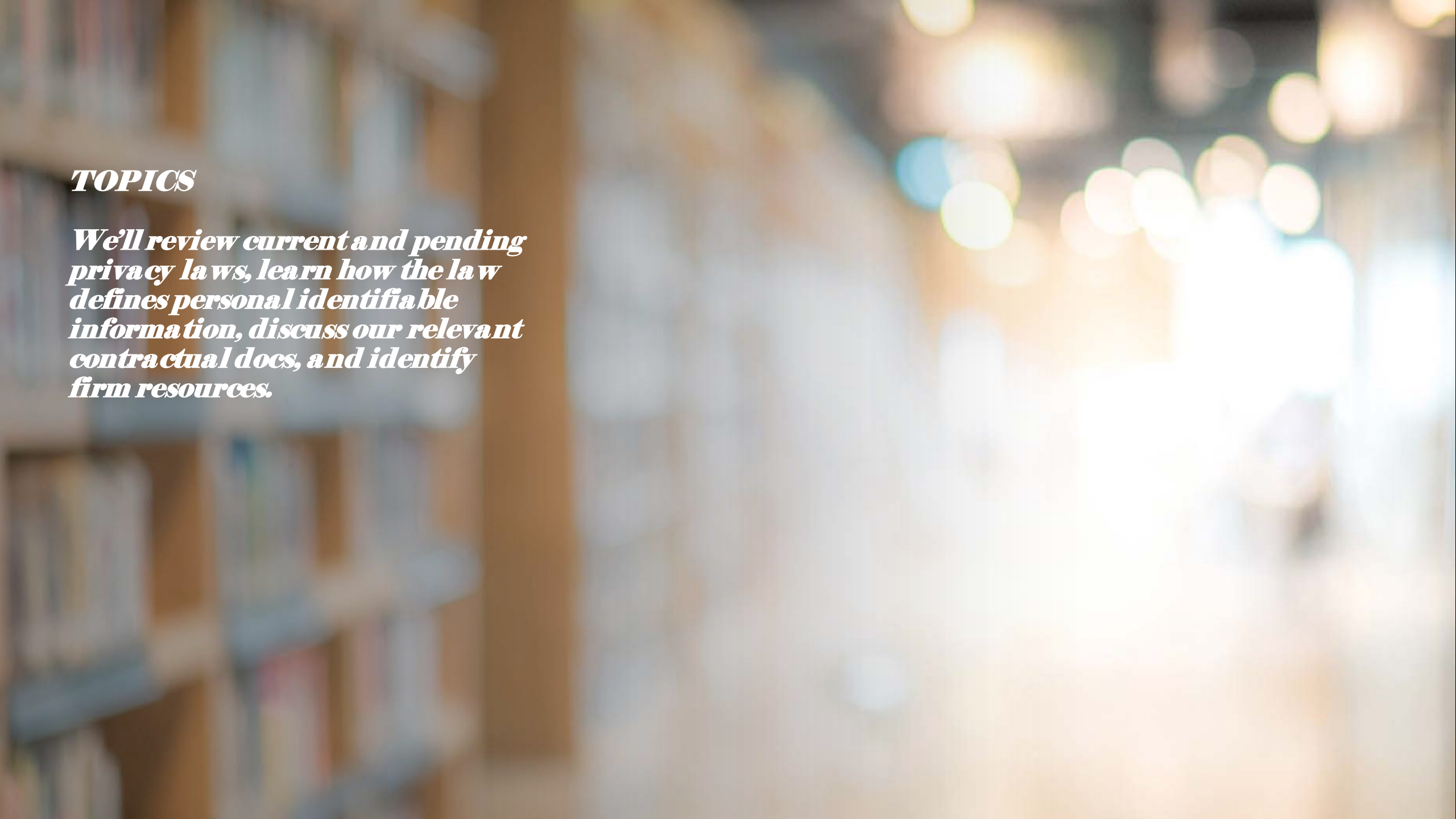


TOPICS

We'll review current and pending privacy laws, learn how the law defines personal identifiable information, discuss our relevant contractual docs, and identify firm resources.

THE WAY THE WORLD WAS...

Until recently, privacy law had been a pretty quiet area of the law.

- **US Privacy Act (1974):** governs information held by government agencies.
- **Health Insurance Portability and Accountability Act (1996)**: protects “personal health information” of individuals.
- **Gramm-Leach-Bliley Act (1999):** requires financial institutions to explain how they share and protect their customers' private information.
- **Children’s Online Privacy Protection Act (2000):** protects the personal information of children.

Then GDPR, the General Data Protection Regulation, was enacted in 2018...

- And suddenly, anyone that collects the personal information of EU residents could be subject to massive new data protection and processing requirements.

Now, various states are getting in on the action...

US States with Privacy Laws

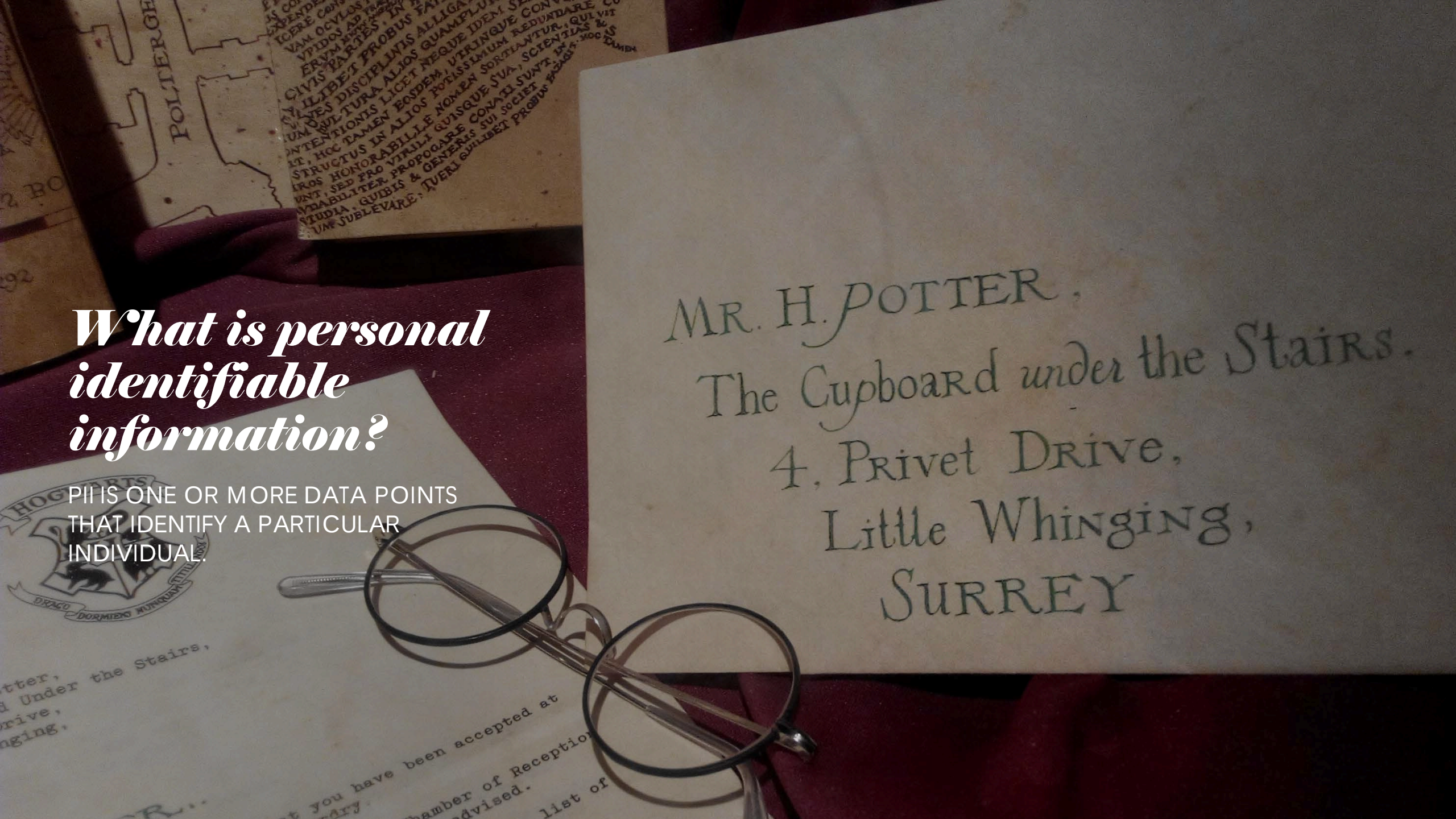
- **California –** The California Consumer Privacy Act (2020)
- **Nevada –** Nevada's Opt-Out Law (2019)
- **Maine –** Act to Protect the Privacy of Online Customer Information (2020)

Pending Privacy Laws

- **Massachusetts –** Massachusetts Data Privacy Law
- **New York –** New York Privacy Act (SHIELD)
- **Hawaii –** Hawaii Consumer Privacy Protection Act
- **Maryland –** Maryland Online Consumer Protection Act
- **North Dakota –** HB 1485
- **Washington –** Washington state data privacy bill (failed this spring, expected to pass in 2021

With so many new laws, how do we get our arms around this area of law?

FIRST, WE NEED TO KNOW WHAT "PII" IS.



What is personal identifiable information?

PII IS ONE OR MORE DATA POINTS THAT IDENTIFY A PARTICULAR INDIVIDUAL.

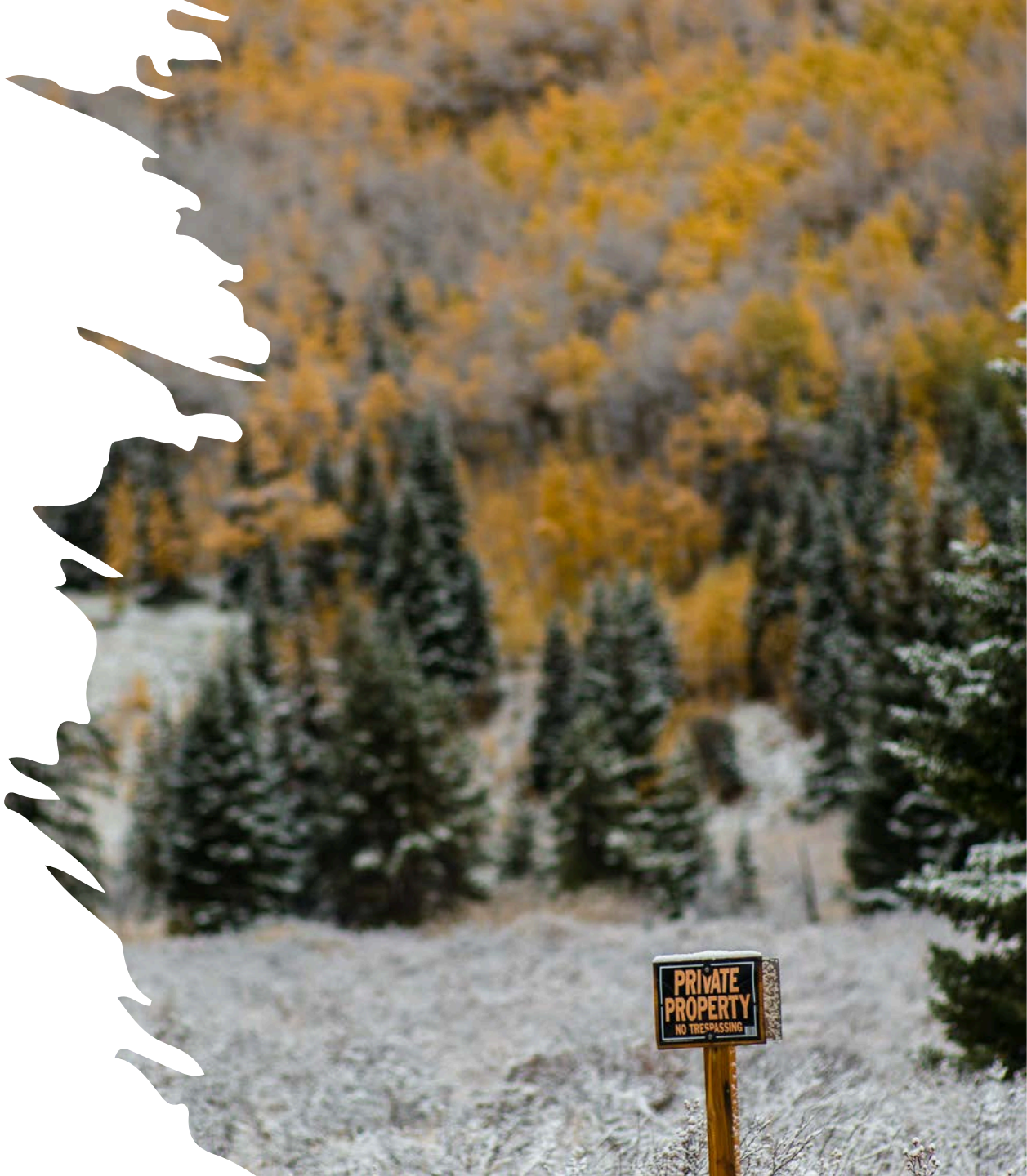
PII can include a wide variety of data points.

* Name
* Alias
* Online identifier (e.g. social media handles)
* IP address
* Unique device IDs
* Account name
* Postal address
* Street address
* Email address
* Telephone number
* Social security number
* Driver's license number or state identification number
* International ID number (e.g. passport number, other international governmental ID number)
* Other unique personal identifier
* Physical characteristics or descriptions of a person
* Geolocation data
* Family and lifestyle details
* Genetic data
* Biometric data
* Racial/ethnic/color data
* Political opinion or affiliation data
* Religious or philosophical beliefs data
* Trade union membership data
* Sex life, sexual orientation, and gender identity data
* National origin
* Citizenship status
* Disability
* Insurance policy numbers
* Educational background
* Current employer
* Employment history
* Bank account numbers
* Credit card numbers
* Debit card numbers
* Other financial information
* Medical/health information
* Health insurance information
* Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
* Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.
* Audio, electronic, visual, thermal, olfactory, or similar information (e.g. voice recordings)
* Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

How do we contract for it?

There are a variety of contracts you can put in place to ensure proper use and protection of PII. The main ones include:

- Privacy Policies
- Personal Information Processing Agreements and Data Processing Agreements
- Confidentiality Agreements and Provisions
- Incident Response Plans



Which contract is used when/where?

You Have to Know What You've Got.

- What data do you collect?
- What are the sources (e.g. contracts, contact forms, provision of services, social media) where you get data?
- After you collect data, where and how is it stored?
- How do you use the data (e.g. is it ever sold to third-parties)?
- Can you readily find and delete the data if necessary?
- What security measures do you have in place?

There is No One Size Fits All Agreement.

- You may need one agreement, or a combination of agreements, depending on your data processing and collection practices.
- Accuracy and knowledge of your internal processes is paramount to building a legal compliance plan!

Privacy Policies

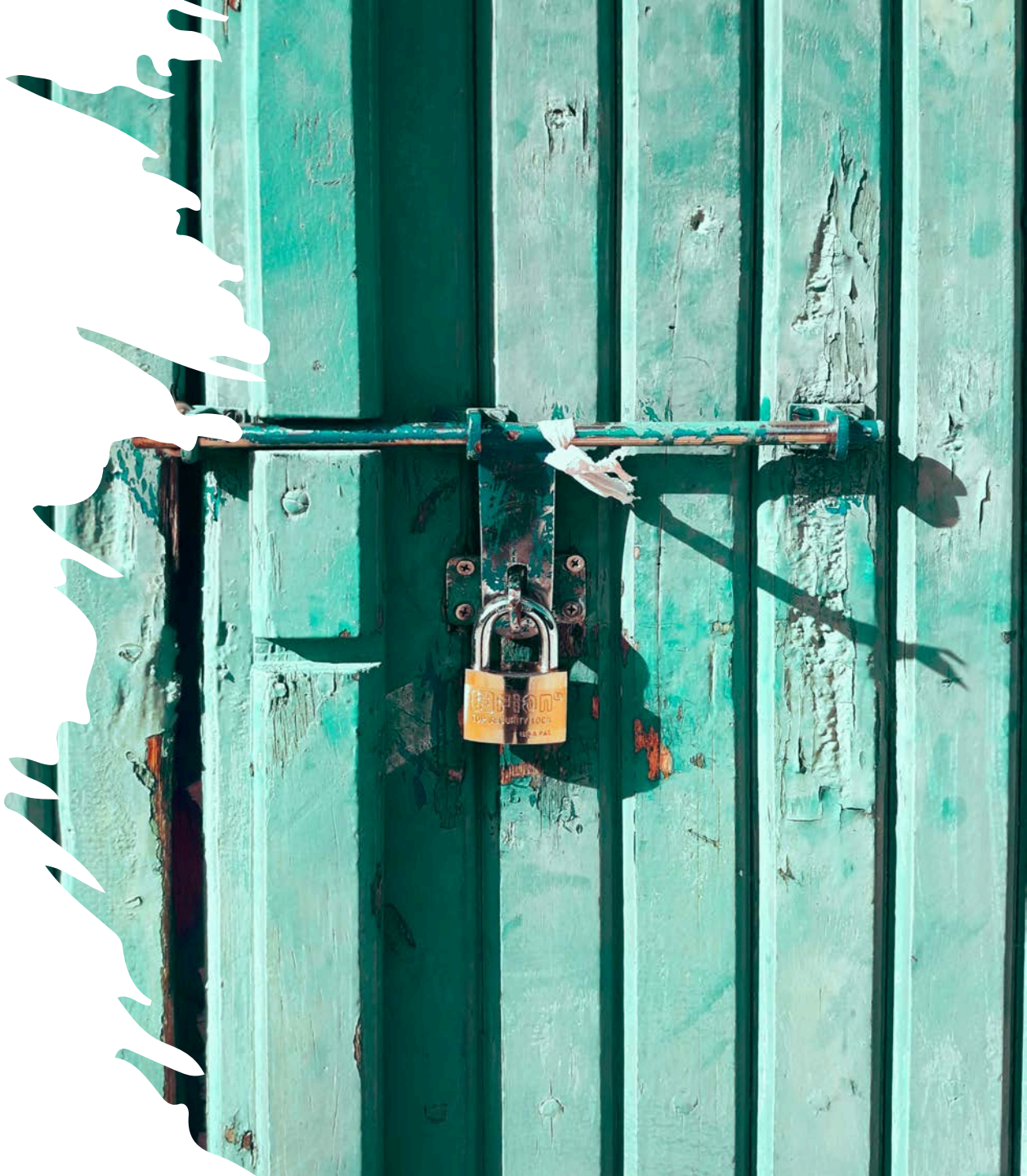
These are generally B2C, but can also be B2B as well. Great for websites and online consumer services where users can provide PII in a variety of ways.

Data Processing Agreements and Personal Information Processing Agreements

- These are useful for B2B transactions where one party is going to be processing the personal information of the other party's customers, contacts, etc.
- Data Processing Agreements (or Addendums) are most often used where European data is processed.
- Personal Information Processing Agreements are generally more US centric, and don't include the required GDPR contractual provisions of their DPA counterparts.

Confidentiality Provisions and Agreements

CAN COVER A WIDE VARIETY OF CONFIDENTIAL INFORMATION, INCLUDING CUSTOMER PII, ETC. THESE ARE GOOD TO USE WHEN THE AMOUNT OF PII IS MINIMAL.



Incident Response Plans

- An IRP is an internal company document that governs how the company responds in case of a data breach.
- It also includes best practices for data governance and protection.
- You can also use an IRP in tandem with an internal PII processing policy.

What's the goal here?

TO MAKE SURE YOUR AGREEMENTS ARE

ACCURATE AND **UP TO DATE.**

What resources are available?

- Fortunately, Carney Badley Spellman has many example agreements, checklists, and practice notes on privacy law.
- We can also introduce you to third-party service providers who can provide cyber security securities.

Finally, are you covered?

Cyber security coverage is quickly becoming a requirement in service provider agreements. If you haven't already, you should speak with your insurance broker to discuss whether this coverage is right for your business.


You can also ask our Privacy Team for help!
YOU CAN REACH OUR GROUP VIA EMAIL AT PRIVACYGROUP@CARNEYLAW.COM