DATA ETHICS AND PRIVACY
BRIEF

THOUGHTS ON THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018

You are probably already familiar with the CCPA and the fact that its January 1, 2020,[1] effective date is quickly bearing down on covered businesses. As a reminder, the CCPA requires covered businesses to provide California residents substantially increased notice, access, and control. For an overview of the CCPA, please see our initial client FAQ document.

As expected, there are many questions that have arisen in the course of analyzing the CCPA with our clients, data suppliers, and service providers, and, during the last month, through our participation in public workshops hosted by the California Attorney General. This privacy brief is intended to provide an update regarding Acxiom's drive for compliance readiness and to share our current thinking on certain aspects of the new law.

From a compliance readiness perspective, Acxiom has put together a comprehensive, cross-functional task force comprised of associates from our engineering, product, delivery, IT, security, legal, and data ethics teams to develop methods of compliance for Acxiom to utilize throughout the entire data lifecycle — from collection to destruction. Various team members have been meeting almost weekly since August 2018, with more than 1,000 man-hours expended on requirements-gathering and planning.

It was very important to get started early. Fortunately, Acxiom is not starting from square one. As a result of the GDPR initiative and our goal of future-proofing our compliance, we built a framework to handle many of the requirements. Nevertheless, there are significant differences that will require additional work to get ready for the CCPA. Below are a few examples of some of the similarities and differences.

Sample Business Requirement	GDPR	CCPA
Applies to both "offline" and digital personal data/information	Y	Y
Must provide detailed information on how personal data/information collected is used and processed	Y	Y
Must provide consumers access to information held about them	Y	Y
Must provide a right to rectification (i.e., correction)	Y	N
Must provide individuals a right to have data about them deleted	Y	Y
Must include a "Do Not Sell My Personal Information" link on websites and privacy notices	N	Y

Not only do we have extensive experience based on our GDPR readiness efforts, but we also built and have been operating a U.S. consumer access portal for almost five years. In our view, that puts us well ahead of our competition and will ultimately enable us to help our clients with their compliance efforts as well.

[1] The CCPA was amended in September, 2018. SB1121. As a result of that amendment, the Attorney General may not bring an enforcement action under the CCPA until six months after the publication of its final regulations or July 1, 2020, whichever is sooner. The AG has indicated it intends to publish its draft rules in early fall.

For questions on this brief, please contact the Acxiom Global Data Ethics and Privacy Team at GlobalDataEthics@acxiom.com

Based on the type of personal information that Acxiom has, the purposes the data is used for, and with whom we share the data, we have identified a number of broad, but interrelated, workstreams that must be addressed: data source compliance, impact to processing/storage of client data, impact to Acxiom data products/solution offerings, obligations for responding to consumer requests, internal documentation/training, external communications, and obligations for employee data. A more in-depth discussion of several of the workstreams, including our thoughts on some recurring questions, may be helpful.

One workstream that we have developed relates to our data sources. Based on a recent inventory, Acxiom has more than 200 third-party data sources that supply personal information. Importantly, the CCPA prohibits a business like Acxiom from licensing personal information to our clients unless our data suppliers have first provided explicit notice and an opportunity to opt out to California consumers in accordance with the CCPA.

For more than 20 years, and as part of our data ethics program, Acxiom has provided consumers notice about our data collection and use practices and offered U.S. consumers the opportunity to opt out of our marketing products. We have also required our data suppliers to do the same. As part of our CCPA readiness, Acxiom is currently contacting our data suppliers to obtain a supplemental certification that confirms they are in compliance with the notice and opt out provisions of the statute. We are also obtaining our sources' categorization of the data they provide to us, as well as documentation regarding each source's plan to respond to consumer access, opt out, and deletion requests. Speaking of consumers' access, opt-out, and deletion requests, another workstream we are focusing on deals with Acxiom's own obligation to respond to those requests.

The CCPA requires consumer access for three types of information: (i) data collected, (ii) data sold, and (iii) data disclosed. Covered businesses must be able to provide California consumers who make access requests a report showing the categories of personal information and "specific pieces of information" for the data the business has collected, and the categories of personal information and third parties for the data it has sold or disclosed. Acxiom is developing a framework that will allow us to track such information across our products.

While Acxiom already has a robust process in place to manage opt-outs and deletions, we are revisiting this process to ensure it meets the requirements of CCPA, including the management of opt-outs that are received from third parties acting on behalf of a consumer. Moreover, while the California attorney general is required to promulgate regulations on, among other things, what will be acceptable/required to qualify as a "verifiable request" for purposes of a consumer request, we have chosen not to take a wait-and-see approach. We are building our process based on guidance in other areas, such as the FCRA, as to what constitutes an adequate proof of identity.

In future privacy briefs, we will cover other workstreams. But before closing, it may be helpful to address several questions that have arisen related to the CCPA.

One over-arching question is whether Acxiom intends to extend its obligations and protections to consumers outside of California. The short answer is "yes," as we believe it makes sense and is consistent with our data ethics and privacy leadership to offer most of the rights granted to California residents under the CCPA to consumers nationwide. However, we do not plan to initially extend every right under the CCPA to consumers outside of the state of California. For example, we will not offer third-party opt-outs to consumers nationwide. Historically, our opt-out rates have been low. We suspect our clients and others in our industry share the same experience. Third-party opt outs have the potential to wreak havoc on covered businesses' marketing databases. We can envision entities, even non-profits, offering (for a fee) to opt consumers out of dozens or hundreds of covered businesses at once. That could be an attractive business model even if it was limited to California.

Another question Acxiom and others have is whether or not employee data is covered by the CCPA. While the CCPA's definition of "consumer" seems to include employee data, we believe the proponents and drafters intended the law to apply to consumers in their capacity as participants in the information economy, such as when buying a product or surfing the Internet. We are hopeful the California legislature will amend the statute to clarify the issue.

While several coalitions, including the U.S. Chamber of Commerce and the Business Roundtable, are proposing frameworks for a national privacy law, we do not expect passage of one before 2020. Therefore, it is imperative that companies start, if not accelerate, their CCPA compliance now.

For questions on this brief, please contact the Acxiom Global Data Ethics and Privacy Team at GlobalDataEthics@acxiom.com