Boston Hospitality Review

www.bu.edu/bhr

Published by the Boston University School of Hospitality Administration

Privacy Policies Outside the US and Effective Digital Marketing

By Mackenzie Miers, SHA ’21, MMH ’22

Digital Marketing - August 2021

About the Author

Mackenzie Miers, SHA ’21, MMH ‘22 (Digital Marketing concentration), her previous experience includes a venue sales internship for the renowned Live Nation Entertainment and a club lounge attendant for Intercontinental Hotel Boston. At BU, Mackenzie was a four-year scholarship athlete, playing for Boston University's women's basketball team. Within her athletic conference, she has been recognized for achieving the Patriot League Honor Roll each year for her scholastic success as a student-athlete.

Privacy Policies Outside the US and Effective Digital Marketing

Source: Image by greenbutterfly on Shutterstock

Foreign Data Privacy: Strict or Soft?

Digital is today's most popular form of marketing (Singh, 2021). Access to the internet has transformed our way of life; it enables people to engage with individuals from all over the world, thus strengthening a brand's ability to connect and boost awareness, campaigns, branding, sales outreach, community relations, and advertising among other forms of connections. Marketers are presented with platforms to speak with consumers all across the globe, whether through video, social media, or email. But marketing across borders, internationally, requires a more profound breadth of knowledge, particularly an understanding of the various laws that impact a company's ability to market to specific nationalities or customer bases.

For example, U.S.-based digital marketers must discern the data privacy laws relative to the homeland of each targeted customer. Interestingly, with the exception of California, data privacy regulations are genuinely relaxed within the United States. This means that it is in the marketer's best interest to follow guidelines under the strictest data privacy laws outside of the United States if they aspire to market globally, successfully.

"Europe, and almost everywhere else, is much more government-controlled. The government is far more involved with everyday life compared to the United States," explains Max Starkov, former president of HEBS, a hospitality-focused digital marketing

agency, and now an NYU professor of hospitality technology. “There is a different mindset in the U.S. It is less ‘government control’ and less ‘intrusive’ if you will.”

Despite the U.S. government’s relatively laissez-faire approach to digital marketing privacy, more than 100 countries within six continents have enacted some sort of data privacy law and regulation (Dearie, 2020). Thus, it is critical to know the essentials of some of our world’s other privacy policies, particularly to avoid significantly hefty fines that can be imposed, even if marketing naively. Plus, the advantages of strong knowledge in global marketing “will make up for all the disadvantages, as it gives marketers a much larger customer base, increases visibility, leads to higher revenue, reduces competition and offers more stability” (Gaille, 2017).

The European Union and GDPR

The improvements made in technology have undoubtedly changed how the world works, which is why the European Union (EU) decided that it was time to drastically update the prior 1995 Data Protection Directive (“The History of the General Data Protection Regulation”). It was in 2016 that the General Data Protection Regulation, or GDPR, was introduced and since then has impacted and influenced many other countries around the world.

GDPR shifts the power of privacy and connection to the consumer rather than the marketer. It allows consumers within the EU to ask companies for all the information that they have about them and to delete all that information as well (Cerulus, 2018). Additionally, consumers are given the option to either agree or disagree with marketers to use cookies when clicking through websites (Cerulus, 2018). Interestingly, marketers are not responsible under this regulation to notify consumers if there has been any sort of data hack. If a company does not fully comply with all of these standards, then they are subject to a fine worth up to 4% of a company’s annual turnover. A fine like that can cost companies billions of dollars.

An infamous example of non-compliance leading to billions in fines is the British Analytica scandal for which Facebook found itself at the center. Facebook was charged for deceiving its users into believing that their personal information could not be kept private. After a year-long investigation, Facebook was instructed to pay a $643,000 fine in settlements to the United Kingdom alone (Zialcita, 2019). Nominal in the scheme of the situation, it fails to account for many other settlement fees that Facebook also had to pay to various other countries. Facebook paid the United States a total of $5 billion as another settlement (Davies, 2019). The multi-billion-dollar Facebook was able to survive this scandal. However many other companies and organizations likely do not have that same luxury.

Australia and the Privacy Act of 1988

Updates to this Act, passed in 2014, state that "any company conducting business within Australian borders and is worth over AUD $3 million, is subject to following all the data privacy requirements" (M., 2020). However, a company could also fall under the Act if it collects private information for personal benefit, has mobile applications that require an email address for activation, or holds a large amount of sensitive data (M., 2020). The consequences of not abiding by the Privacy Act of 1988 are quite different from the previous few data privacy legislations. The severity of the consequence depends on which section of the Act was breached. It can range anywhere from a written apology (if there is an accidental privacy breach) to a fine worth AUD $2.1 million if the breach was not handled sufficiently (M., 2020). With this in mind, it is necessary to truly understand what kind of data is collected and keep abreast of managing all personal information safely, openly, and accurately.

Brazil and the General Data Protection Act

Brazil's General Data Protection Act, or Lei Geral de Proteção de Dados (LGPD), was inspired by Europe's GDPR and was passed in 2018 ("Brazilian General Data Protection Act", 2021). Similar to other regulations, it was designed to protect consumers' privacy by establishing rules on handling, collecting, and sharing personal data managed by organizations. Companies were given 18 months to adjust, and after that, they could face a variety of sanctions including "warnings, fines, embargoes, suspensions, and partial or total bans to performing their activities" if not all aspects of the act were being followed ("Brazilian General Data Protection Act", 2021). A large focus for the LGPD has to do with the famous "cloud" that people often refer to instead of saying their data storage. Since August 2020 LGPD will force many enterprises to change their once public cloud access to private networks with updated encryption services (Miyazu, 2021). Although there are other countries within South America that have data protection laws, Brazil has taken the most significant steps towards as strict of a policy as the EU's GDPR.

Canada and PIPEDA

On April 13, 2000, The Personal Information Protection and Electronic Documents Act (PIPEDA) was passed through Canadian legislation. Similar to the policies of the EU and India, the PIPEDA was created to protect the privacy of citizens by requiring organizations to disclose all personal information they use and validate why collections are in place (Tunggal, 2020). However, as in India, there are new proposals for an updated data privacy legislation. The Consumer Privacy Protection Act, or CPPA, intends to give more power to the Federal Privacy Commissioner so that he/she may fine or halt any organization that is not complying with the updated privacy legislation

(Solomon, 2020). The feedback to this legislation has been generally negative, as it does not change much except for the consequences that companies could face. For marketers, it is important to remain current on the progression of this legislation. If this Act is passed, comparable to GDPR and GDP, fines can result in as much as 4% of a company's global revenue. A fine this large could be detrimental to an organization and is subjected to any organization that collects data within Canadian borders.

China and Cybersecurity Law

China is known to have one of the most tightly government-controlled data privacy legislations in the world (Wagner, 2017). In November 2016, the Cybersecurity Law was passed by the National People's Congress. The Law was created to pass new regulations for internet usage and to give jurisdictional control over all content online, including unlimited data access (Wagner, 2017). The most important aspect to note is that the Chinese government can ask any organization that works within the Chinese territory, or is partnered with a Chinese company, for all the data they hold. This can happen at any time without provision of reason, which is why some foreign networks have been unhappy with this Law. Many of the United States' larger technology companies pushed against it, stating that having to share their source codes with the Chinese government increases the risks of it getting into the wrong hands. Microsoft and IBM are two examples of companies that used this argument as their main point to fight the Cybersecurity Law's strict policies (Dou, 2016).

Although it has been said that the intention of this law is not to halt foreign businesses from operating within China, firms that wish to do so had to invest in new data servers or hire expensive local service providers such as "Huawei, Tencent, or Alibaba, which have spent billions in recent years establishing domestic data centers" (Wagner, 2017). This allows the government to conduct random spot-checks or data collection whenever desired. Popular hospitality home-sharing app, Airbnb, has had to comply with all these rules, submitting personal information about its users for example, so that it may operate within the country (Wagner, 2017). Digital marketing in China is not impossible, but keeping data confidential is. Typically, the purpose of data privacy law is to protect consumers' data. This is not the case when it comes to the Cybersecurity Law in China.

India and GDP

In the past few years, GDPR compliance referred to almost all of the various data protection regulations across the globe, since it had the strictest rules. However, that may not be the case anymore with India's new Personal Data Protection Bill or GDP. This is going to be the most difficult for marketers within India who were accustomed to its prior relaxed data privacy program.

The GDP pertains to three specific areas of an individual's privacy: personal data, sensitive personal data, and critical personal data (Gill, 2021). The particular data a company collects determines the category of GDP by which they need to abide. Marketers must recognize the data categorizations. If a company fails to do so, it will be fined up to 4% of their company's revenue, or a fine of several billion dollars, whichever is higher. There are other punitive measures under this bill that range from payment of only a few thousand dollars to imprisonment for up to three years. A marketer may think they have a legitimate reason for data collection, as the GDPR has all eligible reasons for collection clearly outlined. However, it is up to the Data Protection Agency, or DPA, of India to decide on a case-to-case basis whether or not a firm's reason for data collection is indeed legitimate (Gill, 2021). So, if a company is trying to reach the Indian market, it would be in their best interest to abide by all the requirements and ask for a review by the DPA.

South Africa and POPIA

July 1, 2021 marks the start date of the new POPIA legislation, the Protection of Personal Information Act, in South Africa. It is imperative that companies comply, as punishments range and can include up to ten years in prison. Although the South African government has acknowledged the importance to have the right to access information, they believed that it was time for there to be an equal acknowledgment of the right of personal data protection ("South Africa", 2021). Mentions of a "data war" emerging has been introduced, as some companies consider this bad timing since the entire country is still trying to reconstruct the economy due to the hardships of COVID-19. However, others believe this is the perfect time to take the country's digital technology to the next level by implementing clearer policies (Mtimde, 2021). Either way, as of July 2020, POPIA is the country's digital marketing new normal.

Best Practices for Global Digital Data Savvy

1. **Educate, Educate, Educate!**

It is imperative to keep up with global changes in data privacy. Policies are continually evolving, so it is necessary for marketers to remain educated to understand proper steps and avoid serious consequences. The California Consumer Privacy Act for example is updated annually (Meyer, 2019). With constant evolution in policies all across the world, marketers must also remain updated. The more a marketer understands about an upcoming policy change, the easier it will be to comply with the new rules and regulations.

2. **Follow the Strictest Standard**

Economically, legally and practically, it would be wise to follow the strictest standard when marketing nationally or globally. Following one standard enables practicality from an economic and legal standpoint. Barry Barth, Director and Legal Counsel for Panera Bread, and adjunct faculty at Boston University School of Hospitality Administration shares, “It’s nearly impossible to market differently when marketing beyond one country; laws vary within states let alone countries. You narrow yourself if you market this way to people in Massachusetts and this way to people in California. As a practical matter, you need to follow the most restrictive standard.”

3. Know the Target Market

As data becomes increasingly more difficult to collect, it’s a great time to start researching other ways to find target markets. Does the audience utilize social media platforms? Would they complete satisfaction surveys for an incentive? Would they understand how to click on a banner ad? These are questions for behavioral analytics, research that allows marketers to tailor a unique experience for the target audience (Wiggins). This type of research can have great benefits in terms of agility, delivery, and successes of past marketing plans (Wiggins).

As data collection and privacy concerns only become more prevalent, global laws will likely emerge stricter and unforgiving. The time is now to put plans into place for savvy and responsible data collection and appropriate usage.

References

Cerulus, L. (2018, February 20). The General Data Protection Regulation: What it says, what it means. Retrieved from The General Data Protection Regulation: What it says, what it means

“Brazilian General Data Protection Act”. (2021, January 20). Retrieved from https://www2.deloitte.com/br/en/pages/risk/articles/lgpd.html

Davies, R. (2019, July 24). Facebook to pay $5bn fine as regulator settles Cambridge Analytica complaint. Retrieved from Facebook to pay $5bn fine as regulator settles Cambridge Analytica complaint

Dearie, K., Paruch, Z., & Xu, L. (2020, December 18). Privacy Laws Around the World: Infographic. Retrieved from Privacy Laws Around the World | Infographic

Dou, E. (2016, December 01). Microsoft, Intel, IBM Push Back on China Cybersecurity Rules. Retrieved from Microsoft, Intel, IBM Push Back on China Cybersecurity Rules

Gaille, B. (2017, January 14). 14 Pros and Cons of Global Marketing. Retrieved from 14 Pros and Cons of Global Marketing

Gill, P. (2021, March 15). Retrieved from Being GDPR compliant doesn't necessarily make companies ready for India's upcoming data protection laws

M., J. (2020, December 21). Australia Privacy Act of 1988. Retrieved from Australia Privacy Act of 1988

Meyer, C., Nara, F., & Franco, J. (2019, July 08). Countdown to CCPA #3: Updating your Privacy Policy. Retrieved from Countdown to CCPA #3: Updating your Privacy Policy

Miyazu, H. (2021, April 21). Brazil Data Center Market Current Trends, Segmentation, Key Players Analysis and Forecast to 2025. Retrieved from Brazil Data Center Market Current Trends, Segmentation, Key Players Analysis and Forecast to 2025

Mtimde, L. (2021, April 20). OPINIONISTA: Government must step up its capacity to handle and analyse big data. Retrieved from OPINIONISTA: Government must step up its capacity to handle and analyse big data

Read, A. (2020, January 21). Everything You Need To Know About Global Marketing Strategy. Retrieved from Everything You Need To Know About Global Marketing Strategy

Singh, P. (2021, January 02). The Popularity Of Digital Marketing In The World. Retrieved from The Popularity Of Digital Marketing In The World | by Dr. Preeti Singh | Technology Hits | Jan 2021

Solomon, H. (2020, November 18). Canada's Privacy Commissioner to gain power to recommend stiff fines under proposed legislation: IT World Canada News. Retrieved from https://www.itworldcanada.com/article/canadas-privacy-commissioner-to-gain-power-to-recommend-stiff-fines-under-proposed-legislation/438377

South Africa: Countdown for Compliance With Protection of Personal Information Act. (2021, March 25). Retrieved from South Africa: Countdown for Compliance With Protection of Personal Information Act

The History of the General Data Protection Regulation. (n.d.). Retrieved from The History of the General Data Protection Regulation

Tunggal, A. (2020, August 05). What is PIPEDA (Personal Information Protection and Electronic Documents Act)?: UpGuard. Retrieved from What is PIPEDA (Personal Information Protection and Electronic Documents Act)?

Wagner, J. (2017, June 01). China's Cybersecurity Law: What You Need to Know. Retrieved from China's Cybersecurity Law: What You Need to Know

Wiggins, J. (n.d.). You Can't Market to Strangers: What you need to really get to know your customers. Retrieved from

https://www.bizjournals.com/washington/news/2021/03/23/you-cant-market-to-strangers-what-you-need-to-really-get-to-know-your-customers.html

Zialcita, P. (2019, October 30). Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal. Retrieved from Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal.