Gunderson Dettmer - How to Get...ctical Tips with Anna Westfelt

Thu, Jul 11, 2024 4:06PM 22:19

SUMMARY KEYWORDS

regulators, privacy, data, website, privacy policy, consumer, consent, tools, requests, compliance, enforcement, third party, organization, settlement, collect, vendor, point, plaintiff, claims, pay

---

00:07

Hi, my name is Anna Westfelt, and I'm the Head of Gunderson Dettmer's data privacy practice. Today I'm going to give you a short and practical presentation on how to avoid becoming a privacy enforcement target, mostly focused on your public facing website today. And my presentation is based on what I've seen in my practice, and also what the regulators have told us that they are prioritizing.

00:34

To kick things off, let's take a look at where we are now in the US privacy landscape. And it is very different from the six years ago when the EU GDPR came into effect. At that time, we didn't even have a single US state comprehensive privacy law. At this time in July 2024, we have 19 comprehensive US state privacy laws that have been passed and many more on the way. We have seen three publicized settlements in California under the California Consumer Privacy Act by the California Attorney General, one against Sephora for $1.2 million, one against DoorDash for $375,000, and one recent settlement against the video game developer Tilting Point Media for $500,000. We know that there are many more investigations ongoing and California now also has a dedicated agency working on enforcement.

01:29

We also have a very aggressive privacy regulator in the Federal Trade Commission. And we are seeing a lot of enforcement activity not only from the FTC, but also in the state attorney general level. Not only that, we're seeing an incredible surge in privacy class actions, and particularly those relating to a very common website tracking tools, such as the megapixel and session replay technology. Of course, the question is, are we going to get a federal privacy law to unify this complex patchwork of state laws. And there are efforts on the way there is a bill in Congress, but it has hit numerous roadblocks, and it is very unlikely that we will see a federal privacy law passed before the next election.

02:19

02:19

With that in mind, I want to share some practical tips that are based on what regulators tell us are their enforcement priorities. And my hope is that you can take these back to your organization and get the right business stakeholders to the table, whether that be engineering, web development, marketing, or legal, and that you can help reduce the risk of your organization becoming an enforcement target.

02:41

Tip number one, and this is a really important one, know what is on your website. This is really the low hanging fruit for enforcement. It's very easy for regulators and consumers to visit your public facing website and look for non compliance, it is right there. This was in fact the focus of both the Sephora and the DoorDash investigations and settlements. And there are plenty of tools for regulators and for plaintiff's counsel to scan your website for non compliance. So first of all, I really urge everyone to perform a thorough audit of personal data collected on your website, figure out which tools and technologies that you have deployed and what your third party integrations are. If you collect any sensitive data categories, such as health data, financial information, or biometrics, then you have to exercise extra caution, as you will likely have more onerous compliance obligations, more regulatory scrutiny, and you may actually need to obtain consent. So we really recommend that you consult with your legal counsel in that case. Figure out if you're using any website tools that are considered risky, and what is currently considered risky may be surprising. These include the incredibly common megapixel, which has been the target of 1000s of private plaintiff lawsuits and claims based on the wiretapping theory. Also, are you using chatbots session replay technology, all very common very useful website tools that are becoming the subject of both regulatory action and private plaintiffs claims and class actions. Do you have videos in the website? And if so, do you use tracking technologies in connection with those videos to send information about who is viewing them, how they interacted with the website, all that kind of information to a third party that has also been the subject of wiretapping claims and claims under the video Privacy Protection Act. So if you are using videos even if they're your own videos, not even advertising videos and you are sharing information about video viewing with meta if you're using the meta pixel, you really need to pay extra attention because we're seeing a lot of enforcement and litigation and activity in that space. Are you selling or sharing data? This concept is much broader than you think selling is really any disclosure to third party in return for valuable benefits. So it doesn't even mean that money has to change hands. And a sale was in fact the focus of the Sephora and DoorDash action. Using really common third party retargeting cookies and marketing cookies will likely be a sale in the eyes of the regulator, even if you don't think that it meets the common sense definite meaning of sale. And in that case, you have to provide an opt out, and Sephora didn't provide an opt-out on the website. And they used very common analytics, cookies, retargeting cookies, marketing cookies. So this is a really, really important website practice that you need to be on top of. Of course, if you collect children's data, you will have heightened compliance obligations, and you're going to face more scrutiny from both regulators and in the public. We know that the collection and processing of children's data is an enforcement priority for state regulators and for the FTC. And the recent settlement by the California Attorney General against tilting point media was in fact based on that company's collection and processing of children's personal information without appropriate consent, and also their age and appropriate advertising to children. Tilting Point media, which publishes a popular SpongeBob game was not only required to pay $500,000 as part of the settlement, they also had to take several corrective actions and implement some very specific operational requirements. It's worth noting that Tilting Point Media was also found to be violating the federal Children's Online Privacy Protection Act COPPA and also the California unfair competition law UCL. So actions by AG are not limited to the CCPA. There are also many other laws that are relevant.

07:10

So tip number two, now that you know it is on your website, make sure you get your website disclosures in order. Does your privacy policy accurately reflect everything that you have on your website and everything that you collect on the website? What are your data practices? What kind of data do you collect? How do you share it? Where does it go? How can consumers exercise their rights with respect to the data that you collect? Your privacy policy has to state all these things. And it has to tell consumers how they can exercise these rights in an easy way. It's worth noting that under the CCPA, you have to update your privacy policy at least once a year. And what that means is that the the effective date or last review date of your privacy policy should never be older than 12 months. If you have an out of date privacy policy, that is very easy for regulators to find. And that is evidence of non compliance. So this is something that is pretty easy to comply with. As as part of your broader compliance program, just make sure someone who's on top of reviewing the privacy policy at least once a year. Even if you decide that no changes are needed, you review the policy, everything is so accurate, it's up to date for all the new state laws. Make sure that you update the effective date or the last review date so that it is clear that the policy is not out of date. If you're subject to this CCPA California, you also have to provide a notice at collection. This is different from the privacy policy, it is a very clear notice that has to be provided at the point of collection. And it has to cover what the CCPA prescribes for a notice at collection. So this is worth paying attention to. Another really important point is that you should review any representations and badges on your websites. What kind of statements are you making about your privacy and security practices? And I'm now mostly talking about statements outside of the privacy policy. Maybe you are claiming to be 100% GDPR compliant, maybe you are claiming that you have the absolute best security in the industry? Are other statements entirely true. Are you using badges such as GDPR compliance or HIPAA compliant? Just paying a third party for the use of those badges doesn't make you compliant with those laws. And in fact, displaying them if you are not compliant is in itself an actionable violation. And we have actually seen some regulatory actions focused on this. So if you are planning to make any statements representations about privacy and security, or if you're planning to use any of these badges, make sure that you've run that by your lead either internal legal or your outside counsel. Because use of these can have real legal consequences. And if you are using them and they're not actually accurate and true that is actionable as a misrepresentation potentially as a as a misleading act as a deceptive practice, there are many many pitfalls there.

10:27

Make sure you disclose the use of any tracking technologies, any session replay and chatbots be clear that it is in fact a chatbot, where users are interacting with not a real person. And of course, pay a lot of attention to use of the metapixel. It is still very commonly used as a very handy tool for websites. But you have to exercise caution if you use it and make sure that you provide the required disclosures and get the appropriate consent if needed so that you are not vulnerable to a wiretapping lawsuit. Make sure that you have a solid consent management tool. Make sure that involves getting affirmative consent where required and we recommend that you talk to your legal counsel to figure out if you in fact need to get affirmative consent to anything on your page. On your website. Make sure it's easy for users to find the consent management tool. And you need to honor universal opt out signals such as the global privacy controller GPC. And I will cover cover more of that shortly. And don't forget, if you're collecting any data offline, you need to provide notices there too. And they have

to be appropriately aligned with your online practices, you have to make sure that there aren't any discrepancies, we are actually seeing a little bit more regulatory attention now on offline data collection. So don't forget that important point.

11:58

Tip number three, make sure your consumer opt-in tools are actually working. This is a big enforcement priority. And again, this is really low hanging fruit because it is pretty easy to figure out on your website if these tools are not working. It is not enough that you have the updates and choices on the website, they have to actually be functioning properly. And you have to address consumer requests appropriately on the back end. Regulators can and will audit you so make sure that you have a paper trail of compliance ready. And we have fact heard from the California regulators that they will exercise this audit right the right to come and look under the hood, they are very interested in how these requests get implemented throughout an organization on the back end. If you use a cookie banner with an accept button, make sure that no non essential cookies fire on your website. Unless and until the visitor clicks accept. It is incredibly common for these banners consent tools to not function properly. And there are many handy tools out there, including those used by regulators and plaintiff's lawyers to find nonfunctioning cookie banners.

13:13

You also have to honor universal opt out mechanisms, like the global privacy controls. And what this means is that your website needs to recognize if a visitors browser is set to opt out of say a sale of information or other privacy protective settings. Support didn't recognize the global privacy control. And this was a big part of the case against them. If you're using a vendor to do your consent management tool, they should be able to configure your website to honor the global privacy control. It's really, really important and non compliance is really, really easy to find if you go to website and you have the right tools to evaluate whether that website honors the GPC. And in fact, a recent study by the privacy tech company data grail of 5000 websites found that 75% of them did not honor the global privacy control, which is a pretty staggering number considering how important this was in the Sephora settlements and how much we know that the regulators do focus on this. So it is a very, very important point. Make sure you talk to your content management vendor or whoever configures your website. Your website needs to recognize the global privacy control.

14:33

Make sure someone actually handles consumer requests. If you don't assign someone to do it. Nobody who's going to do it is the email in your privacy policy actually monitored inbox. Don't set up a privacy@company.com email and then not have anyone look at the emails that come in that is a surefire way to upset consumers and ending up on the regulator's radar

15:04

However, the app that's carried through which third party databases has consumer information, this is where it's really important that you've done some kind of data inventory, some kind of mapping or audit to figure out where all this data is, is being held. Because if you get an access or a deletion

requests, you have to search all those third party databases, in addition to your own internal databases. There are some really great privacy tech tools that can help you with this. So it doesn't have to be a manual process. But there are a lot of pitfalls if you don't do this correctly. And something we do see sometimes is a data subject or consumer submits an Access Request, they get a response with the data that an organization holds about them. They follow that up with a deletion request, the organization confirms, yes, we have deleted all your personal data. And then they follow up with another access request. And it turns out that the organization still had some data, maybe it was in some databases that they forgot, maybe they didn't do a proper inventory, they didn't know where all the data was. Now that consumer has some very clear evidence of non compliance against you can, they're pretty likely to take that to regulator and complain about it. Or they may tweet about it. And regulators pay attention to that as well. And it could lead to an investigation. And finally, on this slide, prepare for regulator audits. Both the California Attorney General and the agency have stepped up, they have powers to audit companies, they are going to do it, you have to make sure that you have solid evidence that you have a good paper trail, that basically that you can show your homework to the regulator to make the case for your compliance program.

16:56

Tip number four, avoid dark patterns and nudging. And what I really mean here is in essence that you cannot make it confusing and difficult for the user to exercise their right. Don't have a complex of that process hidden behind many clicks. Don't make the app that link grayed out and tiny font. We see this all the time, it is very unpopular with the regulators. Don't shame the consumer for exercising their rights. And don't ignore the requests. As I mentioned, if you ignore a consumer and upset them, that is a very risky behavior, it can get you on regulators desk and it can lead to an investigation. So make sure that you address any consumer requests or even queries promptly, and that you make sure that they feel like you're handling their requests.

17:51

Finally, make sure that your unsubscribe links in your marketing emails actually work is something that should be very simple, but there is still a lot of noncompliance there. And again, it's a very easy way to upset a consumer and it can lead to regulatory complaints.

18:08

Tip number five is really about data hygiene. This is where I want to emphasize the importance of data minimization. Another way to end up on the regulator's radar is if you have a highly publicized data breach, and if it turns out that you collected and retained more data than you needed, and more data than you said that you would collect or retain. That means it didn't comply with data minimization requirements, then you are much more likely to have an investigation against you. Of course, also always keep an eye on your security measures. A really important part of that is role based access and password hygiene. Make sure that only employees who have a need to see personal data have access to it and make sure that you rotate passwords and immediately disable access for outgoing employees. Data breaches are incredibly common, and many of them are caused by current or former employees, whether by accident or on purpose. So it is it is incredibly common that data breaches are actually caused by a human at the organization and you can prevent a lot of those risks by having really, really tight role based access controls and really good password hygiene.

And of course make sure someone is in charge of your security measures. Make sure that you document that you have reasonable security in place. Document this before anything happened. Data breaches do happen, they can happen to any company, but it is it is a defense and a protection for you if you can show that you had put security reasonable security measures in place before anything happened.

19:52

Some quick bonus tips to wrap things up. As I mentioned throughout it is really important to create compliance records to have a paid betrayal and make sure it's time stamped, you can send it to your lawyer, they will keep you record that shows there's a timestamp to email. So you have a record of your security measures, make sure that that gets circulated. So that you can provide evidence that you had security in place before something happened. And then, of course, your security and privacy program is only as strong as your weakest link. And sometimes that weakest link is your vendor actually, quite commonly as your vendor. So you do need to have a really solid vendor management program. And that includes vetting how vendors will use your data, how good their security is, what the contracts look like, what can they actually do with the data? Are they allowed to sell it? Or are they allowed to use it for their own purposes. These are really, really important controls you need to have in place when you deal with the vendors. And, of course, conducting employee training is a really important part of any privacy compliance program. And here, I really urge you to set up a regular annual program for your existing employees or a lot of really good elearning providers, and also make this part of your new hire protocol. And of course, make sure that you keep a paper trail of all this training that you provided, this is going to be really solid evidence if you ever have a regulator asking questions, if anything happens, you really want to be able to show that you that you have conducted regular employee training and that the level of training is appropriate to the sensitivity and the risk of the data that you have. So that was a quick walk through with some practical tips on how to avoid ending up on the regulator's radar and also how to avoid the attention of private plaintiffs. If you have any questions or you want to chat about your privacy compliance program, feel free to reach out to me. My email is awestfelt@gunder.com and keep an eye out for more of these bite sized presentations in the future. And thank you all for your time today.