The California Consumer Privacy Act (CCPA) and the American Data Privacy Protection Act: The Good, The Bad and The Ugly

By Dr. Eric Cole, Advisor - Theon Technology

Since 2018, there has been serious discussion of a new national privacy law promising Americans enhanced data protection, much like the European Union's General Data Protection Regulation (GDPR). Nearly five years later, the US is still the only prominent actor in the world without an established federal data protection. In the US, we have always relied on state-level and local laws such as the California Consumer Privacy Act (CCPA), coming into effect on January 1st, 2023, as opposed to the government proposing something that serves the nation in its entirety. It's a step in the right direction that Congress is finally acting and is putting a law in motion that will protect US citizens, our information, and precious data. However, the proposed bill is not without potential flaws and implications; some may even argue the proposed bill falls short of the protections already in place at the state level. In addition, the law would fall under the scope of the Federal Trade Commission (FTC), which means that the law would only cover existing issues already addressed by the FTC. These issues include identity theft, children's privacy, consumer fraud, and only some cybersecurity issues.

What's more, as we embark on the new year, we expect to see a spike in regulation across the country. As we see California implement CCPA, other states will begin to follow suit. At a national level, we will see a rollout of new stricter regulations, and business leaders must be prepared. Organizations that have yet to play in the regulatory playground or have not had to deal with GDPR will be caught in a difficult position and will be pressured to implement these changes fast. As a result, they will be rushed through the process, all due to the US being slow to enforce these laws.

What does CCPA mean for the wider nation?

After various delays, on January 1st, 2023, the California Consumer Privacy Act (CCPA) will come into effect, and some common questions I've been hearing are:

- What does this mean for various organizations across the country?
- What impact will it have?
- How should organizations prepare for the rollout?

In today's interconnected world, most organizations and states deal with California in some capacity, so my advice is to look at CCPA as a precursor to what is going to be happening at a national level in the very near term. If you take a step back and consider January's rollout vs. what is being rolled out nationally, you'll notice it's very similar. Organizations and business leaders across the country should assume they must comply and follow all the regulations regardless of their state. Further, whether you deal with Europe or not, you should be GDPR compliant as GDPR will be similar if not identical to what is being proposed at the state and national level in the US. It is a significant hurdle to consider, however, because the US is so far behind in implementing these regulations, it will be a rushed ordeal.

What about encryption?

Everyone is overlooking the encryption of consumer data and ensuring keys are stored on separate servers. Most organizations have encrypted their data in the past, but the problem is they are leaving their data exposed, similar to locking your door but leaving the key under the floor mat. Are we locking our door? Yes. Is it really effective and safe - not in the slightest. A lot of old regulations we have grown accustomed to were all about encrypt encrypt, encrypt, but it remained unclear as to what was considered good or bad encryption. The majority of data theft we've seen in the US was from data that was "technically" encrypted but wasn't encrypted correctly because the keys were all the same. Today, regulators are doubling down and enforcing the use of different keys, which must be on separate servers. This is where we will see many organizations get themselves in hot water in California and across the country if strict enforcement is implemented. Historically, the US has not been a strict enforcer of these types of regulations, and as a result, executive teams are not taking them seriously. The difference between laws in the US and GDPR is that GDPR was strictly enforced from the start and made an example of companies who were not taking it seriously by making them pay millions for their mistake. As a result, the law was taken very seriously.

The most important factor in getting it right and establishing efficiency is ensuring individuals and organizations are compliant. The reasons why organizations are compliant with GDPR has nothing to do with the European Standard. GDPR is effective because of the enforcement and significant fines. If we look at PCI and HIPAA compliance, the US has struggled with enforcement, and for CCPA and ADPPA to be effective, better enforcement will be critical to its success. It will be a make-or-break moment, and questions like who will enforce the law? What will the penalties be? and what are the costs of implementation? These questions and answers will have to be clearly defined in order to raise the likelihood of compliance and prove effective or ineffective.

The good, the bad, and the ugly

If and when these laws come into effect, the US government will have made tremendous strides by introducing a protection law at both the federal and national levels. One immense benefit of this is that it is being kept bipartisan and will be clear and concise, with no contradictory state laws that could get messy. But as with anything, there are potential challenges and downsides. With the ADPPA, a tremendous negative is that it is not compatible with European laws and will have many contradictions with companies abroad as well as US subsidiaries abroad, and different laws and regulations will be enforced in addition. In order for CCPA and ADPPA to be successful, strict enforcement will be essential. As we've seen with our European counterparts, if companies don't have real consequences or penalties, enforcement will be unlikely. What will the enforcement of CCPA and ADPPA be? One thing that is clear is that it will have to be enough to scare to take action and implement.

Overall, decision-makers have much work to do in order to make CCPA and ADPPA a success. Enforcement will be the most crucial factor. The stricter the enforcement, the higher likelihood of compliance and will dictate implementation willingness across the board. In the US, regulators have notoriously just given a smack on the wrist, ultimately causing executives and security leaders to not fear potential consequences. What needs to happen is CIOs and Security officers need to communicate effectively to the executive team that these regulations could result in significant fines. They should ask themselves whether they want to be the company that pays the 10 million fine and is made an example of?

Lastly, compatibility with GDPR will be key because the world is so interconnected in every sense. Because GDPR is tried and tested, the closer CCPA and ADPPA are made to mirror it, the bigger a win it will be for everyone.

About the Author

World-Renowned Cybersecurity Expert With more than 30 years of network security experience, Dr. Eric Cole is a distinguished cybersecurity expert and keynote speaker who helps organizations curtail the risk of cyber threats. Dr. Cole has worked with a variety of clients ranging from Fortune 500 companies, top international banks to the CIA. He has been the featured speaker at many security events and also has been interviewed by several chief media outlets such as CNN, CBS News, FOX News and 60 Minutes.