WASHINGTON POLICY CENTER
Improving lives through market solutions

POLICY BRIEF

Washington state small business guide to data privacy laws

Mark Harmsworth,
Director, Center for Small Business

December 2020

Key Findings

1. Data privacy law is complex and is applied to large corporations and small business equally requiring small business owners to consider the impacts to their customer data and business.
2. There are different laws governing data protection and data privacy depending on the country and geographical locality of both the customer and business.
3. There are significant fines and penalties for data breaches and non-compliance with the new data privacy laws.
4. Privacy law should include graduated compliance when crafting personal data laws to differentiate large and small companies' capabilities appropriately.
5. Small businesses (in Washington) are subject to the same regulations as larger corporations but have far fewer resources to handle the additional work needed to protect private data and to comply with data privacy laws.
6. Washington State should include language in the Washington Privacy Act for more flexibility for small business compliance, rather than taking the broad, one-size fits all approach that the General Data Protection Regulation and California Consumer Privacy Act have taken.
7. Washington Privacy Act compliance thresholds should be combined with a secondary trigger or measure to avoid penalizing small business.
8. The rules to reach compliance for small business should be more flexible than the rules applied to large business who often are able to scale to handle privacy regulations more cost effectively.
9. Provide more explanatory exception clarification for the type of data that is exempt from the privacy law.
10. Allow documentation and process compliance and not automated systems as the only solution for compliance to privacy law.

WASHINGTON POLICY CENTER
Improving lives through market solutions

POLICY BRIEF

Washington state small business guide to data privacy laws

Mark Harmsworth,
Director, Center for Small Business

December 2020

Washington state small business guide to data privacy laws

Mark Harmsworth,
Director, Center for Small Business

December 2020

Introduction

Over the last few years data privacy has been added to the cost of doing business not only in the United States, but worldwide. With high-profile data breaches becoming more common, companies are increasing their data privacy efforts and governments are introducing new data protection requirements through far-reaching statues and legislation.[1] This not only effects large corporations, but also imposes significant data privacy requirements on small business.

Small businesses in Washington are subject to the same regulations as larger corporations but have far fewer resources to handle the additional work needed to protect private data and to comply with data privacy laws.

Existing and proposed privacy law does not appropriately address the financial impact to small business of getting to compliance often forcing a business to spend tens of thousands of dollars in a short amount of time.

Small business owners need to be mindful of these statutes as they do business in Washington, in the U.S. and internationally and to adjust their business policy and practices accordingly. Even if the business is based in Washington and the customer is in a different locale or jurisdiction, there may be additional data privacy requirements with which a business will need to comply.

Background

As the internet and compute resources have become critical to running a business in Washington state, companies are often required to follow data privacy statutes passed not only in Washington, but also the statutes in force in other states and other countries.

Traditionally, data privacy was considered in the context of Personally Identifiable Information (PII), Payment Card Information (PCI), Health Insurance Portability and Accountability Act of 1996 (HIPAA) and various other data

1 "Target to pay $18.5M for 2013 data breach that affected 41 million consumers," by Kevin McCoy, *USA Today*, accessed March 15, 2020, at https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/; "California's new data privacy law the toughest in the US," by Laura Hautala, CNET accessed March 15, 2020, at https://www.cnet.com/news/californias-new-data-privacy-law-the-toughest-in-the-us/.

protection standards such as HITECH, NIST-800 and ISO/IEC 27001.[2]

However, while these statutes are essential to data protection, they focus on the protection of the data and not on the consumer rights for data that has been collected. There is a growing desire by some policy makers for additional data privacy regulation to govern the use of the data, consumers rights and the definition of who is the owner of the data. This gave rise to several new laws focused on individual privacy rights.

The first of these privacy statutes was the European Union (EU) General Data Protection Regulation (GDPR) which places requirements on data privacy and data handling on companies doing business in the EU.[3] Since many U.S. companies do business in the EU, several U.S. companies have already adopted GDPR and operate under GDPR requirements inside the U.S. to simplify their operations.[4]

In response to GDPR, several states proposed legislation that broadly follows the GDPR requirements.[5]

The first state to pass data privacy legislation was California. The California Consumer Privacy Act (CCPA) went into effect in January 2020.[6] CCPA is broadly based on the GDPR statute.

Washington state has been working on its own version of a data privacy law, the Washington Privacy Act (WPA). The Washington legislation, while still a work in progress, came close to passing during the 2020 legislative session and will be re-introduced in 2021 in some form because there is now broad legislative agreement

---

2 "Personally Identifiable Information (PII)," by Jake Frankenfield, Investopedia, accessed March 15, 2020, at https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp; "PCI Security Standards Council," accessed March 15, 2020, at https://www.pcisecuritystandards.org/; "Health Insurance Portability and Accountability Act," accessed March 15, 2020, at https://www.hipaa.com/; "NIST Special Publication 800-53," accessed March 15, 2020, at https://nvd.nist.gov/800-53; "ISO/IEC 27001 Information security management," accessed March 15, 2020, at https://www.iso.org/isoiec-27001-information-security.html; "What is the HITECH Act?" accessed March 15, 2020, at https://www.hipaajournal.com/what-is-the-hitech-act/.

3 "General Data Protection Regulation", accessed March 15, 2020, at https://gdpr.eu/.

4 "Workplace Privacy, Data Management & Security Report" by Joseph J. Lazzarotti, Maya Atrakchi and Mary T. Costigan, Jackson Lewis, accessed April 25, 2020, at https://www.workplaceprivacyreport.com/2018/01/articles/international-2/does-the-gdpr-apply-to-your-us-based-company/.

5 "US states pass data protection laws on the heels of the GDPR" by Jeewon Kim Serrato, Chris Cwalina, Anna Rudawski, Tristan Coughlin and Katey Fardelmann, Norton Rose Fulbright, accessed April 25, 2020, at https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

6 "California Consumer Privacy Act (CCPA)" accessed March 15, 2020, at https://www.oag.ca.gov/privacy/ccpa; "California passes major legislation, expanding consumer privacy rights and legal exposure for US and global companies," by Spencer Persson, Jeewon Kim Serrato, Steve Roosa, Arleen Fernandez and Anna Rudawski, Norton Rose Fulbright, accessed April 25, 2020, at https://www.dataprotectionreport.com/2018/06/california-passes-major-privacy-legislation-expanding-consumer-privacy-rights/.

on the statute's language.[7]

Many of these statutes introduce a concept called the "Right to be Forgotten". This requires companies that collect personal data to provide to the data owner, customer or employee, the policy they use to manage the data and the ability for the data to be removed from their data store and records.[8] There are severe penalties for non-compliance that can bankrupt a business.[9]

The average financial cost for a data breach in the U.S. can be as high as $150 per row of personal data.[10] The majority of the $150 is spent in notification costs, staff time and offering free credit monitoring services to the party effected by the breach. There often is an additional, significant cost associated with the damage to the business brand and reputation plus the risk of an individual or a class action lawsuit being brought against the business for damages.[11] In legislative discussions in Washington, the inclusion of the right to private action, or the ability to employ the state's office of the attorney general to pursue the case, has been a key sticking point for the passage of the legislation.

Data privacy is quite different from data protection or data security, which is traditionally focused on encryption and keeping data safe from un-authorized access, individuals or systems use. Both types of data protection have significant requirements for a business to follow to remain compliant.

The new data privacy laws have a profound effect on the way both small and large businesses operate. Businesses now need to handle private data differently than they did just a few years ago or run the risk of significant fines and penalties.[12]

Policy analysis

General Data Protection Regulation (GDPR)

GDPR is a set of regulations designed to give European Union (EU) citizens more control over their personal data. It applies to any business operating within

---

7 SB 5376, "Protecting Consumer Data," introduced January 18, 2019 at https://app.leg.wa.gov/billsummary?BillNumber=5376&Year=2019; "The new Washington Privacy Act raises the bar for privacy in the United States," by Julie Brill, Microsoft, accessed March 15, 2020, at https://blogs.microsoft.com/on-the-issues/2020/01/24/washington-privacy-act-protection/.

8 "Everything you need to know about the 'Right to be forgotten,'" accessed March 15, 2020, at https://gdpr.eu/right-to-be-forgotten/.

9 "What Are The Penalties For Non-Compliance With CCPA?" by RSI Security, RSISecurity, accessed March 15, 2020, at https://blog.rsisecurity.com/what-are-the-penalties-for-non-compliance-with-ccpa/.

10 "Cost of a Data Breach Report," by the Ponemon Institute, IBM Security, accessed April 25, 2020, at https://www.ibm.com/downloads/cas/ZBZLY7KL.

11 "Analyzing Company Reputation After a Data Breach," by Sarah Hospelhorn, Varonis, accessed April 25, 2020, at https://www.varonis.com/blog/company-reputation-after-a-data-breach/.

12 "GDPR Fines," AGDP Associates, accessed April 25, 2020, at https://www.gdpr.associates/data-breach-penalties/.

the EU, including a business located in the U.S. that offer goods or services to customers or businesses in the EU. It also applies to U.S. businesses doing business with EU residents in the U.S.

Key GDPR principles for small business

The following list covers the key GDPR requirements imposed on a business located in the U.S. The GDPR principles broadly fall into the categories of collection, use, consent, use of minor data and special cases.

Collection - Personal data shall be:

- Collected and used lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not used in a manner that is incompatible with those purposes.
- Kept up to date and accurate.
- Deleted when the data is no longer needed for its original purpose.
- Have appropriate security applied for the protection of the data.
- Protected against unauthorized or unlawful use and against accidental loss, destruction or damage.

Use - Personal data shall be only used when:

- The owner of the data has given consent to the use of his or her personal data for one or more specific purposes.
- It is necessary for the performance of a contract to which the owner has agreed or at the owners request prior to entering into a contract.
- It is necessary for compliance with a legal obligation to which the processor of the data is subject.
- It is necessary to protect the vital interests of the data owner.

Content - Before data can be collected or used:

- The data processor shall be able to demonstrate that the data owner has consented to processing of his or her personal data.
- The request for consent shall be presented in a manner which is easily accessible and using clear and plain language.
- The data owner can withdraw his or her consent for use at any time.

Minor - When dealing with children:

- Where a child is below the age of 16 years, you must get consent from the holder of parental responsibility over the child.
- The data processor shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child.

Special Cases - Processing of special categories of personal data:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited. This does not apply if:

- The data owner has given explicit consent to the use of the personal data for one or more specified purposes.
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the processor or of the data owner in the field of employment and social security and social protection law.
- Processing is necessary to protect the vital interests of the data owner.
- Processing is carried out in the course of legitimate activities with appropriate safeguards.
- Processing relates to personal data which are manifestly made public by the data owner.
- Processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for reasons of substantial public interest. The data processor still must provide measures to safeguard the fundamental rights and the interests of the data owner.

Processing which does not require identification:

If the reason the data was originally collected is no longer applicable, the data processor shall not be obliged to maintain data on the data owner.

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) was enacted in 2018 and took effect on January 1, 2020. The CCPA creates new privacy rights for California consumers.

Key CCPA Principles for Small Business

The CCPA is applied to businesses that have gross annual revenues in excess of $25 million and buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices and/or derives 50 percent or more of annual revenues from selling consumers' personal information.

The CCPA grants the following legal rights to the consumer,

- The right to know what personal information and categories of information is collected, used, shared, or sold.
- The right to delete personal information held by businesses and by extension, a business's service provider.
- The right to opt-out of the sale of personal information.
- Children under the age of 16 must provide opt in consent, with a parent or guardian consenting for children under 13.
- The right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA.

For businesses it adds the following requirements,

- Notice to consumers at or before data collection.
- Documented procedures to respond to requests from consumers to opt-out, know, and delete.
- A "Do Not Sell My Info" link on their website or mobile app.
- Businesses must respond to requests from consumers within specific timeframes.
- Verification of the identity of consumers who make requests to see or request deletion of their data.
- Disclosure of financial incentives offered in exchange for the retention or sale of a consumer's personal information and explain how they calculate the value of the personal information.

As proposed by the draft rules, businesses must maintain records of requests and how they responded for 24 months.

California Proposition 24 – Consumer Personal Information Law

Proposition 24, also known as the California Privacy Rights and Enforcement Act of 2020, expanded and amended the provisions of CCPA. It created the California Privacy Protection Agency and increased penalties on businesses that violate CCPA.

It also requires businesses to do the following,

- Not share a consumer's personal information upon the consumer's request.
- Provide consumers with an opt-out option for having their sensitive personal information used for advertising or marketing.
- Obtain permission before collecting data from consumers who are younger than 16.
- Obtain permission from a parent or guardian before collecting data from consumers who are younger than 13.
- Correct a consumer's inaccurate personal information upon the consumer's request.

The measure passed by 56% of California voters in November 2020.

Washington State Privacy Act (WPA) – *Proposed*

The proposed Washington State Privacy Act, similar to GDPR and CCPA is a consumer data rights act.[13] It would create new rights for consumers and obligations for businesses that collect personal data. An updated version was introduced on August 5, 2020 which is likely to be the basis for the 2021 WPA legislation during the 2021 legislative session.[14]

Scope of 2021 Washington Privacy Act proposal and application summary

Applies to legal entities that conduct business targeted to Washington residents and:

- Control or process personal data of more than 100,000 consumers during a calendar year or derive over 25 percent of gross revenue from the sale of personal data and process or control the personal data of over 25,000 consumers.

WPA does not apply to:

- State agencies, local governments, or tribes.
- Nonprofit corporations.

---

13 SB 6281, "Concerning the management and oversight of personal data," introduced January 14, 2020 at https://app.leg.wa.gov/billsummary?BillNumber=6281&Initiative=false&Year=2019

14 "2021 Washington Privacy Act," introduced September 9, 2020 at https://urldefense.proofpoint.com/v2/url?u=http-3A__sdc.wastateleg.org_carlyle_wp-2Dcontent_uploads_sites_30_2020_09_WPA-2D2021-2DMaterials-2DCarlyle.pdf&d=DwMFAg&c=LFYZ-o9_HUMeMTSQicvjIg&r=Ttb0dPx8vQjv9D3080UQVw&m=K4Strp90Uwpl9h7CL6-27aVZE8ZV4TBnG0z4MZnd2gU&s=ZNIizKpgDiTulJfuNbfZRSJfjewm3AcNWTnJ2pN8-mc&e=.

- Institutions of higher education.
- Municipal corporations.
- Personal data governed by certain state and federal regulations.
- Employment records.
- HIPAA data.

2021 WPA and Health Emergencies

A section was added to the proposed legislation for the use and protection of data collected for health emergencies, such as COVID-19.

Key 2021 WPA principles proposed in the draft legislation for small business

A business that conducts business in Washington for data it stores:

- When requested, confirm the data stored about a consumer and provide a copy of the data.
- Maintain accurate personal data.
- Establish, implement, and maintain reasonable administrative, technical, and physical data security practices.
- Not process personal data on the basis of a consumer's or a class of consumers' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, lawful source of income or disability.
- Delete a consumer's personal data if certain requirements are met.
- Shall not discriminate against a consumer for exercising any of the rights in the legislation.
- Inform the consumer of the third parties to which the data was disclosed.
- Restrict the use of a personal data and use the data only with the consumer's consent or for other limited reasons.
- Provide data to the consumer in a commonly used readable and portable format when requested.
- Allow the consumer to block the processing of their personal data for targeted advertising, sale of personal data and profiling in furtherance of decisions that produce legal effects.
- Respond to consumer request inquiring on the use of the consumers data within 45 days, which may be extended an additional 45 days based on the complexity and number of requests. Responses to requests must be provided

to a consumer free of charge unless the requests are excessive or repetitive.

- There must be an appeals process, conspicuously available and easy to understand, for consumers to appeal a decision made by the business on the consumers data.
- The data policy and use of data notice must be provided twice a year to the consumer.
- Provide a meaningful privacy notice. It must include the categories of personal data collected, the purposes for which the categories of personal data are used and disclosed to third parties, consumers' rights, the categories of personal data that are shared with third parties, and the categories of third parties with which the data could be shared.
- Conduct risk assessments if the data use activity includes:
  - Processing for targeted advertising.
  - Sale of personal data.
  - Processing for purposes of profiling where reasonably foreseeable risks are present.
  - Processing of sensitive data.
  - Any processing activities that present heightened risk of harm to consumers.

Once data is changed so that it is pseudonymous and no longer can be traced back to the original data owner, the proposed WPA controls for consumer data no longer apply. However, a controller that uses pseudonymous data or deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data are subject.

Recommendations for changes to GDPR and CCPA

The underlying principles for General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) focus on granting consumers and employees the right to ask a business what data it has stored on the consumer or employee, how it is used and the procedure by which to remove it when the relationship with the business ends.

Lawmakers who are refining and passing new laws governing the use and protection of personal data should consider the different impact the legislation would have on small business owners compared to larger corporations.

In summary new privacy proposals should:

- Consider economic impact differences from rule requirements between large corporations and small business.
- Allow additional time for compliance for small business.
- Provide broad policy goals, not specific implementation requirements.

- Consider minimum or graduated thresholds and compliance mechanisms before compliance becomes mandatory.
- Provide clear consumer notification requirements.

Current GDPR and CCPA law gives little flexibility to small businesses who may not have the same resources as a larger company to meet compliance.

In some cases, a change that would cause no cost or only minor disruption to a corporation, can place a huge burden on a small business owner. Reasonable accommodations should be made to allow a business to protect personal data and be in-compliance without significant impact to business operations.

As an example, consider the deletion of data from systems, including backups of that data once a relationship has ended with the consumer or employee. In many larger companies that deal with significant amounts of data across state and country boundaries, this process is well documented and often automated. The amount of data the corporation stores drives the need to automate processes to achieve economies of scale and is considered part of the cost doing business with large datasets. These automated systems cost significant capital to develop both in monetary and employee cost.

In the case of a smaller business, it is not cost effective to invest significant amounts of development time and capital into building systems to automatically remove data. The deletion process is often a manual, repeatable written procedure, and takes significantly less staff time and effort than an developing an automated system. Allowing additional time for small businesses to complete tasks required to remain compliant would be a good compromise to reduce operational impact on the business.

Broad rule definitions should be adopted that detail compliance goals, not specific implementation requirements. As an example, the NIST SP 800-53, Security and Privacy Control states for compliance:

a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and

b. Reviews visitor access records [Assignment: organization-defined frequency].[15]

This rule gives business owners flexibility in implementation. A large corporation may choose to deploy an automated system such as a card key entry to record visitors to the facility. For a small business, this can be as simple as a clipboard and a written procedure on its use.

Providing clear exemptions to allow a small business to be compliant through a combination of process documentation and system processes and not requiring automated systems would reduce the compliance burden on the business.

Exemption clarification for data collection where the data is not stored on any business systems and only consumed by third party processors need to be clearly

15 "NIST Special Publication 800-53 (Rev. 4)," accessed March 28, 2020, at https://nvd.nist.gov/800-53/Rev4/control/PE-8.

defined. As an example, in a retail transaction collected at the point of sale, the retailers often do not collect the payment nor customer information. The data is sent directly to the payment processor.

This type of customer interaction should be documented as a clear exemption, and the conditions to qualify for the exemption in the rules since the data is never stored in systems the retailer owns or has control over.

Lawmakers should consider minimum or graduated thresholds before all the elements of the statutes are enforced.

Consider the sole proprietor who may have 50,000 customers for marketing purposes in a small database or spreadsheet. The data should be protected against unreasonable access through reasonable encryption standards but a written policy describing how data is removed when requested, would be sufficient rather than an automated system for removal. Likewise, annual risk assessments, that can cost over $10,000, would be overkill for a simple spreadsheet. While the sole proprietor is subject to CCPA for the 50,000 rows of data, financially no other thresholds are met.

Another example is a data analytics company that could fall below an annual revenue monetary threshold, but often has millions of rows of data purchased from other companies. Again, the data needs to be protected and encrypted, but it is impractical for the business to notify every user in a database that the business has their data. A dataset could be retained by that business for multiple uses. Under the current CCPA statute (section 1798.100), it is unclear on the definition of transient use and when notification requirements would be triggered.[16]

The current CCPA thresholds have not considered real-life use of data and will cause significant financial impacts to a business to reach compliance.

Small business owners located and operating primarily in Washington state should assume that statutes like GDPR and CCPA will be enforced in the protection of data they collect and store on their employees and customers even though the statute was developed outside of Washington state.

Recommendations for WPA

Washington State should include language in the WPA for more flexibility for small business compliance. Rather than taking the broad, one-size fits all approach GDPR and CCPA have taken, Washington State should,

- Consider economic impact to small business and provide allow additional time for compliance.
- Provide broad policy goals, not specific implementation requirements.
- Consider more reasonable minimum or graduated thresholds before compliance becomes mandatory.

16 "California Consumer Privacy Act of 2018," accessed September 9, 2020, at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

- Provide exemptions for written policy, documentation, and annual compliance reporting under minimum thresholds.

- To avoid frivolous litigation, not include a private right of action.

In addition to the GDPR and CCPA recommendations made earlier in this document, the WPA threshold for personal data set at 100,000 rows of data will hurt many small businesses. Exceeding 100,000 rows triggers compliance to the complete WPA, there is no graduated compliance requirements or exemptions. The 100,000-row threshold should be combined with a secondary trigger, such as gross revenue set at a sufficiently high level, to avoid penalizing small business.

Conclusion

The collection and storage of private data has requirements which, if ignored, can impose a large financial liability and cause a loss of reputation to a business in the event of a data breach. A data breach can literally put a company out of business and cause financial distress and other impacts to the owner of the data.

Recent laws such as California's CCPA increase the personal penalties for corporate officers and small business owners who either willfully or show gross negligence in the protection of personal data, demonstrate that governments are serious about enforcing data protection law.[17]

Current GDPR and CCPA law gives no flexibility to small busines who may not have the same resources as a larger company to meet compliance.

There are extensive industry-recognized standards that can be applied to a business to bring it into compliance and mitigate the risk of a data breach of personal data. Additionally, the insurance industry provides cyber insurance options that provide legal and financial support to reduce costs of a data breach, often including data security review services to reduce their own financial exposure.

Updates to GDPR, CCPA and the pending WPA privacy legislation should include:

- Flexibility to small business and not apply the same rules as are applied to large business who often are able to scale to handle privacy more cost effectively.

- Exception clarification for the type of data that needs to be excluded.

- Threshold and graduated exemptions for small business.

- Documentation and process compliance examples

- and not automated systems as the only solution.

---

17 "Business Owners face Severe Penalties due to Data Breach Incidents," George Johnson Insurance, accessed April 25, 2020, at https://www.georgejohnsonins.com/news/28/Business+Owners+face+Severe+Penalties+due+to+Data+Breach+Incidents.

The GDPR, CCPA and WPA are statutes that place data privacy protection requirements on business. They are focused on consumer data protection rights and granting consumers and employees the right to ask a business what data it has stored on the consumer or employee, how it is used and the procedure on how to remove it when the relationship with the business ends.

Small businesses in Washington are subject to the same regulations as larger corporations but have far fewer resources to handle the additional work needed to protect private data and to comply with data privacy laws.

Existing and proposed privacy law does not appropriately address the financial impact to small business of getting to compliance that often forces a business to spend tens of thousands of dollars in a short amount of time.

Lawmakers who are refining and passing new laws governing the use and protection of personal data should consider the different impact the legislation would have on small business owners compared to larger corporations.

Published by Washington Policy Center

Washington Policy Center is an independent research organization in Washington state. Nothing here should be construed as an attempt to aid or hinder the passage of any legislation before any legislative body.

Chairman	**Mark Pinkowski**
President	**Daniel Mead Smith**
Vice President for Research	**Paul Guppy**
Communications Director	**David Boze**

If you have any comments or questions about this study, please contact us at:

Washington Policy Center
PO Box 3643
Seattle, WA 98124-3643

Online: www.washingtonpolicy.org
E-mail: wpc@washingtonpolicy.org
Phone: (206) 937-9691

About the Author

Mark Harmsworth joined WPC in 2019 and became WPC's Center for Small Business Director in January 2020. He was elected in 2014 to the Washington State House of Representatives where he served two terms. His focus was on transportation and technology, including serving as the ranking member on the House Transportation Committee.

Prior to the legislature, Mark served two terms on the Mill Creek City Council and was elected Mayor Pro-Tem in his last year.

He recently finish serving as a Director on the Everett Community College Foundation Board and currently serves as a Director on the Boys and Girls Club of Snohomish County.

Mark works in the technology industry and is an owner of a small business after completing a long career at Microsoft and Amazon.

Mark and his family live in Mill Creek, Washington.