ironwall
by Incogni

The (positive!) impact of consumer privacy legislation on small businesses

Summary

Businesses today collect and have access to a wealth of customer information. For the past two decades, the widespread commercial use of personal data has grown with little to no restriction over what can be acquired, shared or sold. But that is now changing due to consumer mistrust, government action, and competition for customers.

Large corporations, particularly data brokers, have lobbied against online data privacy laws, and many small businesses have been recruited to join this crusade. However, the majority of these small companies would not be affected by the legislation being considered in several states, and would actually benefit from their provisions.

As large companies trade, collect, and monetize data, they often handle it carelessly or fall victim to hacks. This leads to more phishing and ransomware attacks, which disproportionately harm smaller companies that lack the resources to defend against data breaches. These attacks also put employees at risk, exposing them to personal harassment, identity theft, and other threats.

This whitepaper explains how current and pending legislation impacts small businesses, and why supporting these bills – rather than opposing them – offers significant advantages in security and customer retention.

Online Consumer Data Protection is Coming

Privacy was not a primary concern as the internet evolved from a novelty into what has become, for most of us, our primary conduit for communication, business, commerce, and entertainment. As we willingly entered whatever personal information was requested by whatever website we were on, we didn't consider how that data could be exploited – or weaponized. We just wanted an easier way to pay the power bill or order a pizza.

But, as with most things that come easily, there were consequences.

Companies shared or sold customer lists; data brokers acquired this content and supplied them to people-finder websites. Judges have been murdered at their homes by disgruntled defendants who found their addresses online. Police officers and election workers have been doxed. Cases of identity theft proliferated, along with annoying robocalls and online scams.

"We have these companies that are amassing just gigantic amounts of data about each and every one of us, all day, every day," said Kate Ruane, senior legislative counsel for the First Amendment and consumer privacy at the American Civil Liberties Union.

"Your data is being taken and it is being used in ways that are harmful." [1]
Given these inconvenient yet undeniable truths come to light, and more people realize their privacy has been compromised, public opinion has shifted in favor of data privacy legislation.

Europe has been ahead of the US on this challenge with the 2016 enactment of the EU's General Data Protection Regulation (GDPR), one of the few laws that successfully champion user data ownership. California followed suit with the California Consumer Privacy Act (CCPA), granting residents various rights over their personal data, including the right to know what information is being collected, processed, and sold, as well as the ability to request that business delete any collected personal data.

Other states have followed suit, with laws already passed or legislation pending. A flurry of bills have been introduced over the past two years, and by 2026 it is almost certain that states in more than half the country will provide their residents with more authority over how their personally identifiable information (PII) is handled.

Small Business Concerns

In states where legislation is currently pending, some small businesses have expressed unease over the passage of data privacy legislation, and how it would impact customer insights and targeted marketing, as well as concerns over the cost of compliance.

Chambers of Commerce have spearheaded these efforts, warning that such legislation would encourage an influx of abusive class action lawsuits, create further confusion regarding enforcement of privacy rights, and hinder data-driven innovation.

There is no dispute about whether the issue of personal privacy and information security will have some impact on small businesses as digital data grows in importance. Even if a website is simply a landing page with a company's fixed address, attention must be paid to how a company browses, sends, and receives data online.

However, in most cases, the laws that have passed or are now under consideration would not apply to the overwhelming majority of small businesses. In Vermont, for example, the law applies only to businesses that make a majority of their revenue selling data, as well as large data holders, which are companies processing data from 100,000 Vermonters or more a year.

Most small businesses would be exempt from the requirements of these bills; while enjoying the benefits they provide (see chart).

Consumer privacy laws are already in place in several states. There has been no negative impact on small businesses – but many security advantages.

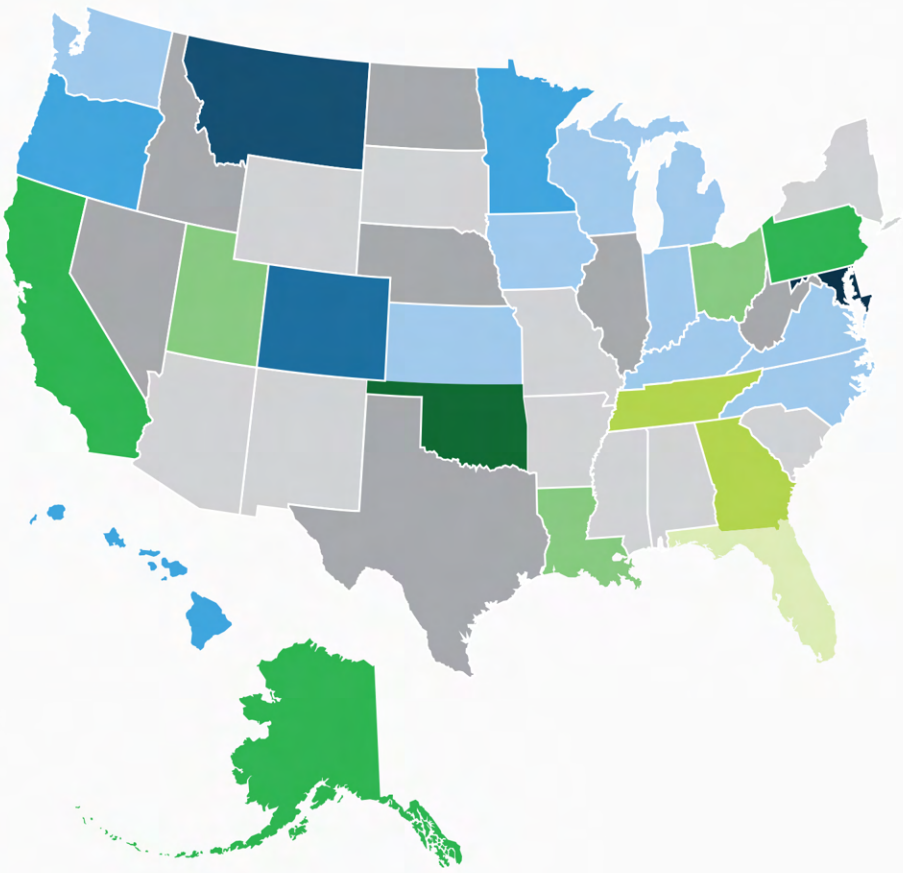
And since this legislation impacts only personally identifiable information, with today's technology it is possible to acquire insight from data on everything from demographics to shopping, all while never acquiring, selling or transferring the data itself.

---

[1] https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

CONSUMER PRIVACY LAWS BY STATE

Thresholds by revenue and number of records controlled



Threshold includes gross annual revenue:

- >$10 mil
- >$25 mil AND controls 100,000+ consumer records per year
- >$25 mil AND controls100,000+ consumer records per year, OR derives >50% of revenue from selling the personal data of 25,000+
- >$25 mil AND controls175,000+ consumer records per year, OR derives >50% of revenue from selling the personal data of 25,000+
- At least $1 billion in global gross revenue

Number of consumer records controlled or processed per year:

- At least 35,000
- At least 50,000
- At least 100,000 OR derive revenue (or receive discounts) from selling personal data of at least 25,000 consumers.
- At least 100,000 OR derive over 25% of revenue from selling the personal data of at least 25,000 consumers
- At least100,000 OR derive over 50% of revenue from selling the personal data of at least 25,000 consumers

- Privacy law doesn't have threshold numbers
- No specific privacy laws

Georgia
Control or process personal information of at least 25,000 Georgia residents and derive more than 50% of gross revenue from sale of personal information; OR control or process personal information of at least 175,000 Georgia residents

Maine
The Maine privacy law applies to providers of Internet access services. Internet access services are defined as "mass-market retail service by wire or radio that provides the capability to transmit or receive data from all Internet endpoints"

Maryland
OR control or process personal data of 10,000 Maryland consumers and derive more than 20% gross revenue from the sale of personal data.

Massachusetts
OR collects and sells sensitive or personal information of at least 10,000 individuals

Montana
OR controls or processes personal data of not less than 25,000 Montana residents AND derives more than 25% of its gross revenue from the sale of personal data (excludes payment transactions)

New Hampshire
OR control or process personal data of 10,000 unique New Hampshire consumers AND derive more than 25% of gross revenue from the sale of personal data

Oregon
Excludes personal data controlled or processed solely for the purpose of completing a payment transaction

Pennsylvania
OR derives 50% or more of annual revenues from selling consumers' personal information

Delaware & Rhode island
OR controlled or processed the personal data at least 10,000 consumers and derived more than 20% of their gross revenue from the sale of personal data (excludes payment transactions)

Florida
50% of global gross revenue comes from the sale of advertisements online, OR operates a digital distribution platform or app store that has at least 250,000 different software applications, OR operates a voice command service or consumer smart speaker

California
OR at least 50% of annual revenue comes from selling or sharing personal information, regardless how much revenue you make in total.

Connecticut
25,000 or more consumers and derived over 25% of gross revenue from the sale of personal data over the last calendar year

Where Do These Objections Really Come From?

There is some question as to whether the loudest apprehensions are truly emerging from neighborhood shops and restaurants.

Chambers of Commerce and groups promoting this argument also advocate for larger businesses, including data brokers, and derive most of their revenue from these clients. Such companies – particularly data brokers that subsist on the collection and sale of PII– do not engender admiration from the public, so they advance their cause by recruiting other companies to make their case for them.

Whether small business advocates genuinely fear consumer privacy legislation, or are acting as sympathetic fronts for those profiting from personal data collection, their efforts are likely doomed to fail. Regardless of their current beliefs, that failure will ultimately benefit the very businesses they've worked so hard to build.

Data Privacy Protection Also Protects Your Business

Privacy legislation is intended to help consumers and small businesses protect themselves and lower their exposure to various online threats. It is imperative to stop companies from indiscriminately selling PII without consent or proper oversight.

Business owners are not immune from the risks everyone faces from data exposure. Their home addresses are easily accessible as well. Is that a comforting thought? Anyone can now find out where you live, and then connect that data other personal details about you and your family, just by obtaining your cell phone number.

In these contentious, quick-to-anger times, when one customer's negative experience can be instantly shared with thousands on social media, this is a potential threat to any public- facing business. Do you want an angry customer showing up at your home?

The accessibility of this content also puts businesses at greater risk for identity theft, phishing attacks, and other online scams that impact millions of Americans every day.

While ransomware attacks against major corporations, municipalities and healthcare organizations make national headlines, the attacks on small businesses are far more numerous, and just as crippling.

According to Michael Kaiser, Executive Director of the National CyberSecurity Alliance, "Nearly half of all cyber-attacks target small businesses."[2] Smaller companies are easy targets, as most are either unaware of their vulnerability, or don't invest in the right security software and training to minimize these problems. That is why more than 80% of attacks target companies with fewer than 1,000 employees. Email-based attacks (malicious emails or phishing) have become the starting point for more successful breaches.

"Our Employees Wouldn't Fall For That"

Don't be too sure. Hackers have come a long way from the obvious scams they tried ten years ago. Today, they are leveraging artificial intelligence's adaptability along with the copious amounts of personal data freely available on the internet. This allows thieves to tailor highly personalized and remarkably convincing emails.

Using advanced techniques, they generate scam messages that are personalized with the recipient's name, address, family members, hobbies, mobile number, and even incorporate personal photos and videos. This level of personalization was not possible even two years ago.

If someone receives an email that includes their relatives' names, or photos and videos of family members, it's easier to believe its possible authenticity. If that employee clicks on the link in the email, their device is compromised, which then jeopardizes the business network. This breach typically leads to exposed bank or investment account numbers, as well as social security numbers, and can trigger lawsuits, insurance claims, negative media coverage, and more headaches than a business owner can even imagine.

Consumer data privacy legislation provides a means to request that personal data on business owners and personnel be removed online. Doing so can be a time-consuming process, but companies like Ironwall by Incogni specialize in personal data search and removal.

Once that content is removed, there are ways to prevent new content from showing up; tools such as a VPN and VoIP numbers can replace authentic information (i.e. phone numbers, online search and browsing history) with content that cannot be traced back to an individual user.

Not every business will take these steps, which gives those that do an advantage since hackers, regardless of whatever IT skills they have acquired for their trade, are also lazy. They will seek out targets where the most content on the most individuals can be accessed and weaponized. If enough details about your personnel cannot be easily collected for a phishing attack that is likely to succeed, they will turn their attention elsewhere.

Your Customers Want This

Business owners should also consider that, regardless of their personal misgivings, data privacy is something their customers want, and with good reason.

---

[2] https://www.namecheap.com/guru-guides/a-guide-to-online-privacy-for-your-small-business/

According to a 2024 Gartner survey:

- 84% of Americans are concerned about the security and privacy of their personal data online.
- 79% of Americans say they are somewhat or very concerned about the way businesses use their personal data.

Contrast these numbers with the finding that just 26% of consumers say they understand how their data is used by businesses.

- 74% of Americans feel the government is failing to protect their personal data online.

The passage of consumer privacy legislation will help to alleviate this concern.

- 32% of Americans don't trust businesses to use their personal data ethically.
- 37% don't trust that businesses will not share their personal data without permission.
- 69% said they'd be likely to shop elsewhere if they disagreed with a business's data privacy terms.

These results do not mean that consumers are always opposed to businesses sharing their data. The same survey found that:

- 60% are willing to share data if businesses were more upfront about how it would be used
- 63% would do so if they had a clearer understanding of the benefits of sharing data

Why is data security and privacy such a concern for Americans? Perhaps because the majority of survey respondents (70%) have been cybercrime victims. That is enough to make anyone think twice about what their personal data is being used for whenever providing a phone number or email address, in person or online. [3]

"Prioritizing data protection ensures legal compliance, financial stability, and sustained reputation, fostering a culture of trust among customers and stakeholders. This is important to businesses of all sizes because legal, financial, and reputational repercussions can have a severe negative impact on any business. Those that fail to adhere to privacy laws can face costly (and possibly critical) fines. Data breaches can also lead to loss of customer trust and loyalty, as well as businesses incurring costs for data recovery, legal actions, and reputation management in the aftermath of a breach." – Gregory Manwelyan, Data Privacy Attorney, CIPP/U.S. [4]

Concerned About Cost?

Consider how much instant access to personal content is costing you right now. Businesses now need to protect themselves with cyber insurance, identity theft insurance, and other remediation services. In some areas, the cost of cyber insurance has escalated by as much as 70%, a reality that is indicative of the rising data breach threat level.

Businesses that choose to risk not having this protection, do so despite the fact that the average price of a data breach in 2023 was $4.45 million, representing a 15% increase over three years. There is also a reputational cost in negative customer perception.

Conclusion

Data privacy is a matter we should all take seriously. Most current and pending privacy legislation will have minimal negative impact on small businesses while providing protections customers want and business owners need to reduce their risk of phishing or ransomware attacks. Whatever the future holds for data privacy, every business is responsible for safeguarding customer data to stay compliant and maintain customer trust.

ironwall
by Incogni

[3] https://www.usatoday.com/money/blueprint/business/vpn/data-privacy/

[4] https://termly.io/resources/articles/why-is-data-privacy-important/