30] Informed consent requires clear information, plain language, a voluntary choice, and a reasonable opportunity to decline.[31] Consent is not considered informed simply because a person clicked a button or agreed to a lengthy privacy policy.[32]

Deceptive design further undermines informed consent by steering, pressuring, or confusing people into choices they might not otherwise make.[33] For example, a website may make “accept all” prominent and easy to select while making the option to reject tracking difficult to find or requiring several additional steps.[34] Other examples include bundling consent for unrelated uses, using misleading button labels, or making a privacy choice substantially harder to reverse than to accept.[35] Even when a privacy-protective choice exists, a deceptive design can still push users toward sharing more information or accepting more tracking than they intended.[36]

Collection and sale of sensitive data

Some types of personal information reveal particularly sensitive or lasting details about a person. **Biometric identifiers**, such as fingerprints or facial recognition data, can be used to recognize or verify an individual's identity.[37] Unlike a compromised password, biometric information cannot easily be changed if it is exposed.[38] Precise **geolocation data** can reveal a person's exact or near-exact movements, including patterns involving their home, workplace, medical providers, places of worship, or other sensitive locations.[39]

This data can be especially valuable to data collectors because it can identify a person with greater certainty[40] or reveal detailed patterns about their behavior and movements.[41] However, without adequate safeguards this information can create lasting risks of surveillance,[42] physical violence, emotional distress, and other misuse.[43]

Limited consumer visibility into data broker practices

Data brokers collect, combine, and sell personal information, often without any direct relationship with the people whose information they hold.[44] Because people rarely interact with data brokers directly, they may not know which brokers possess their information, how that information is used, or where it is ultimately shared.[45]

This lack of visibility can benefit data brokers by making privacy choices more difficult to exercise.[46] A person cannot easily request access, correction, deletion, or an end to the sale of their information when they do not know which institutions hold it.[47] Personal information may therefore continue to circulate among brokers and other third parties largely outside the awareness or control of the person it describes.[48]

Despite previous legislative efforts,[49] Washington does not currently require data brokers to register, and there is no centralized system that allows Washingtonians to identify brokers and submit deletion or opt out requests.

Harms to Washingtonians

The practices described in the previous section create real risks of harm for Washingtonians. Personal information can be used to steal money, take over accounts, make scams more convincing, target residents for harassment or abuse, and shape the prices or opportunities they receive. These harms affect financial security, physical safety, reputation, autonomy, and access to essential services. They can also be difficult to reverse once personal information has been copied, sold, or exposed.

Data breaches expose Washingtonians to scams and identity theft

Data breaches occur when personal information is accessed, acquired, or exposed without authorization,[50] often through cyberattacks, theft, employee mistakes, or other forms of unauthorized access.[51] Information exposed in a breach can be used to commit identity theft or fraud, take over accounts,[52] or facilitate stalking and harassment.[53] Data breaches are among the clearest and most measurable privacy harms affecting Washington residents.[54]

In 2025, the Attorney General's Office received notices for 209 separate breaches affecting just over 8 million Washingtonians.[55] It was the second consecutive year in which the number of breach notices exceeded the state's population, suggesting that many residents were likely affected more than once.[56] More than **80%** of reported breaches exposed **Social Security numbers**, which can be misused for identity theft, financial fraud, and other forms of impersonation.[57]

OVER 47 MILLION

data breach notices have been sent to Washingtonians since 2017[58]

Stolen information may also be sold or reused long after the original breach.[59] Although breach notices help residents take protective steps, they cannot recover information that has already been copied or prevent future misuse. Overcollection and unnecessary retention increase the scale of these harms by leaving institutions with a larger and more extensive body of personal information.[60] The more information an institution holds, the more information that may be exposed or misused if its systems are compromised.[61]

Personal data is used for harassment and abuse, with disproportionate effects

Exposed personal details can make phishing, spoofing,[62] and impersonation attempts more credible, pressuring people to send money, grant account access, or disclose additional information.[63] Older adults are disproportionately targeted by fraud schemes.[64] Youth face distinct risks from cyberbullying and other forms of online abuse.[65]

Personal information can also be weaponized to monitor, expose, intimidate, or target people.[66] Home addresses, contact information, photographs, location histories, and details about relationships or routines can facilitate stalking, threats, and other abuse.[67] The sale of detailed personal information by data brokers can increase these risks by making information easier to obtain and combine.[68]

Federal Trade Commission (FTC) actions against data brokers Kochava and Mobilewalla serve as useful examples. In its action against Kochava, the FTC alleged that the company sold location data capable of identifying visits to reproductive health clinics, places of worship, domestic violence shelters, and other sensitive locations.[69] In its action against Mobilewalla, the FTC alleged that the company collected or sold sensitive location data associated with political protests and other activities.[70] The Mobilewalla complaint also alleged that the company attempted to track union organizers[71] and helped clients target pregnant women, Hispanic churchgoers, and members of the LGBTQ+ community through custom audience segments.[72]

Data privacy harms do not affect everyone equally and can be particularly severe for people whose safety, health care, employment, or ability to participate in public life depends on keeping their identity, location, or associations private.[73]

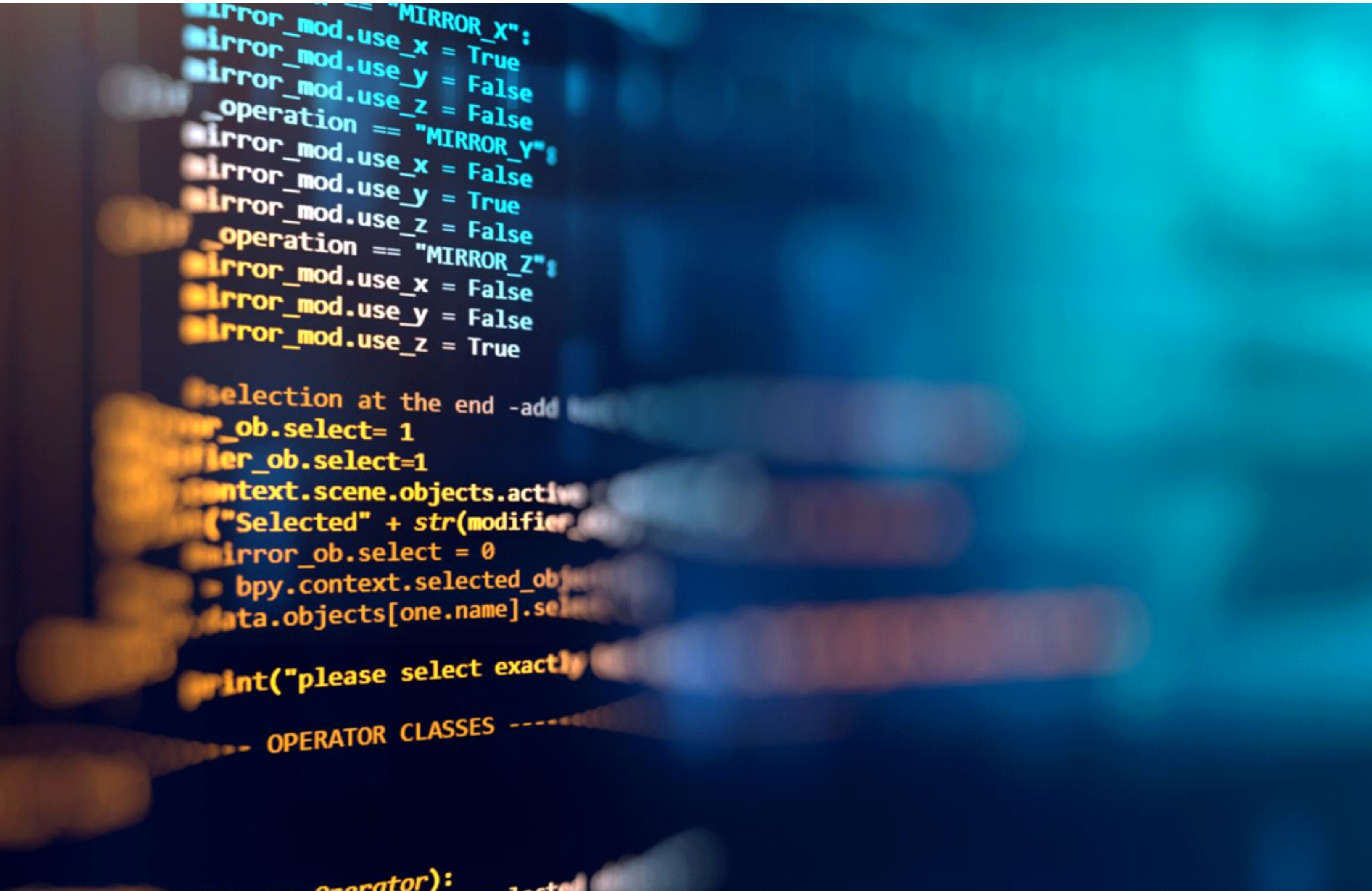
Washingtonians face surveillance pricing and data discrimination

Institutions may use personal information to influence the advertisements, prices, and discounts a person receives.[74] Personal information may also affect access to credit, employment opportunities, and other goods and services.[75] In housing, it can affect which opportunities are advertised to a resident.[76]

In 2025, FTC staff reported that retailers can use information such as a consumer's location, demographics, browsing and purchase history, and even online mouse movements to tailor prices and discounts.[77] These tools may allow a retailer to withhold a discount from customers it predicts will purchase a product anyway while offering it to other customers, causing different consumers to pay different prices for the same product.[78]

In 2022, the Department of Justice (DOJ) secured a court-approved settlement requiring Meta to stop using its Special Ad Audience tool for housing advertisements.[79] DOJ alleged that the tool relied on race, sex, and other characteristics protected by the Fair Housing Act to identify users who resembled an advertiser's selected audience.[80] The settlement required Meta to redesign its ad-delivery system to reduce racial and other disparities in who received housing advertisements.[81]

When the information or assumptions underlying these decisions are incomplete or inaccurate, Washingtonians may be treated unfairly without knowing why or having a practical way to correct the record.[82] Even accurate information can be used to identify when a person is more vulnerable to pressure or likely to pay a higher price.[83]



Washingtonians Want More Transparency and Control

2025 AGO Data Privacy Survey

In 2025, the Attorney General's Office launched a Data Privacy Survey to better understand how Washington residents experience data privacy in their daily lives.[84] The survey received over 700 responses from residents in 26 of Washington's 39 counties.[85]

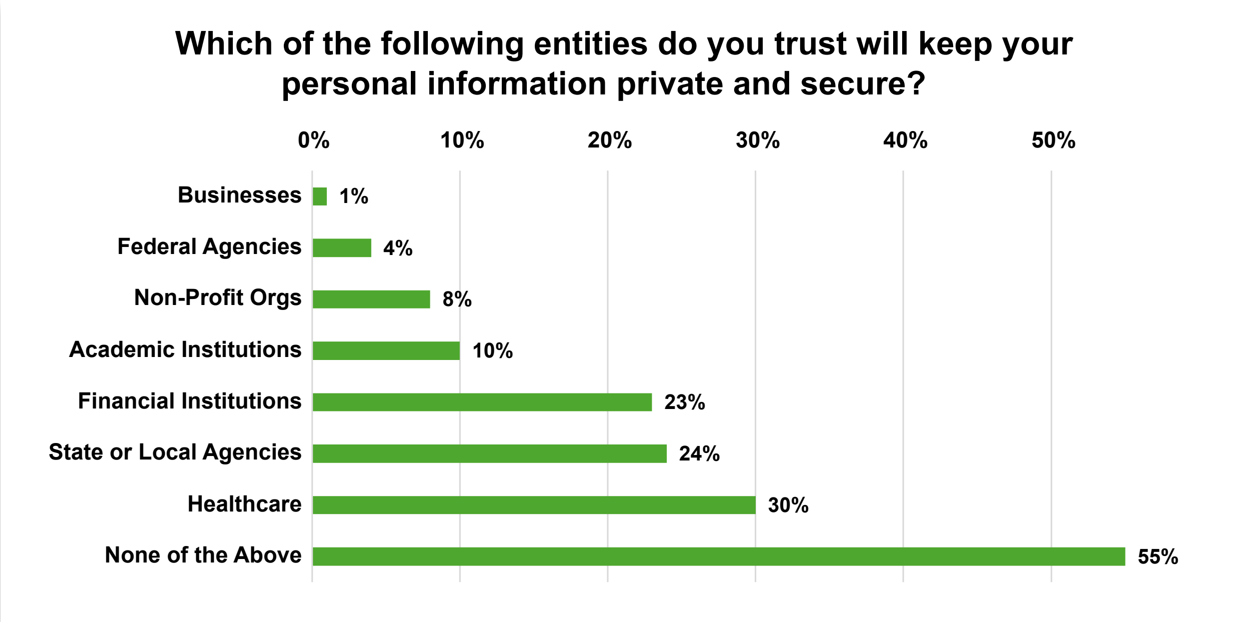
Washingtonians feel they lack control

Eighty-three percent of respondents said they felt they had little or no control over who has access to their personal information.[86] Many respondents attributed that lack of control to confusing privacy policies, limited choices, and uncertainty about where their information goes after it is collected.[87]

> ***"So many entities send out complicated notices about what they do with my personal info, that I wind up feeling pretty powerless about having any control in the matter."***
>
> ***– Survey respondent, King County[88]***

Trust is low across institutions

Respondents also reported low trust in institutions that collect personal information. **Fifty-five percent** of respondents selected 'none of the above' when asked which listed institutions they trusted to keep their personal information private and secure.[89]



Source: 2025 AGO Data Privacy Survey[90]

Washingtonians want to provide informed consent

Respondents were provided with a definition of informed consent requiring clear, plain-language disclosure, a freely made choice, and the ability to withdraw consent.[91] Applying that standard, only **47%** said they had ever given informed consent to an institution collecting, sharing, or selling their personal information;[92] another **25%** were unsure.[93] At the same time, **95%** said there was no circumstance in which they would be comfortable having their personal information collected, shared, or sold without informed consent.[94]

"Data collection must be opt-in and revocable. We must have the right to see what data institutions are collecting about us, and clear disclosure of how they are using it. Personal data should never be for sale without the explicit, informed, opt-in consent of legal adults."

– Survey respondent, King County

Washingtonians are struggling to exercise privacy choices

Washington residents report having difficulty exercising control over how their data is used. **Sixty-two percent** of respondents said it was difficult or very difficult to opt out of targeted advertising,[95] and **65%** said it was difficult or very difficult to request deletion of their personal information from an app or service.[96]

Taken together, the survey responses demonstrate that Washingtonians want greater transparency about how personal information is used, informed consent before personal information is collected or shared, and the ability to easily exercise their rights to limit how their personal information can be used.[97]

Washington's Privacy Laws and Remaining Gaps

Comprehensive privacy regulation across jurisdictions

The European Union's General Data Protection Regulation (GDPR) establishes broadly applicable standards for processing personal information.[98] It requires institutions to have a lawful basis for collecting and using personal information and establishes principles including data minimization, purpose limitation, storage limits, security, and accountability.[99] It also gives individuals the right to understand, access, correct, delete, restrict, and transfer their personal information.[100] The GDPR continues to serve as a model for privacy laws and practices around the world.[101]

The United States does not have a comparable comprehensive federal consumer privacy law.[102] Instead, federal laws generally protect information within particular sectors or contexts, such as health information under the Health Insurance Portability and Accountability Act (HIPAA),[103] student records under the Family Educational Rights and Privacy Act (FERPA),[104] and information collected online from children under the Children's Online Privacy Protection Act (COPPA).[105] This approach leaves some personal information and uses outside those targeted protections.

In the absence of a comprehensive federal privacy law, states including California,[106] Colorado,[107] Oregon,[108] and Connecticut[109] have enacted broader consumer privacy laws that give residents rights over their personal information and establish obligations for covered businesses across many industries.

Washington has not enacted a comparable, generally applicable consumer privacy law.[110] Instead, Washington's privacy protections are targeted to particular types of information, institutions, or situations.

Washington data privacy laws, at-a-glance

Washington has several privacy laws that protect specific types of personal information and require data collectors to be more transparent with consumers. These laws do not create one comprehensive privacy framework for all personal information, but they are an important step toward giving Washingtonians more control over their personal information and holding data collectors accountable.

Data Breach Notification Law[111, 112]

Ch. 19.255; 42.56.590 RCW	**Signed into law on May 10, 2005**
What it covers	*Personal information exposed in data breaches*
What it does	*Requires notice to affected residents and the Attorney General's Office when a breach affects more than 500 Washingtonians*
Limitations	*Reacts after data is exposed, does not limit the collection or retention of information*

Student User Privacy in Education Rights Act[113]

Ch. 28A.604 RCW	**Signed into law on May 14, 2015**
What it covers	*Student personal information collected through certain online services used in Washington K–12 schools*
What it does	*Requires clear disclosure of what student information is collected and how it is used or shared; provides access and correction rights; prohibits sale and targeted advertising; limits profiling and unrelated uses; requires security safeguards; and requires deletion of school-controlled information upon the school's request, subject to limited exceptions.*
Limitations	*Applies only to qualifying K–12 school services and does not cover general-audience websites, apps, or online services*

Biometric Privacy Protection Act[114]

Ch. 19.375 RCW	**Signed into law on May 16, 2017**
What it covers	*Biometric data used for commercial purposes*
What it does	*Limits when businesses can create, share, and retain biometric identifiers*
Limitations	*Does not apply to government agencies and excludes photographs, videos, audio recordings, and data generated from them*

My Health My Data Act[115]

Ch. 19.373 RCW	**Signed into law on April 27, 2023**
What it covers	*Consumer health data*
What it does	*Requires privacy notices, consent for certain collection and sharing, deletion rights, authorization before sale, and limits location tracking near health care facilities*
Limitations	*Limited only to consumer health data, doesn't apply to government usage of consumer health data*

Driver Privacy Act[116]

Ch. 10.130 RCW	**Signed into law on March 30, 2026**
What it covers	*Automated License Plate Reader (ALPR) systems used by state and local agencies*
What it does	*Limits agency use, sharing, retention, and purchase of ALPR data*
Limitations	*Does not directly regulate private companies' ALPR systems*

Washington law also includes additional protections governing medical records,[117] consumer reports,[118] the secure disposal of personal information,[119] and disclosure exemptions for sensitive personal information contained in public records.[120]

Protections remain fragmented

Washington's laws demonstrate how targeted legislation can close significant privacy gaps. The My Health My Data Act extends protections to consumer health data that may not be covered by HIPAA.[121] The Driver Privacy Act establishes guardrails for an important public safety technology.[122] The Data Breach Notification Law gives residents information they can use to respond to a breach and allows policymakers to measure breach trends.[123, 124]

However, these protections apply unevenly and often depend on the context in which a Washingtonian's personal information is collected and used, rather than solely on its sensitivity. Location data may receive specific protections when connected to health care[125] or collected through a public agency's ALPR system,[126] but not when independently collected for another commercial or public safety purpose. Data generated from a resident's fingerprint and used to identify them may qualify as a biometric identifier, while photographs, videos, and audio recordings of that same person—and data generated from them—are excluded from Washington's biometric law.[127] This inconsistency can make it difficult for Washingtonians to understand which protections apply to their information or what rights they can exercise.

Washington also lacks a generally applicable privacy framework establishing common standards for how personal information is collected and used across sectors and institutions. Washington law does not consistently require all institutions to obtain informed consent, minimize collection, explain how information will be used, limit how long it is retained, or restrict its use for unrelated purposes.

Washington has established meaningful protections in several high-risk areas. The remaining challenge is to make those protections more consistent and intuitive by establishing common standards that apply across the data economy.

Recommendations

Addressing data privacy challenges requires a mix of stronger laws, effective enforcement, and improved public awareness. Accordingly, these recommendations are grouped into three areas: **policy**, **enforcement**, and **education**. Together, they aim to limit harmful data practices, hold data collectors accountable, and help Washingtonians better understand the risks to their data and steps they can take to protect it.

Policy – Strengthen Baseline Protections for Personal Data

1. Require meaningful and informed consumer consent

The Legislature should require data collectors to obtain meaningful and informed consent before collecting, using, or sharing personal information beyond what is reasonably necessary to provide a requested product or service.

Consent mechanisms should be clear, balanced, and easy to navigate, offering consumers a genuine opportunity to decline data collection. The data collection, sharing, and retention practices of collectors should be disclosed in clear, plain language. Important privacy terms should not be buried in lengthy legal agreements, privacy policies, or other documents that consumers are unlikely to read or fully understand.

Privacy choices should be easy to exercise and should not place unnecessary burdens on consumers. Where feasible, policymakers should consider centralized mechanisms that reduce the need for consumers to submit separate privacy requests to multiple data collectors.

Furthermore, these rights should be implemented through processes that are timely and accessible. Mechanisms that require lengthy delays or repeated appeals may undermine a consumer's ability to meaningfully exercise those rights.

Lastly, the Legislature should explicitly prohibit deceptive design practices that impair a consumer's ability to make informed and voluntary decisions about their data.

Other states provide useful models for making privacy choices meaningful in practice. California requires privacy-protective choices to be as easy to exercise as less protective choices.[128] Connecticut[129] and Oregon[130] require consent to be at least as easy to withdraw as it was to provide. Colorado requires covered data collectors to recognize qualifying universal opt-out mechanisms.[131]

#1 - Call to Action

- Require clear, plain-language consent mechanisms that give consumers a meaningful opportunity to decline unnecessary data collection.
- Prohibit deceptive design practices that steer consumers toward sharing more data than they intend.

2. Establish data minimization requirements and limit secondary use

The Legislature should require data collectors to limit the collection, use, and retention of personal information to what is reasonably necessary to provide a product or service requested by the consumer. These requirements should also restrict secondary uses of personal information for purposes unrelated to the interaction in which it was collected. Personal information should not be collected or retained simply because it may have future commercial value or could support unrelated business purposes, and consumers should not have to accept unnecessary collection or secondary use as a condition of receiving a requested product or service.

Limiting unnecessary collection and retention reduces privacy risks and the amount of sensitive information exposed when a security incident occurs.[132]

Broader privacy laws in California,[133] Colorado,[134] Connecticut,[135] and Oregon[136] provide useful models for data minimization. California requires the collection, use, retention, and sharing of personal information to be reasonably necessary and proportionate to its stated purposes and limits how long information may be retained.[137] Oregon similarly limits collection to information that is adequate, relevant, and reasonably necessary for specified purposes and requires consent before information is used for an unrelated or incompatible secondary purpose.[138]

#2 - Call to Action

- Limit collection, use, and retention of personal information to what is necessary to provide a requested product or service.
- Restrict secondary uses of personal information for purposes unrelated to the interaction in which it was collected.

3. Create stronger protections for biometric and precise geolocation data

Because biometric identifiers are difficult to replace[139] and precise geolocation data can reveal sensitive movements and associations,[140] both warrant protections beyond those that apply to personal information generally.

The Legislature should require data collectors to obtain clear, informed consent before collecting biometric or precise geolocation data. The sale and unnecessary commercial use of this information should be strictly limited or prohibited, particularly when it is not necessary to provide a requested product or service. Clear retention limits should also prevent this information from being stored longer than necessary. For example, a weather app may need a user's approximate location to provide a local forecast, but it should not retain or sell a detailed history of the user's movements.

Existing Washington laws protect biometric identifiers used for commercial purposes[141] and protect precise geolocation data in limited contexts—for example, when precise geolocation data could indicate that a consumer sought health services,[142] or when it is collected through a public agency ALPR system.[143] However, state law does not comprehensively protect either type of data across all institutions and uses. Virginia and Oregon provide useful models. Their broader consumer privacy laws require consent before precise geolocation data is processed.[144, 145] More recent legislation—Virginia's SB 338[146] and Oregon's HB 2008[147]—prohibits its sale.

#3 - Call to Action
• Require clear, informed consent before companies collect biometric or precise geolocation data. • Limit or prohibit the sale and unnecessary commercial use of biometric and precise geolocation data. • Establish clear limits on how long biometric and precise geolocation data may be retained.

4. Require data brokers to register, safeguard personal information, and provide deletion and opt-out rights

The Legislature should require data brokers processing Washingtonians' personal information to register annually with the state and disclose the types of personal information they collect, sell, or share. The state should make this information available through a public registry.

Registration would give Washingtonians, policymakers, advocates, and enforcement authorities greater visibility into an industry that generally operates without a direct relationship with the people whose information it holds.[148] It would also help residents identify data brokers that possess their information and where to submit privacy requests.

Registration should be paired with specific privacy and data-security requirements. The Legislature should:

- Require data brokers to maintain administrative, technical, and physical safeguards appropriate to the sensitivity and volume of the information they hold;
- Limit or prohibit data brokers from selling sensitive personal information;
- Require data brokers to honor consumer requests to delete their information or opt out of its sale or sharing; and
- Establish a centralized mechanism that allows residents to submit deletion and opt-out requests across all registered data brokers rather than contacting each company individually.

Several states—including California,[149] Oregon,[150] Texas,[151] Vermont,[152] and New Jersey[153]—have enacted data-broker registration laws. These laws provide useful models for annual registration, public disclosure, and state oversight. Vermont, for example, requires data brokers to maintain a comprehensive information-security program with administrative, technical, and physical safeguards.[154] California's Delete Request and Opt-Out Platform (DROP) allows residents to submit a single deletion request to all active registered data brokers.[155]

#4 - Call to Action

- Require data brokers to register annually and publicly disclose the types of personal information they collect, sell, or share.
- Require registered data brokers to maintain appropriate administrative, technical, and physical security safeguards.
- Limit or prohibit the sale of sensitive personal information by data brokers.
- Require data brokers to honor deletion and sale-or-sharing opt-out requests.
- Establish a centralized system that allows Washingtonians to submit those requests across registered data brokers.

Enforcement – Strengthen Privacy Enforcement and Institutional Capacity

5. Ensure privacy laws have clear, practical, and accountable enforcement mechanisms

Privacy rights are only meaningful when they can be effectively enforced. As data collection practices and technology become more complex, investigating privacy violations often requires specialized expertise, dedicated resources, and clear legal authority. To be effective, enforcement mechanisms should be clear, practical, and accountable. When enforcement mechanisms are unclear, difficult to administer, or insufficient to deter noncompliance, even well-designed privacy protections may fail to achieve their intended purpose.

Effective privacy laws should be built around three enforcement principles:

i. **Clarity.** The law should identify who is responsible for enforcement, whether enforcement authority rests with regulators, consumers, or both, and what consequences may result from non-compliance, such as civil penalties, administrative remedies, or other enforcement actions.

ii. **Practicality.** The entity or entities responsible for enforcement should have the legal authority, tools, and resources needed to carry out that role. The law should be written in accessible and specific terms, support consistent application by enforcement authorities, and impose obligations that regulated entities can reasonably comply with in practice.

iii. **Accountability.** Remedies or penalties should be significant enough to encourage compliance, deter harmful practices, and address violations in a timely manner. Enforcement mechanisms that are too limited, too weak, or too slow may fail to meaningfully change behavior.

Policymakers should consider a range of approaches to support effective enforcement. Depending on the circumstances, this may include using existing frameworks such as Washington's Consumer Protection Act, establishing funding mechanisms that support enforcement activities, or creating new enforcement frameworks that authorize investigations, penalties, rulemaking, reporting requirements, or other compliance tools. Different privacy laws may warrant different enforcement models, but all should be designed around the principles of clarity, practicality, and accountability.

Colorado and California's laws illustrate practical ways to support enforcement:

Rulemaking and enforcement authority

- Colorado authorizes the Attorney General to adopt rules implementing the Colorado Privacy Act and gives the Attorney General and district attorneys exclusive enforcement authority.[156]
- California vests the California Privacy Protection Agency with rulemaking and administrative enforcement authority, while preserving the Attorney General's authority to bring civil enforcement actions.[157]

Funding privacy administration and enforcement

- California directs 95% of administrative fines recovered by the California Privacy Protection Agency and 95% of civil penalties recovered by the Attorney General to funds supporting their respective work under the law.[158]

Risk assessments and cybersecurity audits

- Colorado requires covered data controllers to conduct data protection assessments for processing activities that present a heightened risk of harm to consumers.[159]
- California requires covered businesses to conduct risk assessments for processing that presents a significant risk to consumers' privacy and annual cybersecurity audits for covered businesses whose processing presents a significant risk to consumers' security.[160]

Future privacy proposals should be evaluated not only by the rights they create, but also by whether their enforcement mechanisms are clear, practical, and accountable. Lawmakers should also review existing privacy laws through the same lens and consider updates where enforcement roles are unclear, requirements are difficult to administer or comply with, or consequences are insufficient to deter noncompliance. This work would signal that data privacy is a priority for Washington and ensure privacy laws are effectively enforced.

#5 - Call to Action

- Evaluate new and existing privacy laws based on whether their enforcement mechanisms are clear, practical, and accountable, and update existing laws where necessary.

6. Support state agencies in adopting privacy principles and building privacy capacity

State agencies have made meaningful progress in strengthening their approach to data privacy.[161] WaTech's most recent State Agency Privacy Assessment found increased awareness of privacy concerns and broader adoption of formal privacy policies across state agencies.[162] As agencies adopt new tools—particularly those involving artificial intelligence—the need to implement effective privacy practices into agency operations is vital, and dedicated privacy staff are essential to that work.

The Washington Office of Privacy and Data Protection (OPDP) provides valuable support, guidance, tools, and resources to help state agencies strengthen privacy practices,[163] implement WaTech's Privacy and Data Protection Policy,[164] evaluate privacy risks associated with new systems and projects,[165] and incorporate privacy considerations into decisions about technology, data use, and vendor contracts.[166] State agencies should be encouraged to take full advantage of these resources and to partner with the OPDP as they continue to develop and improve their privacy programs.

Furthermore, the Legislature should provide agencies with the tools and funding necessary to continue advancing this work, including support for dedicated privacy staffing where appropriate. A dedicated privacy role does not need to look the same in every agency. Depending on the agency's size, mission, and data holdings, this may include a full-time privacy officer, a part-time privacy lead, or a designated privacy contact supported by legal, information-technology, public-records, data-governance, or risk-management staff.

For example, a privacy officer or privacy lead could inventory personal information, review projects involving personal data, coordinate privacy impact assessments, support staff training, advise on data-sharing and vendor agreements, maintain privacy notices, and serve as a point of contact for OPDP.

Recognizing that agencies vary in size, mission, and data holdings, the Legislature's support should be proportional to the level of risk and complexity each agency manages. Continued investment in privacy capacity will help agencies protect Washingtonians' personal information, use data responsibly, and strengthen public confidence in state government.

#6 - Call to Action

- Ensure agencies have the tools, funding, and staff support needed to strengthen privacy practices.
- Support dedicated privacy roles where appropriate, including privacy officers, privacy leads, or designated privacy contacts.
- Encourage agencies to partner with OPDP and use statewide privacy guidance, tools, and resources.
- Scale privacy support according to each agency's size, mission, data holdings, and level of risk.

Education – Raise the Baseline of Digital Literacy in Washington

7. Develop free and accessible resources that explain data privacy concepts and share tips to keep Washingtonians' data safe

Many Washingtonians report uncertainty about where their personal information goes after it is collected and difficulty exercising privacy choices.[167] These findings indicate a need for accessible public education about how personal information is collected, shared, and sold. When privacy decisions feel difficult or overwhelming, people may disengage from privacy management—a phenomenon researchers describe as "privacy fatigue."[168] The design of privacy choices can also influence whether users make more or less privacy-protective decisions.[169]

The AGO's Tech Policy Team, in partnership with consumer advocates, should create clear, publicly available resources—written in plain language and supported with real-world examples—to help close this gap. These resources should provide objective, jargon-free guidance on topics such as securing personal devices, recognizing deceptive design practices, understanding tracking cookies, identifying risks associated with data sharing, and managing privacy settings. By raising the baseline of digital literacy in Washington, these resources can help residents move from uncertainty and privacy fatigue toward greater confidence and control.

#7 - Call to Action

- Create plain-language public resources that explain how personal data is collected, shared, and sold.
- Provide practical tips on securing devices, managing privacy settings, understanding cookies, and recognizing deceptive design practices.
- Partner with consumer advocates to ensure materials are accessible, objective, and useful for a general audience.
- Help Washingtonians move from privacy fatigue to greater confidence and control over their personal information.

8. Partner with business associations to develop educational resources to support small businesses with data security and compliance

Small businesses often have limited time, staff, and resources to devote to cybersecurity and privacy work.[170] These constraints can make it harder to build and maintain effective privacy and data-security practices. If privacy or cybersecurity problems occur, the consequences can include financial harm, loss of customer trust, and reputational damage.[171] Without practical guidance, small businesses may struggle to understand and implement new privacy standards.

To develop more effective and practical resources, the AGO's Tech Policy Team should partner with business associations that can provide insight into the specific privacy, data-security, and educational needs of small businesses. These resources would reduce uncertainty and lower barriers to responsible data management.

Supporting our local business community is a win-win for privacy. When small businesses are equipped to handle data responsibly, they protect their customers, their reputation, and the local economy all at once.

#8 - Call to Action

- Partner with business associations to identify the privacy and data security needs of small businesses.
- Develop practical, plain-language resources that help small businesses understand privacy obligations and reduce data security risks.
- Lower barriers to responsible data management for businesses that lack dedicated legal or IT teams.
- Support small businesses in protecting their customers, reputation, and local communities.

Notes and Citations

1. Washington State Office of the Attorney General, “2025 Data Breach Report,” 2025, https://agportal-s3bucket.s3.us-west-2.amazonaws.com/Data_Breach/2025%20Data%20Breach%20Report/2025-Data%20Breach%20Report-f1.pdf
2. Id.
3. Federal Bureau of Investigation, “Spoofing and Phishing,” https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing
4. Federal Trade Commission, “FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations,” August 29, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other
5. Federal Trade Commission, FTC Surveillance Pricing 6(b) Study: Research Summaries—A Staff Perspective, January 2025, https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf
6. U.S. Department of Justice, “Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising,” June 21, 2022, https://www.justice.gov/archives/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known
7. Washington State Attorney General’s Office, “2025 Data Privacy Survey Results,” 2025, https://agportal-s3bucket.s3.us-west-2.amazonaws.com/Data%20Privacy/2025%20Survey/privacy-survey-summary_formatted_v2.pdf?VersionId=g9ADF.r8YwBY.OBcnnonhekNAe2zp6gq
8. Id.
9. Id.
10. Washington State Legislature, “Chapter 19.373 RCW: Washington My Health My Data Act,” https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true
11. Washington State Legislature, “Chapter 28A.604 RCW: Student User Privacy in Education Rights,” https://app.leg.wa.gov/RCW/default.aspx?cite=28A.604&full=true
12. Washington State Legislature, “Chapter 19.255 RCW: Personal Information—Notice of Security Breaches,” https://app.leg.wa.gov/RCW/default.aspx?cite=19.255&full=true
13. Washington State Legislature, “RCW 42.56.590: Personal Information—Notice of Security Breaches,” https://app.leg.wa.gov/RCW/default.aspx?cite=42.56.590
14. Washington State Legislature, “Chapter 19.375 RCW: Biometric Identifiers,” https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true
15. Washington State Legislature, “Chapter 10.130 RCW: Automated License Plate Reader Systems,” https://app.leg.wa.gov/RCW/default.aspx?cite=10.130
16. Wrabetz, J.M., “What Is Inferred Data and Why Is It Important?,” American Bar Association Business Law Today, August 22, 2022, https://www.americanbar.org/groups/business_law/resources/business-law-today/2022-september/what-is-inferred-data-and-why-is-it-important/
17. Id.
18. Electronic Privacy Information Center, “Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem,” EPIC, November 2022, https://epic.org/documents/disrupting-data-abuse-protecting-consumers-from-commercial-surveillance-in-the-online-ecosystem/

19. Id.

20. Id.

21. Electronic Privacy Information Center, “Online Advertising & Tracking,” EPIC, https://epic.org/issues/consumer-privacy/online-advertising-and-tracking/

22. Id.

23. Electronic Privacy Information Center, “Disrupting Data Abuse”

24. Electronic Privacy Information Center, “Online Advertising & Tracking”

25. Electronic Privacy Information Center, “Data Brokers,” EPIC, https://epic.org/issues/consumer-privacy/data-brokers/

26. Id.

27. Litman-Navarro, K., “We Read 150 Privacy Policies. They Were an Incomprehensible Disaster,” The New York Times, June 12, 2019, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

28. Information Commissioner’s Office, “What Is Valid Consent?,” https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/

29. Litman-Navarro, K., “We Read 150 Privacy Policies”

30. GDPR.eu, “Art. 7 GDPR — Conditions for Consent,” GDPR.eu, https://gdpr.eu/article-7-how-to-get-consent-to-collect-personal-data/

31. Id.

32. Id.

33. California Privacy Protection Agency Enforcement Division, “Enforcement Advisory No. 2024-02: Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice,” September 4, 2024, https://cppa.ca.gov/pdf/enfadvisory202402.pdf

34. Id.

35. Information Commissioner’s Office, “What Is Valid Consent?”

36. Electronic Privacy Information Center, “Disrupting Data Abuse”

37. National Institute of Standards and Technology, “Biometrics,” Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/biometrics

38. National Institute of Standards and Technology, “Facing the Facts to Keep Our Biometrics Secure,” October 2, 2024, https://www.nist.gov/blogs/taking-measure/facing-facts-keep-our-biometrics-secure

39. Prince, A.E.R., “Location Data Are Revealing Health Information,” The Regulatory Review, August 19, 2021, https://www.theregreview.org/2021/08/19/prince-location-data/

40. National Institute of Standards and Technology, “Biometrics”

41. Prince, “Location Data Are Revealing Health Information”

42. Electronic Privacy Information Center, “Disrupting Data Abuse”

43. Federal Trade Commission, “FTC Sues Kochava”

44. Electronic Privacy Information Center, “Data Brokers”

45. Id.

46. Id.

47. Id.

48. Id.

49. Washington State Legislature, "HB 2483—Creating a Data Broker Registry," 2025–26 Legislative Session, https://app.leg.wa.gov/BillSummary/?BillNumber=2483&Year=2026

50. Washington State Legislature, "RCW 19.255.005: Definitions," https://app.leg.wa.gov/RCW/default.aspx?cite=19.255.005

51. Washington State Office of the Attorney General, "2025 Data Breach Report"

52. Id.

53. Electronic Privacy Information Center, "Disrupting Data Abuse"

54. Washington State Office of the Attorney General, "2025 Data Breach Report"

55. Id.

56. Id.

57. Id.

58. Washington State Attorney General's Office, "Number of Washingtonians Affected by Data Breaches," State of Washington Open Data, last updated July 18, 2026, https://data.wa.gov/Consumer-Protection/Number-of-Washingtonians-Affected-by-Data-Breaches/qf7y-ftb2

59. Federal Trade Commission, "The Dark Web: What Your Business Needs to Know," October 17, 2017, https://www.ftc.gov/business-guidance/blog/2017/10/dark-web-what-your-business-needs-know

60. Federal Trade Commission, "Protecting Personal Information: A Guide for Business," October 14, 2016, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

61. Id.

62. Washington State Office of the Attorney General, "Glossary of Data Breach Terms," https://www.atg.wa.gov/glossary-data-breach-terms

63. Federal Bureau of Investigation, "Spoofing and Phishing"

64. Federal Bureau of Investigation, "Scammers Target Older Adult Victims," May 15, 2026, https://www.fbi.gov/news/stories/scammers-target-older-adult-victims

65. U.S. Department of Health and Human Services, Office of the Surgeon General, "Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory," 2023, https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf

66. Electronic Privacy Information Center, "Disrupting Data Abuse"

67. Id.

68. Electronic Privacy Information Center, "Data Brokers"

69. Federal Trade Commission, "FTC Sues Kochava"

70. Federal Trade Commission, "FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data," December 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data

71. Federal Trade Commission, "Complaint, In the Matter of Mobilewalla, Inc.," December 3, 2024, https://www.ftc.gov/system/files/ftc_gov/pdf/Mobilewalla-Complaint.pdf

72. Id.

73. ACLU of Washington, "The Harms of Data Abuse," January 29, 2021, https://www.aclu-wa.org/publications/harms-data-abuse/

74. Federal Trade Commission, "FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to

Set Individualized Consumer Prices," January 17, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer

75. Consumer Financial Protection Bureau, U.S. Department of Justice Civil Rights Division, Equal Employment Opportunity Commission, and Federal Trade Commission, "Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems," April 25, 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf
76. U.S. Department of Justice, "Justice Department Secures Groundbreaking Settlement Agreement with Meta"
77. Federal Trade Commission, FTC Surveillance Pricing 6(b) Study
78. Id.
79. U.S. Department of Justice, "Justice Department Secures Groundbreaking Settlement Agreement with Meta"
80. Id.
81. Id.
82. Wrabetz, "What Is Inferred Data and Why Is It Important?"
83. Federal Trade Commission, FTC Surveillance Pricing 6(b) Study
84. Washington State Attorney General's Office, "2025 Data Privacy Survey Results"
85. Id.
86. Id.
87. Id.
88. Id.
89. Id.
90. Id.
91. Id.
92. Id.
93. Id.
94. Id.
95. Id.
96. Id.
97. Id.
98. European Commission, "Data Protection Explained," https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en
99. Id.
100. Id.
101. European Commission, "Ten Years of the GDPR: Your Data, Your Rights," May 22, 2026, https://commission.europa.eu/news-and-media/news/ten-years-gdpr-your-data-your-rights-2026-05-22_en
102. Congressional Research Service, "Preemption and Privacy Law," August 29, 2025, https://www.congress.gov/crs-product/R48667
103. U.S. Department of Health and Human Services, Office for Civil Rights, "The HIPAA Privacy Rule," September 27, 2024, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

104. U.S. Department of Education, Student Privacy Policy Office, "FERPA," https://studentprivacy.ed.gov/ferpa

105. Federal Trade Commission, "Children's Privacy," https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy

106. California Privacy Protection Agency, "Frequently Asked Questions," https://cppa.ca.gov/faq

107. Colorado Attorney General's Office, "Colorado Privacy Act," https://coag.gov/resources/colorado-privacy-act/

108. Oregon Department of Justice, "The Oregon Consumer Privacy Act," https://www.oregon.gov/rea/newsroom/pages/2025-oren-j/the-oregon-consumer-privacy-act.aspx

109. Connecticut Office of the Attorney General, "The Connecticut Data Privacy Act," https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act

110. International Association of Privacy Professionals, "U.S. State Privacy Legislation Tracker," updated June 29, 2026, https://iapp.org/resources/article/us-state-privacy-legislation-tracker

111. Washington State Legislature, "Chapter 19.255 RCW: Personal Information—Notice of Security Breaches"

112. Washington State Legislature, "RCW 42.56.590: Personal Information—Notice of Security Breaches"

113. Washington State Legislature, "Chapter 28A.604 RCW: Student User Privacy in Education Rights"

114. Washington State Legislature, "Chapter 19.375 RCW: Biometric Identifiers"

115. Washington State Legislature, "Chapter 19.373 RCW: Washington My Health My Data Act"

116. Washington State Legislature, "Chapter 10.130 RCW: Automated License Plate Reader Systems"

117. Washington State Legislature, "Chapter 70.02 RCW: Medical Records—Health Care Information Access and Disclosure," https://app.leg.wa.gov/RCW/default.aspx?cite=70.02&full=true

118. Washington State Legislature, "Chapter 19.182 RCW: Fair Credit Reporting Act," https://app.leg.wa.gov/RCW/default.aspx?cite=19.182&full=true

119. Washington State Legislature, "Chapter 19.215 RCW: Disposal of Personal Information," https://app.leg.wa.gov/RCW/default.aspx?cite=19.215&full=true

120. Washington State Legislature, "Chapter 42.56 RCW: Public Records Act," https://app.leg.wa.gov/RCW/default.aspx?cite=42.56&full=true

121. Washington State Legislature, "Chapter 19.373 RCW: Washington My Health My Data Act"

122. Washington State Legislature, "Chapter 10.130 RCW: Automated License Plate Reader Systems"

123. Washington State Legislature, "Chapter 19.255 RCW"; Washington State Legislature, "RCW 42.56.590."

124. Washington State Office of the Attorney General, "2025 Data Breach Report"

125. Washington State Legislature, "Chapter 19.373 RCW: Washington My Health My Data Act"

126. Washington State Legislature, "Chapter 10.130 RCW: Automated License Plate Reader Systems"

127. Washington State Legislature, "Chapter 19.375 RCW: Biometric Identifiers"

128. California Privacy Protection Agency Enforcement Division, "Enforcement Advisory No. 2024-02"

129. Connecticut General Assembly, "Conn. Gen. Stat. § 42-520: Controllers' Duties," https://www.cga.ct.gov/current/PUB/chap_743jj.htm

130. Oregon State Legislature, "ORS 646A.578: Duties of Controller; Prohibitions; Privacy Notice to Consumer," https://www.oregonlegislature.gov/bills_laws/ors/ors646a.html

131. Colorado Attorney General's Office, "Universal Opt-Out and the Colorado Privacy Act," https://coag.gov/opt-out/

132. Federal Trade Commission, “Protecting Personal Information: A Guide for Business”

133. California Privacy Protection Agency, “Frequently Asked Questions”

134. Colorado Attorney General’s Office, “Colorado Privacy Act”

135. Connecticut Office of the Attorney General, “The Connecticut Data Privacy Act”

136. Oregon Department of Justice, “The Oregon Consumer Privacy Act”

137. California Privacy Protection Agency Enforcement Division, “Enforcement Advisory No. 2024-01: Applying Data Minimization to Consumer Requests,” April 2, 2024, https://cppa.ca.gov/pdf/enfadvisory202401.pdf

138. Oregon Department of Justice, “Privacy Law FAQs for Businesses,” https://www.doj.state.or.us/consumer-protection/for-businesses/privacy-law-faqs-for-businesses/

139. National Institute of Standards and Technology, “Facing the Facts to Keep Our Biometrics Secure”

140. Prince, “Location Data Are Revealing Health Information”

141. Washington State Legislature, “Chapter 19.375 RCW: Biometric Identifiers”

142. Washington State Legislature, “Chapter 19.373 RCW: Washington My Health My Data Act”

143. Washington State Legislature, “Chapter 10.130 RCW: Automated License Plate Reader Systems”

144. Virginia General Assembly, “Code of Virginia, Chapter 53: Consumer Data Protection Act,” §§ 59.1-575 and 59.1-578(A)(5), https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

145. Oregon State Legislature, “Oregon Revised Statutes, Chapter 646A,” ORS 646A.570(18)(a)(C) and 646A.578(2)(b).

146. Virginia General Assembly, “SB 338: Consumer Data Protection Act; Data Controller Responsibilities; Precise Geolocation Data,” 2026 Regular Session, https://lis.virginia.gov/bill-details/20261/SB338

147. Oregon Legislative Assembly, “House Bill 2008: Relating to Consumer Protection,” 2025 Regular Session, https://olis.oregonlegislature.gov/liz/2025r1/Downloads/MeasureDocument/HB2008

148. Electronic Privacy Information Center, “Data Brokers”

149. California Legislative Information, “Title 1.81.48: Data Broker Registration,” Cal. Civ. Code §§ 1798.99.80–1798.99.89, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?article=&chapter=&division=3.&lawCode=CIV&part=4.&title=1.81.48

150. Oregon State Legislature, “ORS 646A.593”

151. Texas Legislature, “Business & Commerce Code, Chapter 510: Data Brokers,” https://statutes.capitol.texas.gov/?tab=1&code=BC&chapter=BC.510&artSec=

152. Vermont General Assembly, “9 V.S.A. § 2446: Annual Registration,” https://legislature.vermont.gov/statutes/section/09/062/02446

153. New Jersey Legislature, “A5328: Regulates Data Brokers, Data Collectors, and Collection and Dissemination of Certain Sensitive Information,” P.L.2026, c.25, 2026–27 Legislative Session, https://www.njleg.state.nj.us/bill-search/2026/A5328

154. Vermont General Assembly, “9 V.S.A. § 2447: Data Broker Duty to Protect Information; Standards; Technical Requirements,” https://legislature.vermont.gov/statutes/section/09/062/02447

155. California Privacy Protection Agency, “California Data Broker Registry,” https://cppa.ca.gov/data_broker_registry/

156. Colorado General Assembly, “Senate Bill 21-190: Protect Personal Data Privacy,” §§ 6-1-1311 and 6-1-1313, https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

157. California Legislative Information, “California Consumer Privacy Act of 2018,” Cal. Civ. Code §§ 1798.185,

1798.199.40, and 1798.199.90, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&lawCode=CIV&part=4.&title=1.81.5

158. Id. §§ 1798.155–1798.160

159. Colorado General Assembly, Senate Bill 21-190, § 6-1-1309

160. California Privacy Protection Agency, “CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology, and Insurance Regulations,” effective January 1, 2026, §§ 7120–7124 and 7150–7157, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf

161. Washington Technology Solutions, Office of Privacy and Data Protection, “2025 State Agency Privacy Assessment,” April 1, 2026, https://watech.wa.gov/sites/default/files/2026-04/2025%20Privacy%20Assessment_April%202026%20FINAL.pdf

162. Id.

163. Washington Technology Solutions, Office of Privacy and Data Protection, “Government Agency Resources,” https://watech.wa.gov/privacy-data-protection/government-agency-resources

164. Washington Technology Solutions, “Privacy and Data Protection Policy,” https://watech.wa.gov/policies/privacy-and-data-protection-policy

165. Washington Technology Solutions, Office of Privacy and Data Protection, “OPDP Projects and Initiatives,” https://watech.wa.gov/privacy-data-protection/opdp-projects-and-initiatives

166. Washington Technology Solutions, Office of Privacy and Data Protection, “Privacy and Cybersecurity Best Practices,” 2021, https://watech.wa.gov/sites/default/files/2023-11/Privacy%2520and%2520Cybersecurity%2520Report%25202021.pdf

167. Washington State Attorney General’s Office, “2025 Data Privacy Survey Results”

168. Choi, H., Park, J., and Jung, Y., “The Role of Privacy Fatigue in Online Privacy Behavior,” Computers in Human Behavior, vol. 81, April 2018, pp. 42–51, https://doi.org/10.1016/j.chb.2017.12.001

169. Bauer, J.M., Bergstrøm, R., and Foss-Madsen, R., “Are You Sure, You Want a Cookie?—The Effects of Choice Architecture on Users’ Decisions About Sharing Private Online Data,” Computers in Human Behavior, vol. 120, July 2021, article 106729, https://doi.org/10.1016/j.chb.2021.106729

170. U.S. Small Business Administration, “Protect Your Small Business from Cybersecurity Attacks,” October 29, 2021, https://legacy.sba.gov/blog/protect-your-small-business-cybersecurity-attacks

171. Orr, Deborah, “Fallout: The Reputational Impact of IT Risk,” Forbes Insights, 2014, https://images.forbes.com/forbesinsights/StudyPDFs/IBM_Reputational_IT_Risk_REPORT.pdf