INSIGHTS FROM THE BDO TECHNOLOGY PRACTICE

THE TIME TO ACT IS NOW: THE CCPA'S IMPACT ON STREAMING ENTERTAINMENT COMPANIES

On January 1, 2020, the California Consumer Privacy Act (CCPA) will go into effect. While all states have data privacy regulations in one form or another, California is the fifth largest economy in the world, so the impact of the CCPA will be felt far beyond its borders. In the U.S. alone, CCPA could affect more than half a million businesses. For these reasons, the CCPA is the most consequential data privacy regulation since the E.U.'s General Data Protection Regulation (GDPR) came into force in 2018.

For midmarket streaming entertainment companies, there is a misconception among executives that because they are multiple layers removed from interacting with the end-consumer, the CCPA regulation does not apply to them. They're in the entertainment business after all, spending their days developing content for podcasts or reading scripts, leaving the selling and distribution of targeted advertisements based on consumer data to third parties. Even for streaming companies that derive revenue through a monthly subscription model as opposed to ad-supported content, complying with the CCPA is a necessity. Recent deals with media conglomerates demonstrate that data gathering infrastructure that operates in the background of streaming services has become much more pervasive; technology is tracking viewing habits to target consumers with more relevant ads.

Does the CCPA apply to you?*

If you check one or more boxes, the answer is likely yes.

- ☐ Do you collect personal identifiers – e.g., email addresses, cookies, phone numbers?
- ☐ Do you engage in transfers of personal / device / household information to a third party?
- ☐ Do you collect electronic network activity data – e.g., browsing history, ad clicks, app usage?
- ☐ Do you collect data from visitors to your websites – e.g., geolocation, IP addresses, Google Analytics?
- ☐ Do you determine the purposes and means of processing personal information?

Do you have a for profit 'California business' with at least one of the following criteria?

- ☐ a) annual gross revenues exceeding $25 million;
- ☐ b) annually buy, receive, sell or share PI of 50,000 consumers, households or devices; or
- ☐ c) derive 50% or more of your annual revenues from selling consumers' personal information.

*For California resident data

Compounding these misconceptions around relevancy, compliance with regulatory requirements is the most common governance challenge for boards in all industries, according to the 2019 BDO Board Survey. This sentiment indicates that even when there is a *will*, the *way* is not always clear.

If streaming companies haven't already done so, it's critical they take steps *now* to comply with the CCPA. The cost of CCPA noncompliance? Civil penalties range from up to $7,500 per violation to be imposed by the government, or $750 per consumer violation if private action is taken. A recent amendment to the CCPA has provided some relief to businesses—the California Attorney General cannot bring an enforcement action until six months after publication of that office's regulations, or July 1, 2020, whichever comes first. However, this grace period does not apply to private actions by consumers. At the very least, streaming companies should by now have conducted vulnerability testing in order to achieve the Center for Internet Security's Top 20 Critical Security Controls (CSC 20) standard of "reasonable security." This standard dictates a minimum level of information security that all organizations that collect or maintain personal information should meet.

Meeting the aforementioned standard of "reasonable security" is the starting point for a more comprehensive strategy. To comply fully with the CCPA, streaming entertainment companies need to address two questions:

1. WHAT IS THE BREADTH OF THE PERSONAL DATA WE COLLECT, USE, SELL OR STORE?

The enactment of GDPR legislation in 2018 should mean that streaming companies with European resident subscribers have already done a lot of the hard work to put internal measures in place to process and secure consumers' personal data. The CCPA builds upon existing privacy law principles that prohibit unlawful, opaque and limitless capture and processing of personal data. Specifically, it gives consumers more control over their data. While companies can continue to collect consumer data under the CCPA, they have to disclose what personal information they have and who it's shared with or sold to. The CCPA's definition of "personal identifiers" encapsulates a broad sense of personal information, such as commercial, electronic, behavioral, biometric, financial and educational information, amongst others. For streaming companies in the podcasting business, for example, it's standard protocol to identify listeners through their unique mobile phone number—data that must be disclosed upon consumer request under the CCPA.

Unlike the GDPR, the CCPA doesn't overtly speak to privacy principles, which requires a designated Data Protection Officer and a written record of data processing. However, by virtue of its design—to be easily accessible and transparent to consumers—the CCPA necessitates that companies collect and store data in an **ethical** way. What is data ethics? It's an emerging branch of ethics that evaluates responsible and sustainable use related to data. It's about taking a measured and mindful approach to understanding the data needs of a given project and only collecting the information that is necessary. In previous Insights, Data Ethics Part I and Data Ethics Part II, BDO has put forth a Data Ethics Framework to guide companies on developing their own data protection and privacy program based on this philosophy. Its four main principles include:

- Clearly define the project and its benefits
- Use data proportionate to the project
- Understand the limitations of the data
- Develop a transparent program that holds the company accountable for the use of data

To streamline the collection and storage of consumer information, streaming companies should consider leveraging data discovery and analytics tools to identify where personal data resides within an organization. These tools can save a company time and money when developing and maintaining data inventories, which are critical components of any data privacy program.

Information That a Consumer May Request Includes:

Categories of personal information collected about the consumer, as well as categories of sources from which the personal information is collected.

Categories of third parties in which the business shares personal information.

Specific personal information collected about the consumer.

The commercial reason(s) why a business collects or sells the personal information.

Categories of consumers' personal information that is sold to various categories of third parties (note, the CCPA defines "sell," "selling," "sale," or "sold" very broadly).

Categories of consumers' personal information that is disclosed for a business purpose.

2. HOW ARE WE GOING TO RESPOND TO DATA REQUESTS FROM CONSUMERS?

Under the CCPA, streaming companies must disclose what data has been sold, what personal data is collected and/or any third parties with whom their data is shared upon request. It starts with a clear and concise privacy notice. A recent analysis by the New York Times of 150 privacy policies from major tech and media platforms indicated that, based on the Lexile level, or text complexity, many privacy policies exceeded standards for understanding, even for those users in professional careers. To meet data ethics standards, privacy policies should be written in plain language and in short, declarative sentences.

While it has become easier for individuals to attain their "consumer score," based on their online behavior, provisions in the CCPA mean that streaming companies need to create a specific process to handle data requests—a toll-free phone number for submissions and a webpage to ensure that consumers have the ability to opt-out. Passage of the CCPA portends an influx of consumer requests, behooving streaming companies to employ technology tools such as centralized tracking mechanisms and data analytic tools to automate the process. Companies can systematically process requests in the 45 day deadline by using standardized workflows, integrated Application Programming Interfaces (APIs) and Robotic Process Automation (RPA). The use of these tools can streamline requests and offer consumers more timely responses and request resolution.

In light of increasingly stringent regulations such as the GDPR and CCPA, every business—including streaming companies—has to be aware of how they collect, use and store their customers' personal data. To comply with consumer privacy legislation, streaming companies should adopt a data ethics philosophy. They need to understand and define the business purpose for processing personal data, and delete records in accordance with regulations or when it's no longer usable. Luckily, there are emerging technologies and providers that help companies automate these tasks to support compliance efforts.

While preparing for CCPA may be the short-term focus within your organization, it should ultimately support a more robust data privacy initiative. Information governance is the framework of policies, processes, technologies, accountabilities and controls to manage data across its whole lifecycle; from collection to destruction.

For an extensive repository of BDO resources on the California Consumer Privacy Act, visit the CCPA Resource Page.

CONTACT:

AFTAB JAMIL
National Technology Industry Leader
408-352-1999 / ajamil@bdo.com

ALEX IACOBELLI
Assurance Partner
310-557-8590 / aiacobelli@bdo.com

KAREN SCHULER
Principal, Governance, Risk & Compliance National Practice Leader
703-336-1533 / kschuler@bdo.com

SANGEET RAJAN
Managing Director, Governance, Risk & Compliance
415-490-3001 / srajan@bdo.com

ABOUT THE TECHNOLOGY PRACTICE AT BDO USA, LLP

BDO has been a valued business advisor to technology companies for over 100 years. The firm works with a wide variety of technology clients, ranging from multinational Fortune 500 corporations to more entrepreneurial businesses, on myriad accounting, tax and other financial issues.

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 700 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi national clients through a global network of more than 80,000 people working out of nearly 1,600 offices across 162 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.