

A.D.

Privacy Law & Donor Data

What's new in privacy law and AI regulation and what it means for your donors, their data and your fundraising operations

Amy Daultrey 15th March 2024

Copyright © 2024 Amy Daultrey. The author is not responsible for the content and security of external links referenced in this presentation. You may share these slides with colleagues. Editing, distribution without permission, commercial copying and lending are prohibited. The Raiser's Edge 7 and NXT are trademarks of Blackbaud, Inc.



About me

- Independent consultant on RE7, NXT, other CRMs and CMS'
- In fundraising sector since 2002, consultant since 2008.
- I work with clients in US and UK.
- I'm interested in how privacy law is evolving and contrasts in how it affects fundraising ops of US and UK clients.

Disclaimer: this webinar does not constitute legal advice and I'm not a data privacy expert or a lawyer. Please seek legal guidance specific to your organization on the topics discussed.

What we'll cover today

- Current state and federal situation
- Common features of privacy laws
- What you can do
- AI regulation
- Resources and links
- Q&A

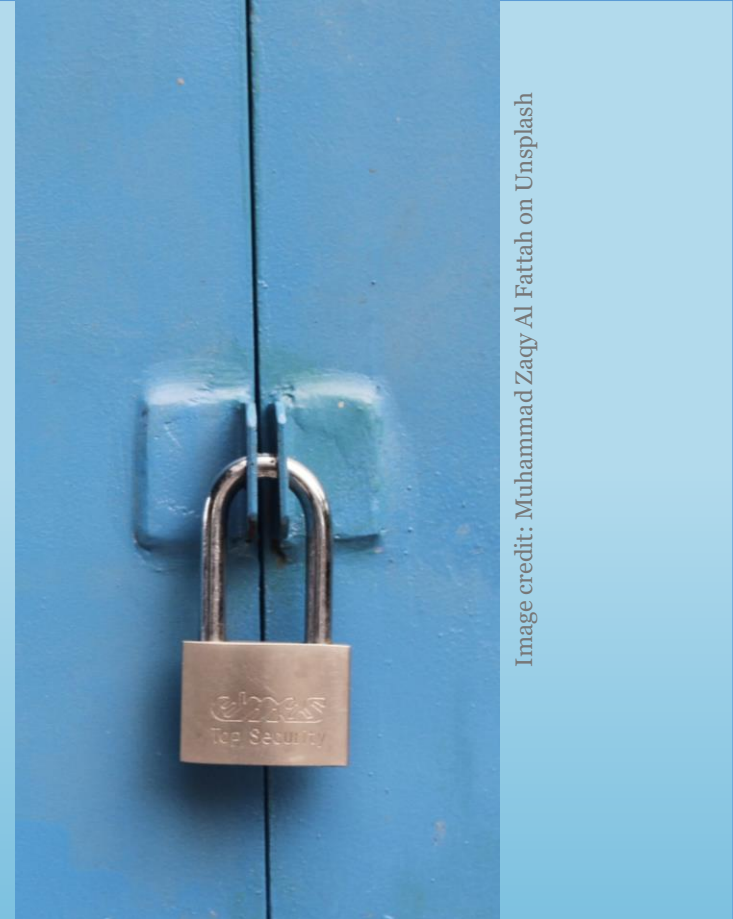


Image credit: Muhammad Zaay Al Fattah on Unsplash

Current situation



The upward trend: state law

Year passed	State and date effective from
2024	New Hampshire (1/1/25), New Jersey (1/15/25). On the horizon: Georgia, Kentucky, West Virginia, Wisconsin...
2023	Delaware (1/1/25), Indiana (1/1/26), Iowa (1/1/25), Montana (10/1/24), Oregon (7/1/24), Tennessee (7/1/25), Texas (7/1/24)
2022	Connecticut (7/1/23), Utah (12/31/23)
2021	Colorado (7/1/23), Virginia (1/1/23)
2020	California Privacy Rights Act (1/1/23) amendment to the CCPA (1/1/20)

***Bold** = nonprofits not exempt*

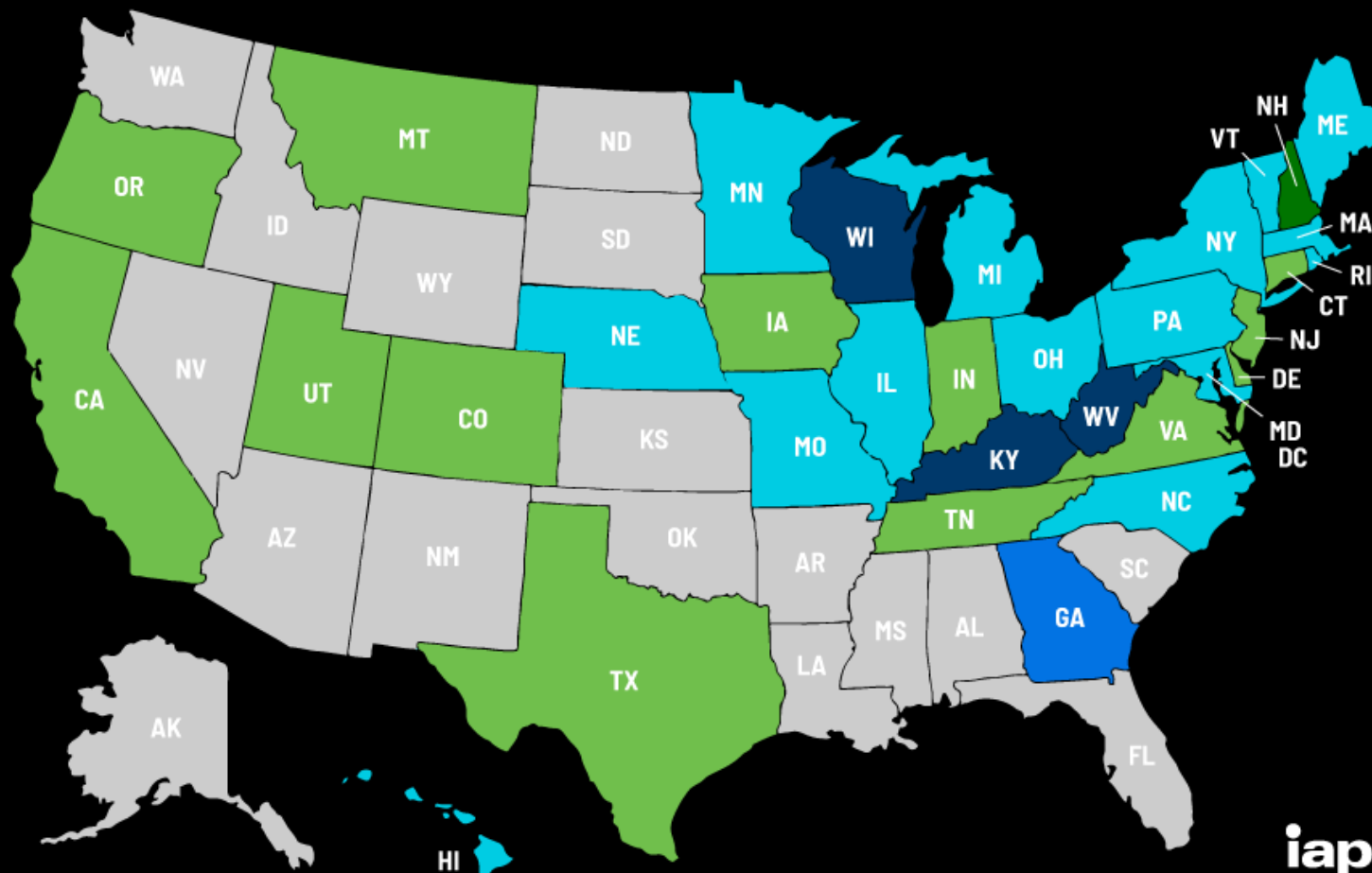
The newest laws

- **Colorado Privacy Act** (effective July 1, 2023) was the first that didn't explicitly exclude nonprofits; compliance required if processing info of 100k residents/year or 25k/year and selling lists.
- **Oregon** (July 1, 2024) became the second, **New Jersey** (Jan 15, 2025) is the third. Similar compliance rules.
- Don't expect all states to follow same structure. New Hampshire has a low compliance threshold (35k). Texas threshold is by small business definition (number of employees).

US State Privacy Legislation Tracker 2024

Statute/bill in legislative process

- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced



Last updated 1 March 2024

iapp

Federal...the guessing game

- 55 privacy-related bills in current congress, of which 3 are comprehensive consumer rights laws
- Federal might follow trend of states exempting nonprofits...
- Or a carbon copy of Virginia, Colorado etc.
- Or it could be more comprehensive.
- Will probably include some sort of AI regulation.
- Expect consumer awareness to grow.

Common features of privacy laws



Some definitions

- **Personal data** = any information that can be connected to a person.
 - Names, addresses, emails, phones, social media handles, geographic locators, friends and connections, employer and job title...
 - **Processing** = any kind of handling of personal data (acquiring, storing, using it)
- Combine the two = what we do on a daily basis!
- **Controllers** = orgs that acquire and use data (nonprofits)
 - **Processors** = third parties that process it (database providers)
 - **Consumer data = donor data. Donors won't see any difference.**

Commonalities: consumer rights

- Right to access/view, correct and delete (including data from third parties); ~up to once per year
- Right to opt out of targeted advertising, selling data & profiling
- Right to opt out of data being processed
- Right against automated decision making
- Right to obtain list of third parties data shared with

Commonalities: business obligations

- Privacy notices that are clear, complete and easy to find
- Limit data collection to what is **adequate, relevant and necessary** to serve purposes contained in privacy notice
- Take all steps to secure personal data
- Don't collect sensitive data without consent
- Provide a means for consumers to opt out
- Be ready to recognize UOOMs (New Jersey 7/15/25, Oregon 1/1/26)
- Conduct risk assessments of projects, procedures, new tech

Sidebar: lessons learned

- Nonprofits are typically overlooked in guidance, or that guidance comes too late to be useful. The focus is on corporate behavior. Nonprofits get lost in the mix.
- Look to well-resourced large orgs and representative bodies to navigate the legalities, but...
- ...don't wait for them. Never too soon to figure out best practices for yourself, aim for high standards and future-proof your operations.
- Don't rely on your tech providers for all the answers or for product improvements to help you comply. Their priority will be *their* liability, compliance needs. Assume you'll be working with the tools you have now.

What you can do: 6 tips



1. Inventory of data

- Compile a data cookbook. Know what you have and why you have it.
- Flag the personal and sensitive fields. Use Colorado and New Jersey for definitions. What would be exposed in event of a data breach?
- Not just your donor database. Giving platforms, email platforms, event apps, social media accounts, spreadsheets, physical paperwork...
- Record volume gotchas: if you've moved gifts of lapsed donors to an anonymous record and each of those gifts contains a name/personal info, that counts as one person.

2. Audit preferences and consent

- How are you gathering preferences and consent, if at all?
- Where are the places you *could* be doing this? Email signups, giving forms, new donor emails, event registrations, membership forms, alumni welcome packs, volunteer forms...
- Examine and test end-user experience (all forms, privacy policy, contact mechanisms): what do constituents see, what might they assume or expect, where are the gaps and errors? Don't forget to test on a mobile too!
- Store where you got consent/opt-ins from and when.
- Determine how best to store preferences so you can use them effectively when segmenting mailings and email campaigns.

3. Spread the word

- Form a task force to examine current processes and identify weak spots.
- Educate staff, board.
- Explain the benefits of getting out in front of privacy law early: reduced impact on time and resources later, reduced risk of contravening new laws (\$\$\$ fines).
- Encourage them to take ownership in everyday work, spotting problems and opportunities.
- Make it a repeat topic in regular meetings.

4. Embrace data minimization

- Reduce surplus information, reduce risk. Less to lose in a breach, less likely to store something you shouldn't be keeping.
- Make a conscious switch. Think about what the donor would think about you storing this information. What would they expect, now and in future?
- Find a mantra and train staff to follow it.
 - If in doubt, leave it out!
 - If you don't *need* it, don't *keep* it!
 - Won't use it? Lose it!
- Use the traffic light system (see Resources slide).
- Bonus: leaner, cleaner databases can be cheaper too.

5. Incorporate it into marketing

- Incorporate preferences into a “welcome series” for new constituents.
- Reiterate/explain where you got their signup from (a gentle reminder), when and how they can expect to hear from you, and how they can alter their preferences if they wish to.
- Set expectations and draw attention to your org’s careful handling of preferences and personal data.
- The message: **We take this seriously. We can be trusted.**

6. Look for opportunities

- This is the time to tackle the cleanup and purging you've been putting off.
- It's a chance to overhaul your processes and bring some focus to training and education if those are on the to-do list.
- Need to convince management that you need resources to do this now? Tell them Amy says it'll cost more if you leave it until the last minute 😊

Artificial Intelligence



AI regulation

- Executive Order on Safe, Secure and Trustworthy AI (October 30, 2023).
- Renewed call for federal comprehensive privacy legislation.
- Generative AI content will probably need to be labelled as such (ie. email content, marketing copy, images).
- Make sure third parties that do screenings for you disclose whether they are using AI on your data. Assess security and privacy risks of these services. Include this in your privacy policy.

AI regulation

- **Don't unleash AI on your entire dataset.** High risk you'll run into future legislation that means you'll have to discard this work.
- Use best quality, least risk data. Exclude bought records, poor quality/never cleaned, deceased, 10+ years old. Check for errors, gaps, inaccuracies, unusual outliers.
- Determine how you'll respond to donor questions about how you use AI.
- Make sure your privacy policy is up to date. Do this *before* working with AI!
- joangarry.com/podcast/ep-196-how-risky-is-ai-for-nonprofits-with-beth-kanter/

Resources



Resources & links

- Colorado as a model: goldendatalaw.com/blog/5-tips-for-nonprofits-on-colorados-new-privacy-law
- Track state legislation iapp.org/resources/article/us-state-privacy-legislation-tracker and federal iapp.org/resources/article/us-federal-privacy-legislation-tracker
- Freebies at amydaultrey.com/resources: Traffic Light data entry system, anticipating AI regulation, Kennesaw case study, data minimization, links to useful websites and much more.

Thank you! Any questions?

- amy@amydaultrey.com
- amydaultrey.com/resources
- linkedin.com/in/amydaultrey
- Hope to see you at AASP Summit in November

