perrimarketing
www.perrimarketing.com• info@perrimarketing.com• (423) 987-4925

Whitepaper

The GDPR has Hit the Shores of the United States, Bringing with It a Data Security Domino Effect in States' Legislation

Almost everything we do in a day is tracked on a computer. The average American spends 24 hours a week[1] online, and that is just active Internet use. Most of us have a smart phone in our pockets at all times with geolocation tracking passively collecting data on where you travel, and we may not even have the power to turn geo tracking off according to a recent lawsuit[2]. Whether we like it or not, our lives are inexorably tied to logged activity on a computer.

Allowing corporations to access our data is often the price we pay for free services like Facebook and Google, leading to the question "is it really free?" However, the idea that these corporations collect detailed digital identities of their users makes many uncomfortable, especially when explicit, written consent to access our data is rarely asked. The recent Facebook, Cambridge Analytica scandal[3] sparked an ethical debate and public come-to-Jesus moment over the scale and power behind this widespread, unwanted data collection. And while Big Data is certainly a threat to our privacy, it's also a threat to our pocketbook. With more purchasing happening online, unprotected credit-card data is wildly abundant on the internet and cyber-criminals are taking advantage of this.

Until the recent GDPR enactment (May 25, 2018), corporate attitudes towards data collection have always been *the more the merrier*. But now, the risks of owning vast amounts of user data are starting to outweigh the benefits, given the wrong circumstances. It is up to the executive, the employee, the government, and you (the consumer) to have greater awareness for soliciting and managing the data that defines us all.

The days of cyber-security being simply an IT issue are over. In a recent Ponemon/IBM study on what

CISOs worry about in 2018, "lack of competent in-house staff" was the number one concern. There is a serious gap between the vastness of an organization's cyber-threats compared to the level of cyber-security literacy their employees have. Couple this dilemma with the fact that those tasked with managing security — the IT and compliance teams — are understaffed and so overwhelmed with IT complexity, security is most times a back-burner item.

This security gap could have a serious effect on the bottom line for any business, and now that the GDPR is in full force the stakes for punitive damages are even higher. Another recent Ponemon/IBM study shows that data breaches are larger, costlier, and take longer to discover year after year. The GDPR will certainly amplify the ramifications for cyber breaches in the years to come.

The GDPR is a legislative attempt to address this growing cyber security threat, and several US states have data breach notification laws[4] on the books, in answer to the EU's May 25, 2018 enaction of the regulation. However, the latest data from the IBM/Ponemon 2018 Cost of a Data Breach Study reports that the average time it took to discover a data breach in the reporting window was 197 days — six days longer than the previous year's 191-day average. We seem to be getting worse at this.

The study also found that data breaches are, and have been, getting bigger and costlier. The trending data does not bode well for companies fighting cyber-crime in 2018, and right now, we have a long way to go before reaching the GDPR or state-level data protection regulation compliance. The cost? A recent breach targeting Ticketmaster UK shows evidence that the data exfiltration took place over (at least) a four-month period. Collective applause for Ticketmaster UK for a discovery time less than the 197-day average, but trouble awaits the online ticket broker. Because the breach started before GDPR go-live date, and spanned after, it is highly likely that Ticketmaster UK will be fined the post-GDPR penalty of £17 million, as opposed to £500,000 had the breach been discovered before May 25th, 2018.

What does this have to do with John Q. Public in Rapid City, Iowa? More and more. It is the marketing function in most large organizations that manages data. Even the smallest company might have hundreds of thousands of contacts in its marketing automation or email systems. And these organizations no doubt have a smattering of EU citizens' contact records in them. And all it takes is one EU citizen compliant from a misplaced email, or worse yet, a photo from a conference that can be used to identify a contact, and your organization will be under the watchful eye of the European Commission[5]. Your company is liable and there could be personal liability

to any employee that mishandles an EU citizen's PII (Personally Identifiable Information).

Okay, so the GDPR is way over there in Europe, that has nothing to do with me. Think again. If you are willing to bet that amongst the 100,000 records in your business's database, no EU citizen records are present, I have some beach property in Arizona to sell you. And even if you can verify that there aren't, you are staring down the barrel of U.S. legislation for data security, what looks like a domino effect from the GDPR regulation.

- The North Carolina Identity Theft Protection Act has been around since 2005, and an even tougher law in that state is up for vote, the Act to Strengthen Identity Theft Practices or ASITP[6]. ASITP has similar requirements that GDPR has including a timeframe for notifying affected individuals in the event of a breach.
- California recently passed one of the toughest data privacy laws in the U.S., the California Consumer Privacy Act of 2018[7]. This law goes into effect in 2020 and will require organizations such as Google, Facebook, Amazon and others to disclose type of data collected and allow consumers to opt out of having their data sold or shared.

The "GDPR" is here, in the U.S., in one form or another and there's no hiding from it. It might not be called the GDPR in the U.S., but effectively you and your organization are under the gun to protect consumer data, watching all instances of any data asset that could identify an individual, possibly down to a mere picture. Then, you have to keep track of that data, and if requested by the consumer, you must remove it and provide proof of the same. You are also going to be tasked with breach notification within specified time frames – the GDPR says 72 hours; North Carolina is going to require 15 days. Given that the average time to ID a breach in 2017 was 197 days, it's clear we're in big trouble.

We talked about these scenarios in our presentation at Cyber Security Atlanta, in Tony Perri's presentation titled "The GDPR Effect on North America and the Land Mines Currently Being Planted." The last national data privacy law was put in place in 1974, long before the birth of the Internet as we know it today. Now that the GDPR is here, there is a precedent for a national data protection law and the U.S. is currently leaving it up to individual states to take the lead in legislation for consumers' rights for how their PII is collected, used and disposed of. And most difficultly, notify a consumer when their data has been used without permission.

- North Carolina and California are just the first domino in the U.S. Other laws are coming:
- Alabama passed its first data breach notification law in June of 2018.
- Arizona updated its breach notification law to define PII and add notification timelines.

- Colorado now requires formal InfoSec policies plus oversight for third-party data partners.
- Louisiana updated its data breach law with timeframes for consumer notifications within 60 days. (Remember that 197-day to discover thing?)
- Other U.S. states' breach laws updates can be found here[8].

For the marketing executive, the responsibility to adhere to data privacy compliance standards will increasingly fall on your shoulders in the coming months and years. CMOs' responsibilities are expanding, and so are their budgets. They're now invading the territory of CIOs in technology spending to accelerate the pipeline and perfect sales and marketing processes, doing what they can to justify their increased marketing spending and its accompanying jump in corporate responsibility. PII is a wonderful thing and for a CMO can be his/her lifeblood depending on its quality. But now that the marketing department must collect, analyze, and protect the massive amounts of marketing data they possess all while making sure that they are proving the ROI of these practices to their Boards of Directors, the pressure to deliver is greater than ever.

As seasoned marketers with 20+ years in the software industry, Perri Marketing knows the power of consumer data. We've been using it religiously for years with our CRM software and with marketing automation tools that we use daily. This unprecedented access to data has revolutionized modern marketing, and we believe for the better. However, on the heels of the latest research and recent data protection legislation, a cultural shift in the way we think about and handle data needs to happen. Cyber security literacy is critical knowledge for the masses now to protect our most sensitive personal, enterprise, and even state-level data.

If you're entering the marketing technology space, or are looking to, consider partnering with Perri Marketing. We are both technology and marketing experts, and our knowledge of the fledgling data privacy legislation (in the US and abroad,) as well as the benefits of marketing automation could be a significant asset to your company in today's era of growing cyber-security risks. We offer a host of marketing services and automation software at a fraction of the cost of large agencies. For a complimentary discovery call, or to view our past work in the software and technology industry please visit **perrimarketing.com**.

Written by Alexandra Perri.

Alex is a Sr. Copywriter for Perri Marketing. After graduating from Brevard College, she worked in the marketing department at her alma mater before making the switch to PMI. Alex has a journalism degree from Brevard, where she also played soccer, and in her free time works for an outdoor, Montessori-inspired preschool at Just Ripe Farm in Brevard, NC.

---

[1] https://www.technologyreview.com/the-download/610045/the-average-american-spends-24-hours-a-week-online/

[2] https://www.reuters.com/article/us-alphabet-google-privacy-lawsuit/lawsuit-says-google-tracks-phone-users-regardless-of-privacy-settings-idUSKCN1L51M3

[3] https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

[4] https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/

[5] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[6] https://www.ncleg.net/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_75/Article_2A.html

[7] https://www.ncleg.net/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_75/Article_2A.html

[8] https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/