State Privacy Enforcement Do's and Don'ts for 2024

Kelley Drye

Before you're a target, consider the following:

- ***Know your audience.*** Monitor concerns from the states. Keep a pulse on the nation's zeitgeist and topics that quickly rise to the top. Establish yourself as a friend of the states and a good corporate citizen.
- ***Understand how priorities are set, and how states collaborate.*** Look for opportunities to hear from and proactively engage with the enforcement community. Recognize the AGs are still in learning mode on new privacy and technology developments, which means you will have the opportunity to show how your program meets or exceeds the obligations under the law.
- ***Know the state of your program.*** Have an understanding of what your current privacy program is comprised of to date – both what is documented and what is in practice – and devote some time to critically assessing how you could demonstrate it is in place. Think about how you would tell your compliance story to an enforcer if they come knocking.
- ***Don't lose the forest from the trees.*** While the new privacy laws have a lot of requirements that get fairly granular, start with a big picture. Document the pillars of your program and people who support it. Know your areas of strength and acknowledge you will never be "done," but that your work will be in constant progress. Have a north star you are working towards.
- ***Peer Pressure.*** Participation in working groups can help with benchmarking and aware of solutions and approaches to addressing compliance challenges and legal developments (e.g., FpF, IAB, NAI, local bar associations, in-house counsel working groups). Peer pressure applies to states too – stay on top of issues that may pressure state regulators as a result of their sister states' actions.
- ***Minimize surprises.*** Have a clear, established plan on what to do if a letter comes in, and who will assist and need to be involved. Understand the process and familiarize yourself with the rules.
- ***Monitor your complaints.*** Complaints about your business for any reason may invite scrutiny from enforcers in ALL areas that you operate. Track, respond, and resolve complaints as they come in. Privacy / data use are newer areas. Check in with your customer care team to see if and how these issues may be monitored to identify trends.

You have received a letter/email/subpoena – now what?

- **What To Do**
    - Place a litigation hold asap.
    - Assess if you have soft spots and if you do, plan and implement updates as soon as you can. Think of these as enhancements, rather than admissions. Every business is working to continually refine and build processes. That's not a bad thing.
    - Create a practical and substantive checklist of things to do to respond and note the timing of your outreach and response.
    - Know the difference between AG interpretations you do not like but need to accept vs. positions on which you should reasonably give push back.
    - Prepare for more – other states may already be engaged or be monitoring the actions of their sister state(s); find out if/who/how they intend to share your information.
- **What *Not* To Do**
    - Be litigious right out of the gate.
    - Assume/act as if you know more about the state's law than the enforcer does.
    - Disrespect the chain of command.
    - Will your tactics make things worse? (Consider this critically).

Keep top of mind the priority areas for privacy enforcement.

- Opt outs
- Consent practices
- Notices, privacy disclosures, and UX – no dark patterns
- Operationalizing rights requests (e.g., is deletion really occurring on the backend?)
- Kids/teens
- Sensitive Personal Information (think broadly here)
- Prepare for the unexpected. Regulators continue to announce new priorities and are also monitoring business trends to identify areas of focus.

Alysa Hutnik
Partner & Chair, Privacy & Information Security Practice
ahutnik@kelleydrye.com

Paul Singer
Partner & Chair, State Attorneys General Practice
psinger@kelleydrye.com