Ain't No QSA 4 CCPA

As of January 1, 2020, the California Consumer Privacy Act (CCPA) is in effect and impacts numerous businesses that collect or process the personal information of California residents. The CCPA carries potentially stiff penalties for noncompliance, but the actual text of the law does not provide a clear roadmap for companies to feel comfortable that they are doing things the right way. As such, we are already seeing dramatic disparities in how companies across the world are interpreting the CCPA and choosing to implement its requirements. They can't all be right.

To compound matters, the California Attorney General has not yet issued its final regulations on how the CCPA will be enforced, so many companies are feeling like compliance is a guessing game at this point and are desperate for answers. As we witnessed with the advent of the EU's General Data Protection Regulation (GDPR), there are plenty of people willing to give advice on how to comply with the law, but many are ill-equipped to provide both technical guidance and legal interpretation. And so, as we saw with the GDPR, there is a rampant proliferation of bad advice from vendors and consultants clogging up Google searches through their SEO efforts. Anyone that has tried to find answers to GDPR questions over the last few years should know exactly what we're talking about.

In this article, we are going to cut through the vapid regurgitation of what the statute says (that you can find pretty much anywhere) and get to the heart of what companies should be focused on to address the largest risk under the CCPA: **class action data breach liability**.

The CCPA, unlike anything we've seen before in the United States, carries statutory minimum penalties of $100-750 per record per incident for data breaches resulting from a failure to implement "reasonable security procedures and practices." Unlike the rest of the CCPA, these penalties are in full effect as of January 1, 2020 and we have already seen the first class action filed that implicates the CCPA in *Barnes v. Hanna Andersson, LLC et al.*, Case 4:20-cv-00812-DMR (N.D.CA. 2020) which is seeking damages in

Related Capabilities

- California Consumer Privacy Act (CCPA)
- Privacy & Social Media

excess of $5,000,000. So, as we should suspect, many companies are scrambling to determine what controls constitute "reasonable security procedures and practices" and are working to put whatever they think that means into place. Enter the charlatans.

The term "reasonable" is a legal term that has a basis in centuries of jurisprudence and is not something that lends itself to any prescriptive checklist. Indeed, although a previous California Attorney General discussed reasonable security, the current California Attorney General, to date, has issued no guidance whatsoever on what constitutes "reasonable security" and so interpreting this amorphous standard can only be competently done by a lawyer.

There is no such thing as a CCPA certification. Any vendor or consultant that claims to be able to provide such a document is, at best, wrong. Much like the GDPR, the CCPA attempts to establish a standard of care for how to protect data, but it is doing so through a legal mechanism. This isn't like PCI DSS, ISO 27001, NIST 800-53, or any other technical standard. Unlike PCI DSS, which is not a law, there are no CCPA auditing bodies, and there are no CCPA QSAs. Only the California Attorney General could feasibly fulfill such a role and that is certainly not what the AG's office is going to do. Anyone that is providing a certificate or stamp-of-approval on a company's privacy or security posture for CCPA purposes is wrong and no competent lawyer would sign off on such a document. One day a California court may recognize some certification as establishing reasonable security, but that is not something we expect in the near term.

This, however, is not to say that it is impossible to meet this standard. Far from it. Companies should be used to having to interpret legal requirements and develop internal policies and processes to meet them in a variety of other areas like accounting, employment, health and safety, etc. There is no reason to believe that the same approach that has worked for these areas will now be useless simply because we are applying it to a perhaps seemingly more technical field like "cybersecurity."

So, instead of freezing up and waiting for Superman to save them, how can companies begin to tackle the development of reasonable security for CCPA purposes? We have developed a simple initial 5-step process to help companies get moving so that they can feel better prepared for when their security posture comes into question:

1. Recognize that the CCPA is a law and so it is important to involve counsel when interpreting it. What constitutes "reasonable" will largely be dependent upon what a large number of similarly-situated companies are also doing. Outside counsel will have the exposure to large numbers of clients to be able to guide companies on what others in the same field are doing. Acting as an outlier is rarely going to be considered a "reasonable" position.
2. Identify relevant industry standards and work to conform the company's information security posture towards them. We have written on this topic before [here]. While this step certainly helps move the needle towards "reasonable" security, it is also critically important to remember that compliance =/= security and so even perfect adherence to an industry standard does not guarantee that a company has been acting reasonably in their efforts to secure data. So more is needed.
3. Prioritize patch and vulnerability management. As we discussed in the previous

article [here], there are studies that indicate that 60% of data breaches are the result of poor patch management practices. Assuming the veracity of these findings, this is the area of greatest risk and should be priority #1 from a technical implementation standpoint.

4. Develop or enhance third party risk and security management. Anytime a company shares any data or access to critical systems, it is relying on that third party's own information security program to protect the company's data. If the company isn't performing adequate diligence with continuing oversight, it is creating a gaping hole in its security posture. Offloading data does not offload the risk, the company is still responsible for the failings of its subcontractors.
5. Develop a solid incident response plan and practice it. We've all heard the cliché "it's not if but when," which means that courts will have heard it too. As we have seen with multitudinous AG and FTC actions related to data breaches in other jurisdictions, the lack of reasonable and timely incident response processes is not something for which we expect there to be much forgiveness. Developing a solid incident response plan will require stakeholder input from across an organization and will take time to implement and practice. Companies may have a difficult time establishing reasonableness for incident response processes that only exist on paper.

The CCPA is an extensive law that impacts much more than a company's website privacy policy. It's important to recognize that there is no Easy Button and, as enticing as it might seem, there is no checklist or certificate that will ensure "CCPA Compliance." The California AG has issued estimates for initial CCPA compliance costs [here] and these need to be considered as companies weigh the risk of noncompliance. Perhaps the most obvious takeaway from all of this though is that the best way to avoid class action liability for data breaches is to avoid data breaches. Enacting reasonable security will help both avoid data breaches and avoid CCPA class action liability.