



Quarles

**DC**BAR  
**Pro Bono Center** 40  
TRANSFORMING LIVES FOR YEARS



A Data Privacy  
Overview for  
Small  
Businesses &  
Nonprofits

**April 11, 2023**

# The Firm

Since 1892, Quarles has provided legal solutions to a wide range of clients on a national stage. Led today by a dynamic and diverse team of lawyers and business professionals, Quarles is a multidisciplinary AmLaw 200 firm with more than 500 attorneys practicing at the top of the profession in Denver, Chicago, Indianapolis, Madison, Milwaukee, Minneapolis, Naples, Phoenix, San Diego, Tampa, Tucson and Washington, D.C.



<https://www.quarles.com/>



<https://www.facebook.com/QuarlesandBrady>



<https://twitter.com/quarlesandbrady>



Search: "Quarles & Brady LLP"

# Our Team

---



Shaniya Johnson



Kiana Baharloo

Shaniya Johnson focuses on a variety of information technology transactions and data privacy and security compliance matters. Shaniya's practice focuses on aiding companies in United States and European data privacy compliance and privacy program remediations.

She also has experience working on commercial transactions, including drafting and negotiating strategic partnership agreements, MOUs, MSAs, SOWs and NDAs.



Shaniya Johnson

---

[Read More](#)

Kiana advises clients with issues regarding intellectual property (IP), data privacy and health law. She is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals.

She counsels clients on compliance with state and federal data privacy laws, including health care privacy laws. Kiana also works with startup clients to advise on the unique issues startups face in order to scale businesses.

---

[Read More](#)



Kiana Baharloo

# Presentation Outline

---



## What is Privacy Law?

An overview of Privacy Law generally.



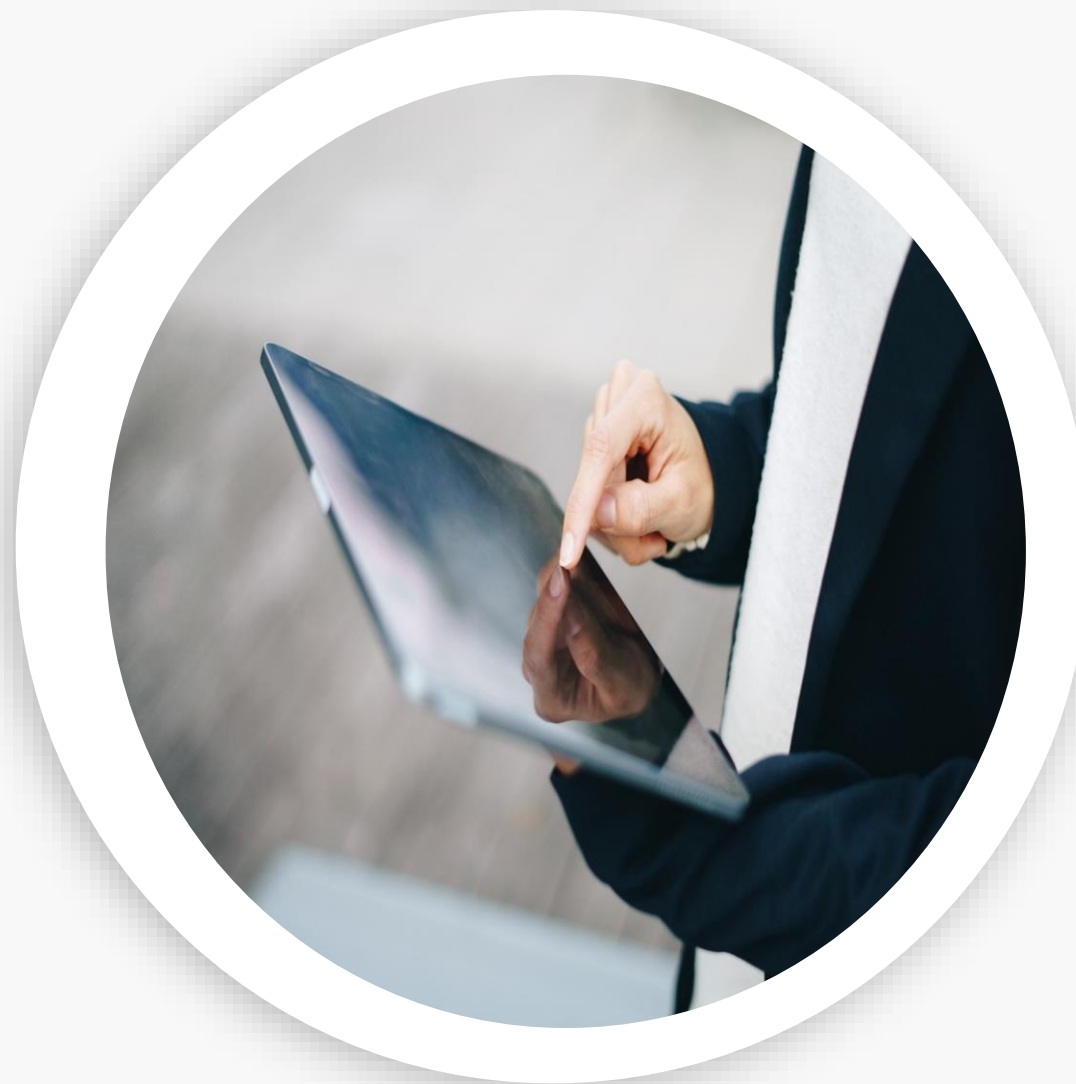
## Privacy and Small Businesses

An overview of how privacy laws can generally impact small businesses and potentially nonprofits.



## Consumer Privacy

A deep dive into consumer privacy, confidential information, and some of the privacy laws that affect consumers.



# Terminology

---

**Privacy** – The ability of individuals to exercise control over collection, use and dissemination of personal information

**Security** – measures to maintain the confidentiality, integrity, availability, access and authenticity of data

- Cannot have data privacy without data security – two sides to the same coin
- If inadequate security, by necessity will have a privacy issue.

**Cybersecurity** – focuses the data security in the technology and electronic realm.



The Internet of Things ("IoT") connects computing devices, machines, objects, animals or people with the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. In other words, **it connects things to operate together without needing humans to be present.**

## Consumer Privacy Considerations

As every day consumers adopt new technologies into their lives, new data is created.

This data is an opportunity for enterprises and companies to get to know and what you like through your interactions with technology.

This data has been valued to be worth more than

**\$214B**

in 2022.

# Interactive Walkthrough

## iPhone Safety Check

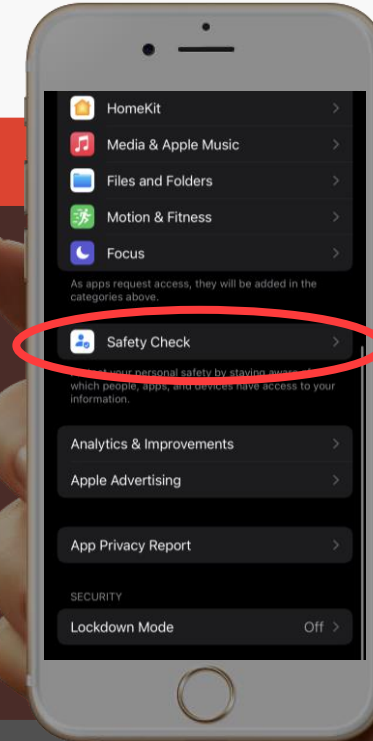
**73%** Of the global population admits to not knowing what happens with their data.

**Let's take a second to run a data privacy safety check. iPhones make this really easy and accessible. If you have an iPhone:**

1. Please open your settings.
2. Either search for "Privacy & Security" or Look for it in the menu
3. Scroll down to "Safety Check".

**If you have an Android device:**

1. Please open your settings.
2. Either search for "Security & Privacy" or Look for it in the menu
3. Scroll down to "App security" and run a check on your device.

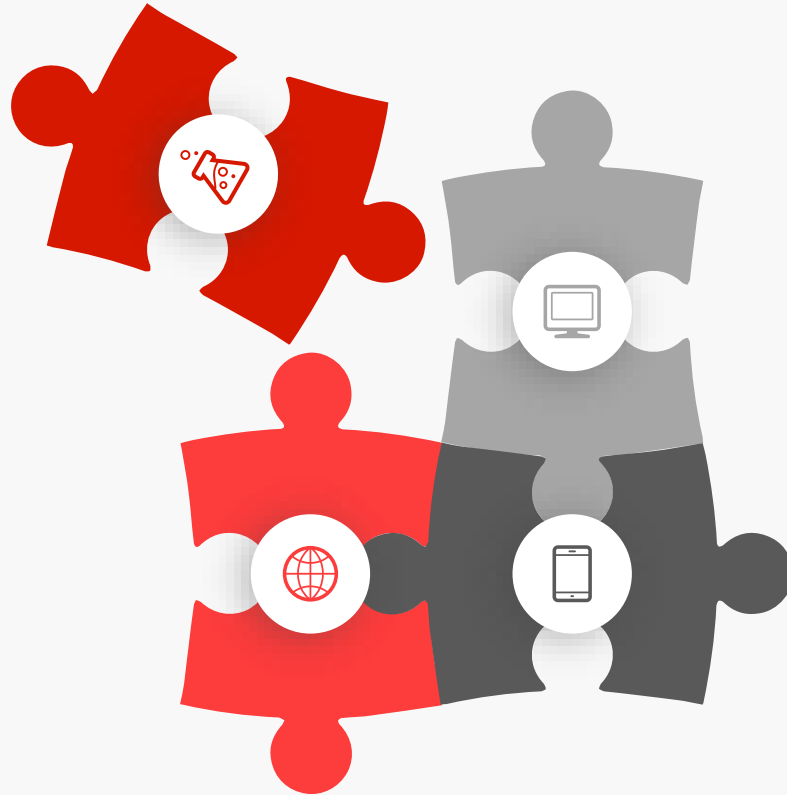


[Read More](#)

# PRIVACY LAW

---

Privacy laws are laws that deal with the regulating, storing, and using of specific types of Information. This information is usually, personal information, protected health information, and financial Information of individuals.



There is no “one size fits all” approach to privacy.

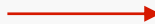
Different entities are subject to different laws based on a variety of factors.

This presentation is intended to provide a general background, and not legal advice.

# Types of Information

---

- **Personal Information:** This definition varies among laws. Typically, any information that can be linked or reasonably linked to an individual (subject to specific exceptions).
- **Sensitive Personal Information:** This definition varies among laws. Examples are social security number, financial account information, precise geolocation data, genetic data, as well as data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status.
- **Confidential Information:** Information that may or may not include Personal Information, but that must be held in confidence. This usually consists of proprietary or business information, and typically requires additional contractual agreements (e.g., an NDA). Some other examples include, customer lists, marketing plans, employee records, HR files, investment information and more.



• **Protected Health Information (PHI):** Individually identifiable health information (as defined in HIPAA, where state privacy laws typically reference this definition).

• **Financial Information:** Nonpublic financial information (generally, privacy laws carve out information that is otherwise regulated by the GLBA and other financial institution laws).

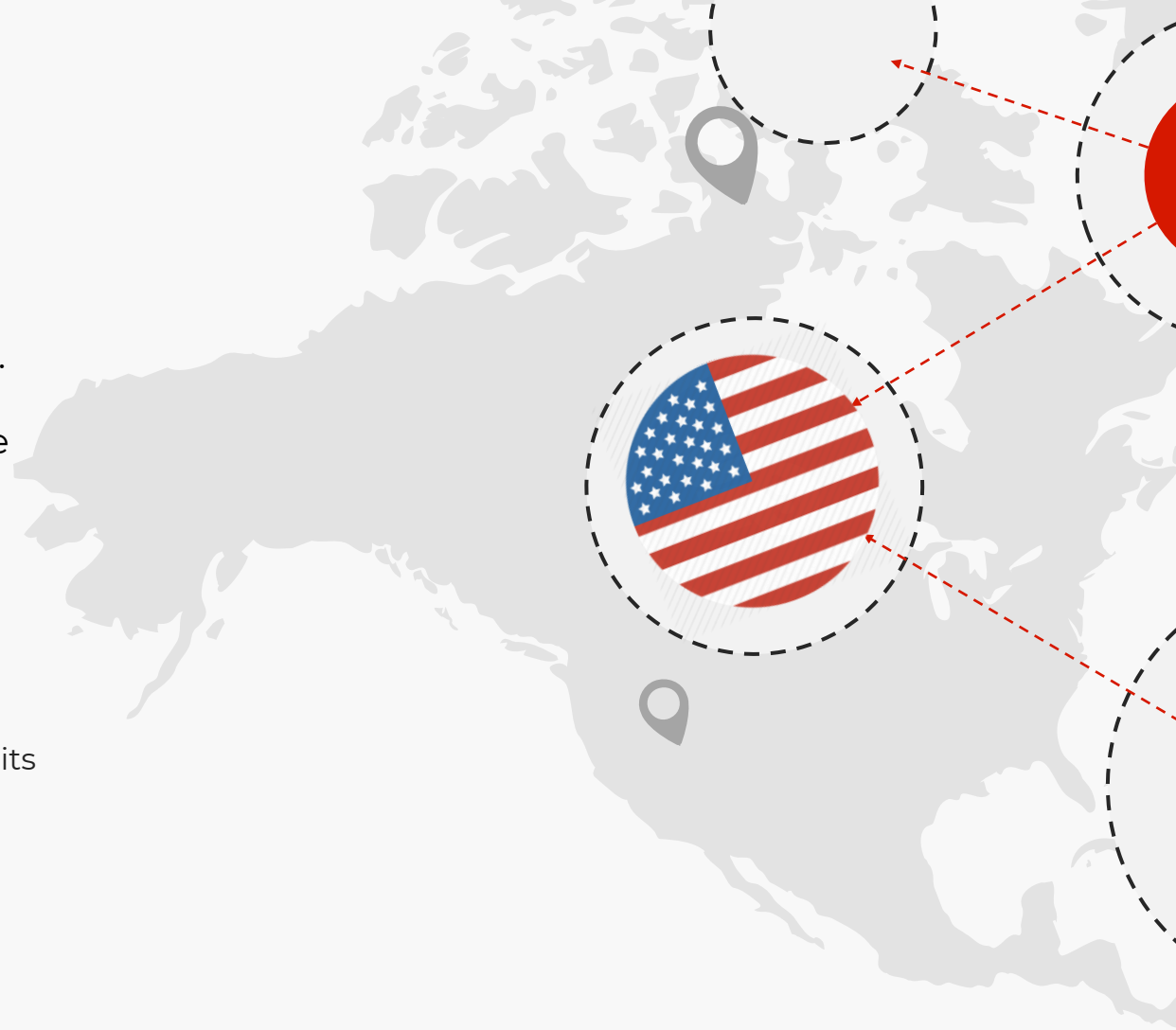
# Privacy in The U.S.

---

There is no comprehensive national privacy law in the United States. Some jurisdictions (such as the EU GDPR) have imposed comprehensive privacy laws. The U.S. has taken the position that the FTC Act's prohibition on unfair, deceptive, and fraudulent business practices protects consumers enough. However, the US does have several sector-specific privacy and data security laws at the federal level, as well as many more privacy laws at the state (and local) level.

The data collected by the vast majority of products people use every day isn't regulated. Since there are no federal privacy laws regulating many companies, they're pretty much free to do what they want with the data, unless a state has its own data privacy law (more on that in the next slides).

- In most states, companies can use, share, or sell any data they collect about you without notifying you that they're doing so.
- No national law standardizes when (or if) a company must notify you if your data is breached or exposed to unauthorized parties.
- If a company shares your data, including sensitive information such as your health or location, with third parties (like data brokers), those third parties can further sell it or share it without notifying you.



# Federal Laws

---

## **Not sector specific:**

- FTC Act
- Children's Online Privacy Protection Act (COPPA)
- CAN-SPAM
- TCPA

## **Sector Specific:**

- Health Insurance Portability and Accountability Act (HIPAA)
- Graham-Leach-Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)

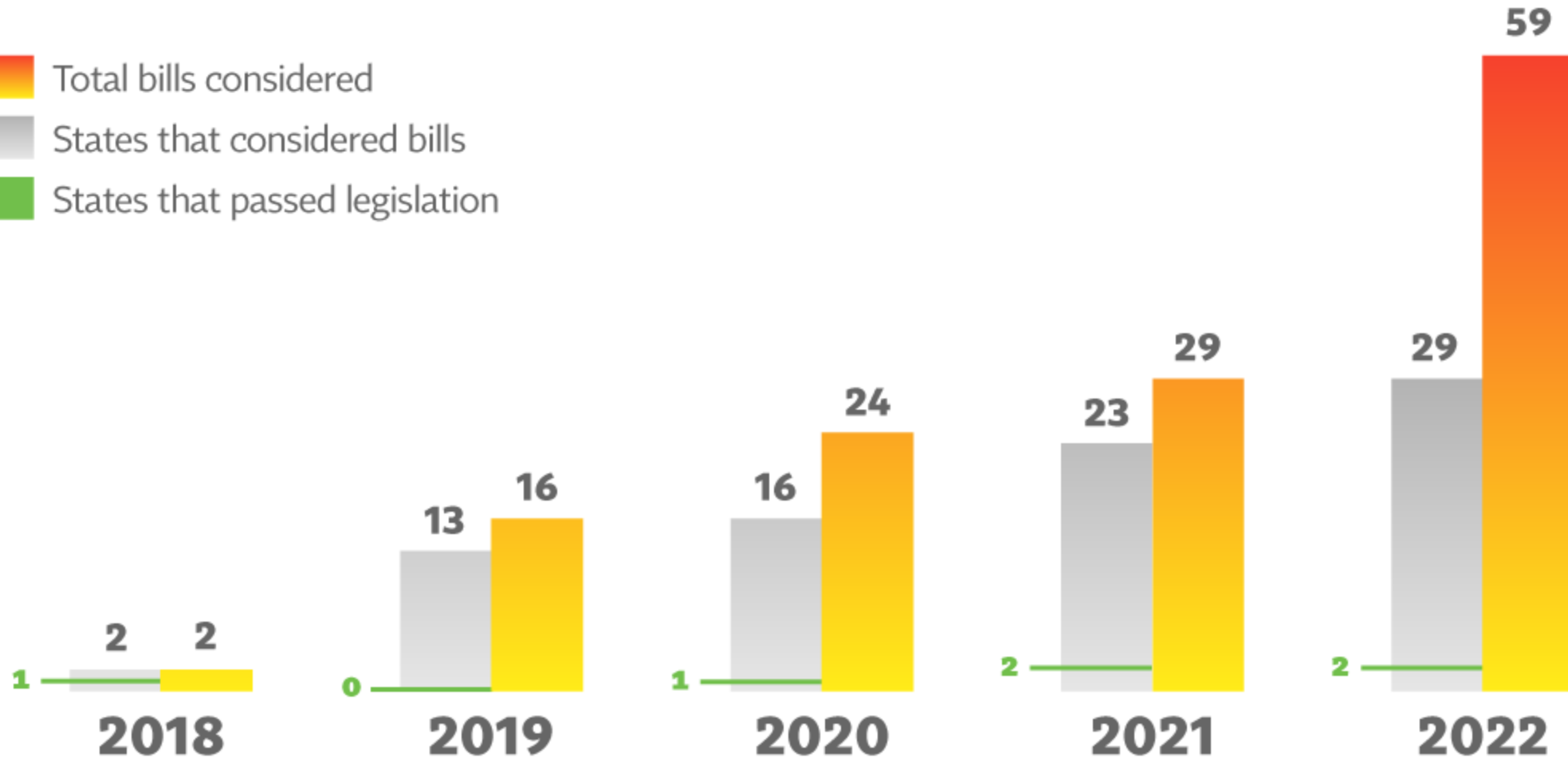
Since these are much more nuanced and often require specialized compliance, we will not be discussing sector specific laws today.



# The Growth of State Privacy Legislation

Comprehensive consumer privacy bills considered from 2018-2022

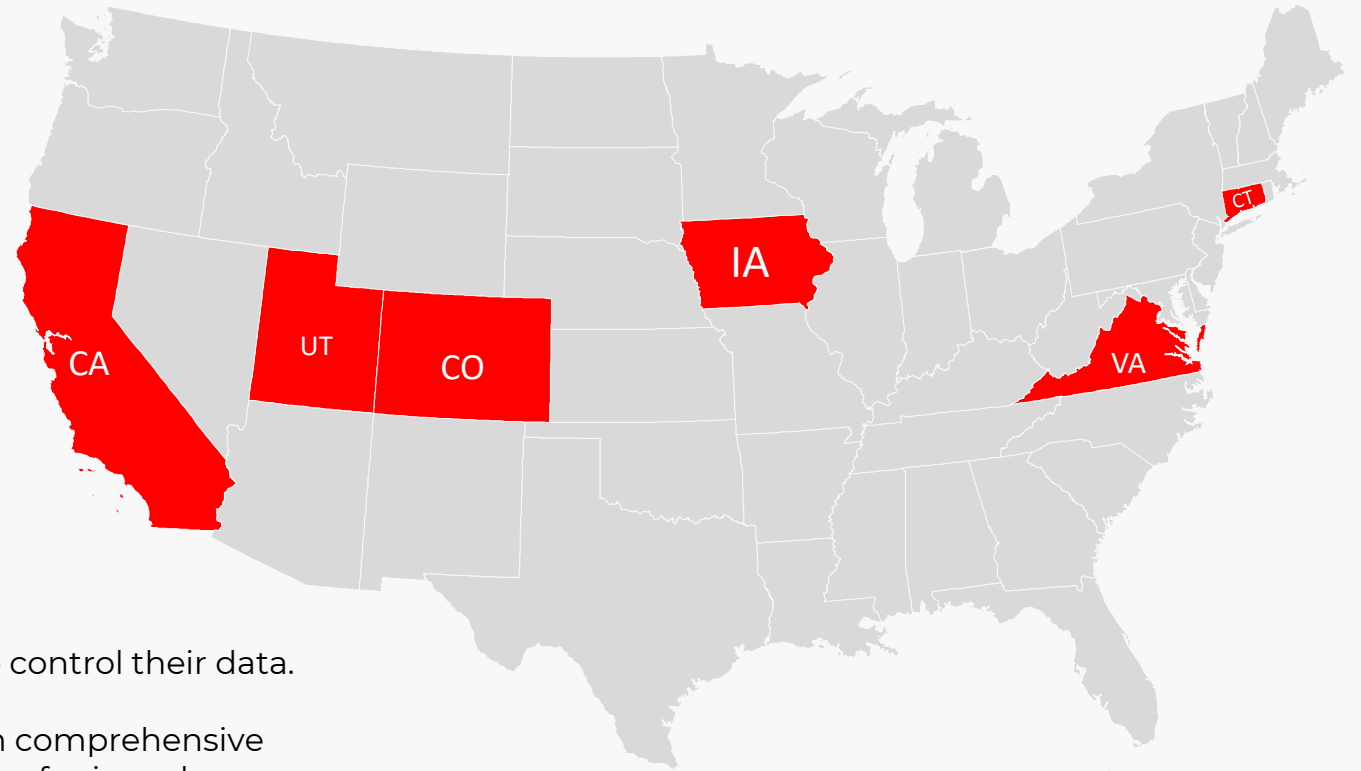
- Total bills considered
- States that considered bills
- States that passed legislation



# States with Comprehensive Privacy Laws

## Types of Concepts Covered:

- Consumer Privacy Rights
- Obligations for Businesses to follow such as minimum-security requirements.
- Required disclosures for businesses to make to consumers.
- Treatment of data belonging to minors.
- Enforcement and penalties associated with each law.



Consumer data privacy laws can give individuals rights to control their data.

**Please note** : While these 6 states are the only states with comprehensive data privacy laws, a number of U.S. states have some form of privacy law focusing on specific business processes such as workplace monitoring, and have their own statutes covering health data.\*

**Also note:** State laws have exceptions, such as not applying to entities subject to HIPAA or GLBA. Many state privacy laws exclude nonprofits.\*



Compliance



Employees



Tech  
Websites  
Cookies



Vendor Contracts

## How These Laws Relate to You as a Small Business or Nonprofit

---

# Privacy Compliance

Much of compliance from a data privacy standpoint for many small businesses and nonprofits will focus on a proactive approach to data privacy problems.

## Some compliance tasks may include:

- Identifying where data is located and how its safeguarded.
- Reviewing and updating your policies related to privacy and IT security measures.
- Reviewing and updating your contracts with third parties.
- Ensuring all data collected is being used for the specific purpose it was collected for and removed in accordance with your retention policies.
- Assessing your data will determine which laws you must comply with. For example, if you are collecting PHI, or If your business or nonprofit is directed towards children.
- Opt-out of marketing communications (opt-out link at the bottom of marketing emails)
- SMS marketing



# Employees

Though employees in the US generally have a limited expectation of privacy in the workplace, various state laws extend specific privacy protections to employees. Your organization should consider the employee privacy laws in each of the jurisdictions in which they operate.



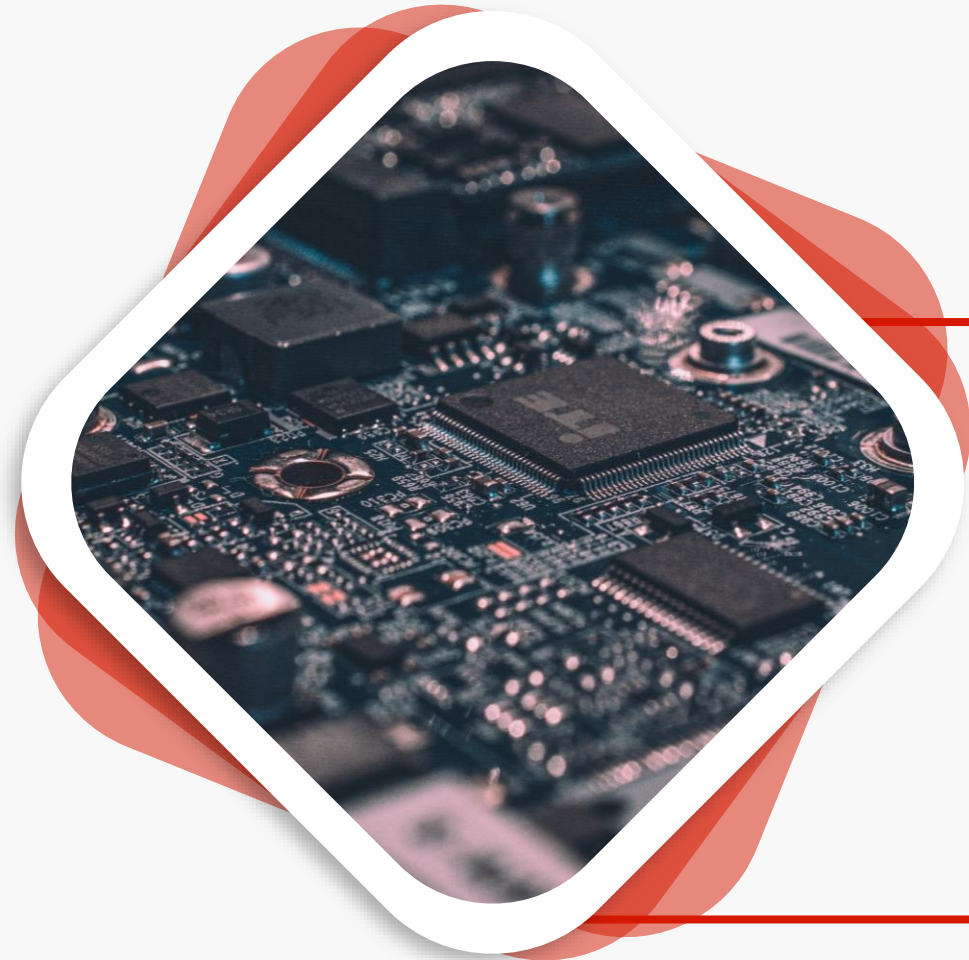
## Employee Privacy

Employee Privacy varies state to state. These privacy laws focus on items such as *Workstation Monitoring and Email Privacy Laws*, *Social Media Privacy Laws*, *Biometric Information Privacy Laws*, and *RFID Privacy Laws*. **Radio frequency identification** (RFID) technology is often used for physical access security, and, in some cases, to monitor employee movement and behavior.

Each state has their own requirements and baseline behaviors that organizations must follow in order to be compliant with their laws on employee privacy.

# Tech/Website/Cookies

When updating your technology policies, applications, and websites, your organization should be extremely specific as to ensure compliance with federal law.



The FTC Act bars “unfair and deceptive” acts and practices in or affecting commerce. This means you need a publicly accessible privacy policy on your website and to adhere to it.

- Unfair?
- Deceptive?

It should be specific to your website and practices and should be updated frequently (about once a year) to ensure it reflects current practices.

The privacy policy should discuss what information is collected, how it is used and who it’s shared with. This includes cookies and data that is automatically collected, such as website analytics.

**Note for developers:** FTC provides guidance for businesses on best practices for developing apps and tech. <https://www.ftc.gov/business-guidance/privacy-security/tech>

# Vendor Contracts

Vendor Contracts are business contracts between two parties covering the exchange of goods or services in return for compensation.

Your business likely has many vendor contracts including vendors who provide food services, internet service providers, and marketing partners.



Many state data privacy laws have references to vendor contract requirements. These requirements must be drafted directly into contracts with third party vendors and usually require items such as requiring vendors to have the same types of privacy and security protections available as the main entity and contractually binding any sub-processors to the same processing obligations that your business has to data.

As a note, this is where confidentiality comes in as well.

Data breaches in small businesses are on the rise. 61% of SMBs experienced at least one cyber attack in the past year, and 40% endured eight or more hours of downtime as a result. In March of 2023, an AT&T Vendor Data Breach Exposed 9 Million Customer Accounts.

These data security obligations cannot be pushed directly to vendors. The diligence you do in selecting a vendor is on your organization.

# Why Else Do We Care?

---



## Legal Risk

- Regulators
- Class Actions



## Valuation Impact

- Reputation
- \$\$\$\$

# Insurance and Security Incidents

---

Insurance coverage may require privacy program compliance

- can use this as a starting place for compliance

In the case of a security incident, there may be several different required actions, depending on the incident

- not every incident is a breach
- for example, federal notice (HIPAA for PHI) and state laws for breach notifications



[D.C. Bar Pro Bono Center Small Business Brief Advice Legal Clinic](#)

Remote consultations available

# Get in Touch!

If you or your business ever needs help understanding any of these concepts, please feel free to reach out at any time!

## Contact



312-715-2738 / 202-780-2648



[Kiana.Baharloo@quarles.com](mailto:Kiana.Baharloo@quarles.com)

[Shaniya.Johnson@quarles.com](mailto:Shaniya.Johnson@quarles.com)

# THANK YOU!