A.D.

Privacy Law & Donor Data

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

Amy Daultrey 11th October 2024

About me

- Independent consultant on RE7, NXT, BBNC and other systems with clients in US and UK.
- In fundraising sector since 2002, consultant since 2008 (including 5 years in California).
- I'm also a gemmologist!

Disclaimer: this webinar does not constitute legal advice and I'm not a lawyer. Any comments made in Q&A are my own opinion and not legal expertise. Please seek legal guidance specific to your organization.

A.D.

Why I'm interested in this

- I believe the GDPR experience will be repeated with US privacy law:
  - Guidance for our sector will be late, if at all.
  - Focus is on corporates; nonprofits get lost in the mix.
  - Tech providers will focus on *their* liability and compliance, not yours. They might roll out new features to help–but don't rely on these being timely or functional.
  - Some organizations will be unnecessarily cautious.
  - Scammers will try to monetize the uncertainty.
  - Small orgs with no legal resources will struggle.
  - Late action will cost time and money.
- Early prep is everything. New laws take a while to bed in. Now is the sweet spot for figuring out what you need to do.

A.D.

Who I'm currently following

- Cobun Zweifel-Keegan, JD **linkedin.com/in/cobun**
  - See Cobun's post from October 1st about the privacy "golden rules" from regulators–including "put yourself in the consumer's shoes. Treat them the way you want to be treated" and "privacy work…requires hard work across teams".
- Jay Averitt **linkedin.com/in/jay-averitt**
- Maverick James, Esq. **linkedin.com/in/maverickjames**
- The Nonprofit Alliance **tnpa.org/get-involved/policy-in-the-states/**

A.D.

Privacy law compliance is a positive thing ☺

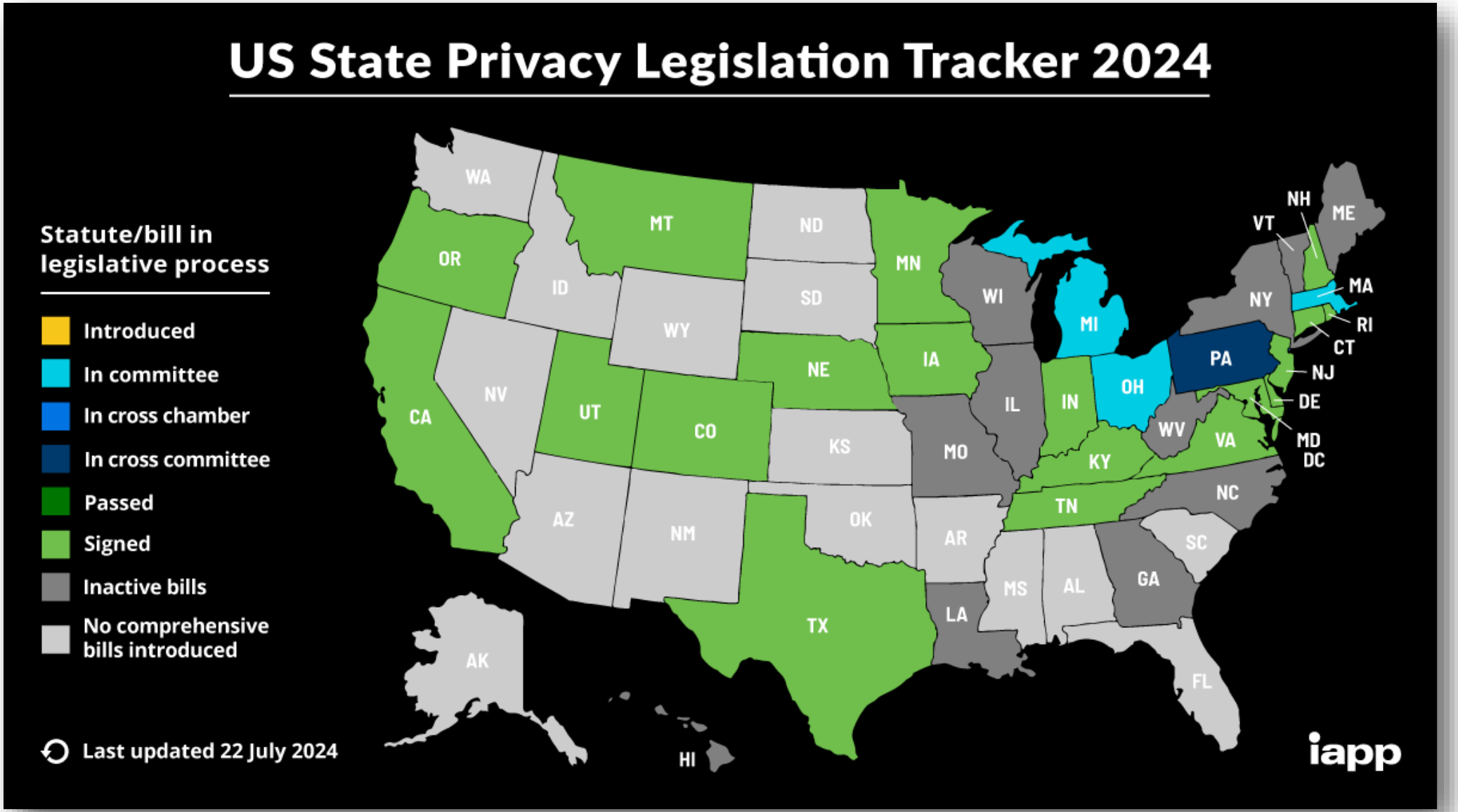
- A framework to get things done (not a one-off compliance checkbox exercise).
- A chance to dedicate resources to cleaning, reducing and refreshing data.
- A chance to obtain long reaching consent.
- Increased engagement.
- Better metrics on preferences, interests.
- A chance to demonstrate to your donors that they can trust you with their information.
- Excellent prep for anything you want to do with AI.

A.D.

“Privacy”?

- IAPP: “Information privacy is the right to have some control over how your personal information is collected and used”
- As custodians of donor data we should always take a **privacy first** approach to how we acquire and use that data.
- It's not about cyber security and breaches but it crosses over with these.
- Inevitable that your organization will be affected by privacy law (if it hasn’t already).

A.D.



https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

A.D.

The upward trend in state law (19 & counting)

Year passed	State and date effective from
2024	Kentucky (1/1/26), **Maryland** (10/1/25), **Minnesota** (7/31/25), Nebraska (1/1/25), New Hampshire (1/1/25), **New Jersey** (1/15/25), Rhode Island (1/1/26)
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) and amendment to the CCPA (1/1/20)

Bold = *nonprofits not exempt*

A.D.

Key takeaways

- Texas is doing a lot of enforcement of B2B compliance. NP exempt there but they are setting a trend.
- Maryland was the first to call out Data Minimization and restrict sharing of sensitive information.
- Variations in each law. Don’t expect new laws to be the same.
- Fine structure is huge (ie. $7,500-$20,000 *per violation*). I have yet to find a definitive guide to what this means. Assume it’s bad.
- Short lead-in times to compliance (typically a year). Clock is already ticking on Delaware, Maryland, Minnesota, NJ.

A.D.

The threshold thing

- ie. “Applies to orgs and businesses processing the information of 100,000 residents per year or processing 25,000 per year and deriving a profit from selling that information.”
- Some states have lower thresholds: New Hampshire 35,000. I *think* it’s related to population size, typical business size etc.
- Some do something completely different: Texas uses small business definition.
- Don’t assume your org is exempt because you have a small database. It’s not just your CRM. Do an inventory of all personal data everywhere you have it.
- **Safest approach: work towards compliance regardless of the threshold.**

A.D.

“Secondary uses”

- If you use data for a purpose other than that which was disclosed at the time you collected it, you will need consent.
- Colorado (rule 6.08)
- Washington (My Health My Data section 4)
- Potential example*: a donor makes an online gift. On the form it says their information will be used for communications. Their info is shared with a wealth screening service. This might be a secondary use infringement because the giving form didn’t say their information could be used for analysis and profile building.
- **This is untested law. I’ll have better examples in future ☺*

A.D.

Commonalities: consumer rights

- Right to access/view, correct and delete (including data from third parties), up to once per year.
  →Be ready for DSARs (data subject access requests). “Best way to comply with DSARs is to minimize the data you collect from the start” (Jay Averitt, LinkedIn September 7th).
- Right to opt out of targeted advertising, selling data & profiling.
- Right to opt out of data being processed (ie. delete me).
  →You’ll need a robust process for handling delete requests.
- Right against automated decision making.
- Right to obtain list of third parties data shared with (ie. wealth screening, address finding, mail houses).

A.D.

Commonalities: business obligations

- Privacy notices that are clear, complete and easy to find.
- Data Minimization: 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.
- Recognize browser Universal Opt Out Mechanisms (Colorado, NJ, Oregon).
- Conduct risk assessments of new projects, procedures, tech, third parties.

A.D.

Federal…the guessing game

- 61 privacy-related bills in current congress, of which 3 are comprehensive consumer rights laws.
- American Privacy Rights Act – being watered down but calls out Data Minimization and would preempt state law. Higher threshold (200k).
- My hunch*: APRA won't pass. Successor passes in 2 to 4 years if it continues to be bipartisan-lead. State laws will continue to fill the void.
- Expect federal to include some sort of AI regulation.
- Expect consumer awareness to grow.

**I'm not a legal expert. This is purely my opinion. Don't come after me if I'm wrong ☺*

A.D.

AI regulation snapshot

- **Executive Order on Safe, Secure and Trustworthy AI** (October 30, 2023).
- **California, Colorado and Utah** have enacted AI bills. CO most comprehensive.
- AI content to be labelled as such (includes email marketing, images).
- Disclosure from third parties on whether they use AI on your data (ie. wealth screening, analytics).
- Your Privacy Policy/Notice includes how you and third parties use AI.
- Right of consumers to opt out of AI being used on their data.
- Risk assessments of using AI.

A.D.

AI regulation thoughts

- Make sure your Privacy Policy is up to date before you go anywhere near AI.
- 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. Build the foundations well and your AI house will stand.
- Determine how you’ll respond to donor questions about how you use AI.
- Listen to this: joangarry.com/podcast/ep-196-how-risky-is-ai-for-nonprofits-with-beth-kanter/

A.D.

To do: Update your privacy policy/notice

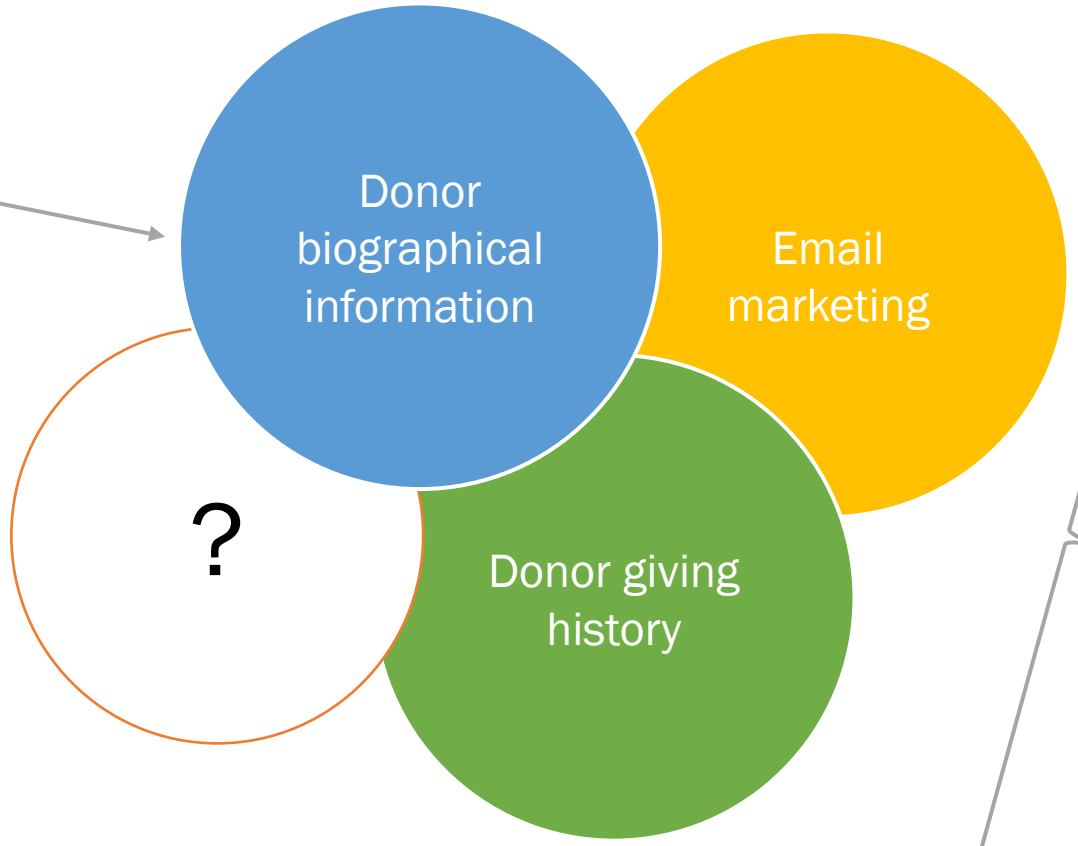
- Look to how large orgs word their privacy notices. **American Red Cross** and **The Nature Conservancy** are good examples. *(I'm not advocating you copy these notices verbatim, use them as a starting point).*
- Identify the gaps in your privacy notice. What activities are you doing with constituent data that are not mentioned? Does your privacy notice explain how someone can view their info, opt-out or have their info deleted?
- If you want the gold standard, try the UK's privacy notice generator: **ico.org.uk/for-organisations/advice-for-small-organisations/create-your-own-privacy-notice/**

A.D.

To do: Data Minimization

Check who is entering what and why. Aim for accuracy and only info covered by your privacy policy, not volume.

Improve accuracy, keep the info you are certain about. Retained info must align with what your privacy policy says you collect.



Stuff you're not certain of where it came from, if you need it or if it's accurate. Target this for correction/deletion.

Make sure you know all the places personal info is being stored.

A.D.

To do: Start asking preferences and opt-ins

- Where could you ask constituents their preferences for communications? Can you add it to your email signup form?
- Test, test, test! Don't forget your mobile site!
- Don't be afraid to be granular. Two checkboxes ☑ **mail me** and ☑ **email me** are infinitely more useful (and future-proof) than one vague checkbox ☑ **contact me**.
- Store where you are getting opt-ins and opt-outs from, and when.
- Use these preferences in marketing campaigns and stewardship.

A.D.

To do: Clean your data

- Do an inventory of your data.
- Flag sensitive information and determine if you really need it (ie. DOB).
- Form a task force to examine current processes and identify weak spots in data entry and handling.
- Prioritise cleaning tasks: sensitive info first, then surplus info that doesn't align with your privacy policy. Plus duplicates, errors and typos.
- Don't wait for a state law deadline to find resources for this work. Start now and chip away at it.

A.D.

Resources

- 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 handout, links to useful websites and much more.

A.D.

Thank you! Any questions?

amy@amydaultrey.com

amydaultrey.com/resources

linkedin.com/in/amydaultrey

Image credit: Andrew Ridley on Unsplash