How to Balance Data Privacy and Personalization

March 6, 2024

Allison Olson
SVP, Media Analytics

Ray Owens
EVP, Customer Intelligence

This blog has been updated to include information regarding the new privacy laws in Nevada and Washington being implemented in 2024.

Online privacy is an increasing concern for consumers across the globe. People want to know if and how businesses are protecting their rights to privacy, and clear data privacy practices provide transparency and can help establish trust. With the ever-evolving privacy legislation landscape, learn how to establish foundational consumer data practices that build security for your company and customers, including implementing ways to opt out of data collection entirely.

As you keep your customers' data privacy in mind, maintaining a certain level of personalization in your marketing and advertising by using the data you do have access to is still important to running an effective campaign.

To a certain extent, we expect brands and advertisers to know our interests well enough to target us with ads for products we are interested in. As a consumer, It can be frustrating to be targeted with ads for wildly irrelevant products — ex., it's a waste of both time and marketing dollars to surface car-related ads to someone without a driver's license.

There is a balance between knowing people well in order to provide them with something useful and knowing too much about someone to the point where it raises privacy concerns over just how much data they're making use of.

Changes to data privacy legislation in the United States

Over the past few years, five states enacted new privacy legislation that dramatically alters what data can be collected by businesses on individuals in those states. The states and legislation in question include:

- California Privacy Rights Act (CPRA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)
- Connecticut Data Privacy Act (CTDPA)

- Utah Consumer Privacy Act (UCPA)

Each of these acts went into full effect on January 1, 2023, and restricts the collection of personal data, including genetic or biometric data, precise geolocation data, information that reveals race, religious beliefs, sexual orientation, immigration status, and more.

These laws are a continuation of ongoing changes to privacy protections in the United States and beyond, most notably the General Data Protection Regulation (GDPR). These protections were implemented in 2018 in the European Union and are key to understanding the current privacy law landscape in the US.

Nevada and Washington also passed data privacy laws in 2023 that will go into effect on March 31st, 2024.

Passed in April of 2023, Washington's My Health My Data Act (MHMD) will affect regulated entities at the end of March, and smaller entities at the end of June. The MHMD Act extensively defines consumer health data, which "includes information that is derived or extrapolated from nonhealth data when that information is used by a regulated entity or their respective processor to associate or identify a consumer with consumer health data".

This means that if a company or organization uses data that is not inherently health-related to make assumptions about or identify health information—especially when combined with actual health data—it becomes subject to regulations around privacy and protection of consumer health data.

MHMD also protects consumer's biometric data. This data can include:

- Imagery of the iris, retina, fingerprint, face, hand, palm, and voice recordings
- Keystroke patterns or rhythms that may contain identifying information
- Buying, renting, accessing, retaining, receiving, acquiring, inferring, deriving, or otherwise processing any consumer health data

Nevada's consumer health privacy law takes a broader, more business-focused approach than Washington's MHMD. Nevada's Senate Bill 370 (SB 370) will apply to "regulated entities", requiring them to publish consumer health privacy data policies that include, but aren't limited to:

- Categories of consumer health data collected
- Categories of consumer health data shared with other entities
- Purposes for collecting, using, and sharing consumer health data
- Whether third parties "may collect consumer health data over time and across different Internet websites or online services when the consumer uses any Internet website or online service of the regulated entity"

Regulated entities need to obtain clear and voluntary permission from consumers before sharing their health data. They should only gather the data that's truly needed or legally mandated, and they can't sell that data without a written agreement.

Core to the protections established by this regulation is the right for people to be forgotten, particularly online. It, as well as the new laws enacted in the US, Japan, Brazil, and more countries around the globe, seeks to grant people tools to choose whether or not certain data can be collected and used by businesses and organizations. Understanding and internalizing these changes is important to ensure your business is fully compliant if you operate in any of these states.

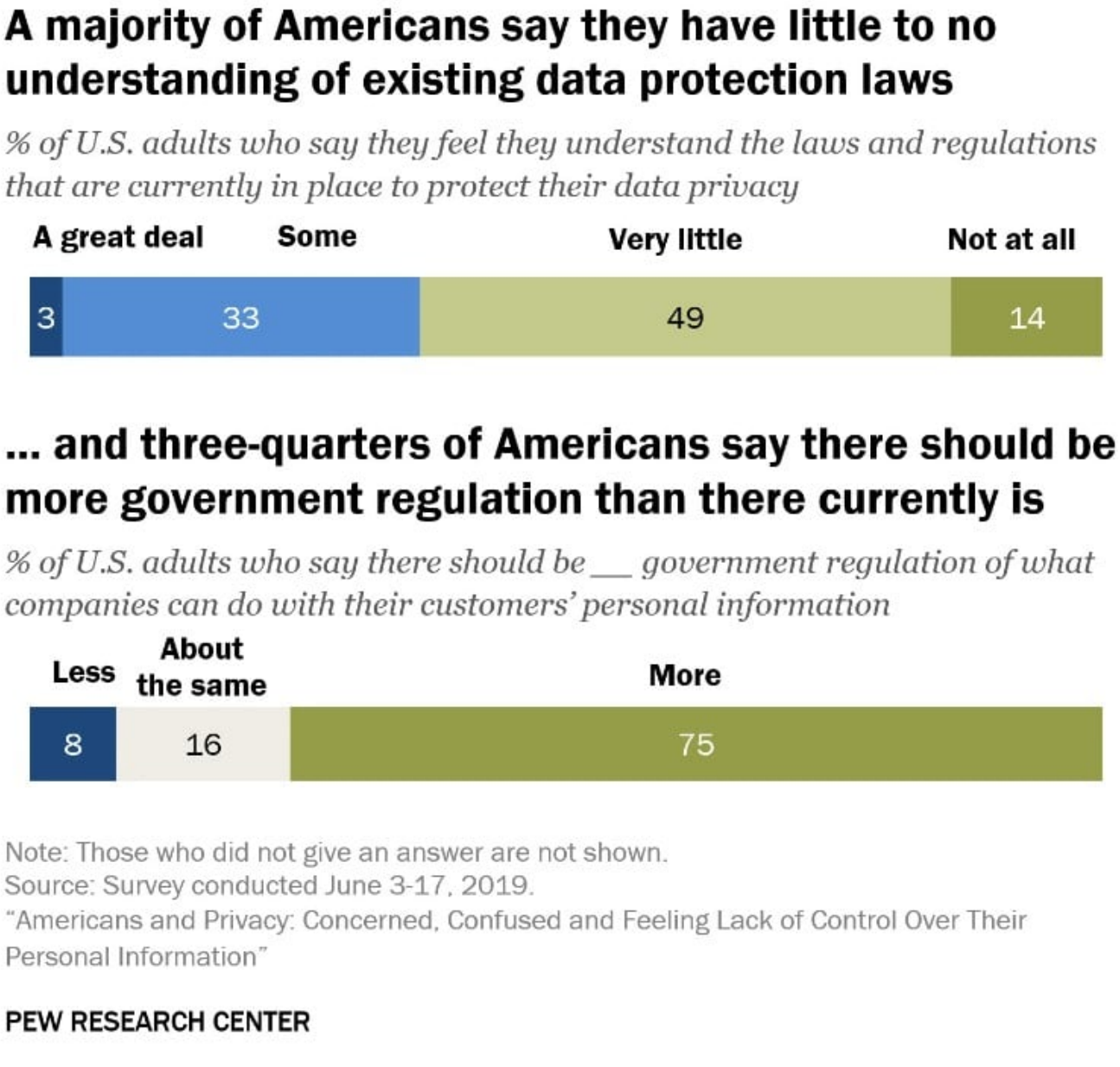
Still, it only represents part of the picture — allowing people the option to opt out of data collection as well as certain types of targeted marketing can benefit your bottom line. There's a high likelihood that the people who take advantage of these tools were never going to respond favorably to those types of advertisements in the first place.

Protecting Customer Data Needs to Be the Core Focus

When you take a broader look at the privacy laws passed in recent years, like do not call, do not mail, etc., they share a common trait. They're all about giving consumers the opportunity to use tools to protect themselves and their personal information from being used in ways they don't consent to.

Granting consumers this level of control over whether or not their data is collected has been a growing topic for years. In 2019, the Pew Research Center conducted a poll that found 81% of American adults say the risks of data collection outweigh the benefits. Consumers in every industry are increasingly

savvy about their data privacy, and providing an avenue for them to protect their personal information can be beneficial to your business.



Protecting consumer data has been a key concern for Americans for years now. Source: [Pew Research Center]

Data privacy needs to be a priority both for your business and for the data collection partners you work with. Do your current partners have rigorous standards in place to ensure the collected data is handled with the utmost care? Do they have processes in place to allow consumers to opt out of data

collection? How extensive are the protections granted to people who choose to opt out, and what kinds of hoops do people need to jump through to confirm their choice?

Screening for these practices when choosing which partner to work with is an important step to ensure there won't be breaches that can affect your customers' data. Even if your chosen partners meet your high standards, creating additional safeguards to closely monitor their data collection practices to ensure they're only collecting the data they say they're collecting can help you prevent data leaks that can harm your customers and your image.

Through our experience working with marketing partners in different data-conscious industries, not only is this something we've identified as a way to set yourself apart from your competition, it's something that deeply resonates with various consumer bases across industries.

How to build a comprehensive data privacy strategy

There are differences and nuances to consider in order to understand how to navigate the new consumer data protections that were recently implemented in California, Virginia, Colorado, Connecticut, and Utah. Reviewing and making adjustments to ensure your business is compliant needs to be a key step — if you aren't already compliant, there are tools available to help ensure compliance with even the strictest of these new laws.

Beyond ensuring you meet the base requirements for compliance, what extra steps is your business taking to protect consumer privacy? How are you setting yourself apart from your competitors? Implementing and enforcing stringent consumer data protection practices can signal to consumers that you're serious about their privacy. Exactly how you implement this can vary, but establishing transparency with your business's data collection practices and surfacing how that information is being used can go a long way toward earning consumer trust. As an example, here is Amsive's privacy policy which includes an opt-out option.

It's important to consumers, and it should be important to your business too. Following these practices is a clear way to set yourself apart from your competitors — it's far less common than you may think across industries. Beyond earning trust and building tools to future-proof your business from new laws and regulations that may pass in the coming years, allowing people to opt-out can also save you money. Why would you want to waste your marketing dollars on someone who doesn't want to see your messaging in the first place?

These Changing Privacy Laws Won't Necessarily Hamper Your Data-Gathering Opportunities

By focusing more on the quality of your target audience rather than just the number of eyes you can reach, you can both improve conversions and save money on your marketing budgets by narrowing the field you're trying to reach.

Even with these new restrictions in place, there's more data available on your target audience than ever before. Refining your targeting capabilities can help you reach the right people with the right message

at the right time based on the right information rather than taking a more scattershot approach to your marketing.

Building a strong marketing plan takes more than just gathering data that can help you build a picture of your ideal customer. It would help if you also had a deeper understanding of the marketing channels available to know where those people are looking. Is your target audience spending most of their time watching streaming services, or would a direct mail campaign reach them best? Would partnering with influencers on social media have more reach than an email campaign? Turning your insights into actionable plans is where the rubber meets the road and is how you can separate yourself from your competition.

While the types of data being gathered are limited through these new laws, finding the people you want to target with your marketing is still possible through the smart implementation of audience science. The key is understanding how people choose to interact with different brands rather than overly focusing on someone's precise physical location or racial ethnicity.

How are you preparing for the future of data privacy?

The data privacy landscape is constantly changing, and the introduction of new consumer protection laws should always be expected. By maintaining business practices that focus on protecting consumers first, it's possible to protect your business from future shifts to digital privacy laws. Maintain transparency on how you're collecting data and what you're using it for, and provide off-ramps for people who don't want to be the target of your brand's advertising.

Consumers are increasingly savvy about the potential risks around data collection, and showing them that you are both aware of their concerns and are taking steps to protect them is vital for businesses in every industry. Creating clear ways to opt out of having their data collected, being transparent about how you intend to use that data, and maintaining high standards of protection for the data you're trusted with can not only help increase trust from your customer base but it can also help set your business apart from your competitors without these practices in place.

Building a foundational data privacy practice is only one part of a data-centric, performance-driven strategy, giving you the power to know more and do more. Dig deeper into how AI is impacting organic and paid search, or let's talk about how to achieve more for your marketing — and your business.

Author: Ryan Smythe, Content Manager