Courtland Brooks

CCPA Review & Advisory, June-July 2020

On June 28, 2018, the California Consumer Privacy Act (CCPA) was signed into law. Although the final language of the act is still under review, the legislation went into effect on January 1, 2020. The Office of the California Attorney General has drafted the final proposed regulations and submitted the complete package to the California Office of Administrative Law (OAL) on June 1, 2020. Normally, the OAL would have thirty working days to review the submission for procedural compliance with the Administrative Procedure Act. However, an Executive Order related to COVID-19 has extended that deadline by sixty calendar days. If the OAL approves the final regulatory package, it will be filed with the Secretary of State as an enforceable state law[1].

CCPA is modeled after the General Data Protection Regulation (GDPR) enacted by the European Union in April 2016. GDPR went into effect on May 25, 2018.

CCPA was designed to protect the privacy of California consumers and provide greater control over the use of personal data. **The law mandates several rights**, including the **right to know**, the **right to delete**, and the **right to opt-out of the sale of personal information**. More restrictive provisions were included for the collection and handling of data related to minors.

The regulations under the CCPA apply to commercial businesses which operate in the state of California and collect, share, or sell the personal data of California consumers, and meet any of the following criteria:

- Annual gross revenues exceeding $25 million; or
- Possesses the personal information of 50,000 or more consumers, households, or devices; or
- Earns more than half its annual revenue from selling consumers' personal data[1].

The CCPA legislation applies to companies which conduct business in California without providing a clear definition of what constitutes that situation. However, the consensus is that **a business is not required to have employees or a physical presence in the state to fall under the provisions of CCPA**. If a company utilizes personal data from California residents and meets any of the three criteria, it will likely be held accountable under CCPA. The enforcement of CCPA is extended to any entity that owns, is owned by, or shares a common branding with a business that is subject to CCPA[1].

Online dating companies, vertical social networks, and other similar online social community services are likely affected by CCPA regulations if they provide services in the state of California under any product or commonly branded offering. If the parent company, subsidiary, or a common-branded service meets the criteria for CCPA enforcement, then all associated entities would be subject the regulation. This provision could potentially impact many online dating portfolios and online social communities.

If it is not immediately clear if your business is subject to CCPA, it is best to err on the side of caution and comply with its regulations.

California is home to nearly 40 million people, making it the most populated state in the United States. California represents a considerable share of the online dating market and online social community market in the US.

What does this mean for your Internet dating app or online social community?

In summary:
Businesses who are subject to CCPA regulations are required to take the following actions:

- Inform consumers if their data will be sold or shared
- Add a "Do Not Sell My Personal Information" option to their website or application
- Provide a toll-free number to facilitate consumer requests related to personal data
- Affirmatively collect consent to sell data from any consumer under 16
- Affirmatively collect consent from a parent or guardian for any consumer under 13
- Do not discriminate against users who exercise protections under CCPA[1]

Businesses who have enacted measures to meet GDPR guidelines will need to take additional steps to comply with CCPA[1].

The CCPA legislation provides significant recourse and penalties for violations. A data breach which compromises the personal data of California consumers may result in substantial damages if the business failed to follow reasonable security practices and procedures. CCPA institutes a private right of action for affected consumers, along with **statutory damages of up to $750 per individual**.

However, the damages may exceed the statutory limit if greater actual damages are proven. A class action lawsuit over a data breach affecting 100,000 California users could result in $75 million in statutory damages[1].

The key stipulation for the private right of action is the failure of a business to follow reasonable practices and procedures. The law does not describe what is considered reasonable. The Attorney General's Office indicates that numerous cybersecurity standards and certifications are available for reference by judges presiding over cases[1].

A provision for a 30-day cure period is included in CCPA to avoid statutory penalties. No definition of such a cure is provided or defined in the law. It is unclear how a business would cure a data breach which has already occurred and affected consumers[1].

The California Attorney General may seek additional penalties for companies who violate CCPA. The **damages could be up to $2,500 for each violation, increasing to $7,500** if the violation is deemed

intentional. The AG may also file an injunction against a business believed to be violating CCPA, which would suspend its operations[1].

The best way to avoid CCPA violations is to implement a comprehensive privacy policy.

The privacy policy must comply with CCPA regulations and should be updated at least annually. It should provide consumers with the details on what personal data is collected, why it is collected, and how it will be used. The policy should also explain the consumer's right to access the personal data held by the company, along with the process for requesting its deletion.

CCPA provides an extensive list of what constitutes personal data. It includes, but is not limited to:

- Real names, aliases, unique personal identifiers, online identifiers, account names
- Physical address, mailing address, IP address, email address
- Social Security number, driver's license number, passport number
- Biometric information
- Geolocation data
- Professional or employment-related information
- Network activity, search history, website or application interactions[1]

The categories of personal information covered under CCPA are highly relevant to many Internet dating services and online social communities.

As such, it is vital to clearly inform consumers of their rights concerning their data before it is collected.

Once the data has been collected, it must be safeguarded from unauthorized disclosure and theft. Businesses in the Internet dating and social networking and online social community industries are stewards of the personal and sensitive information of millions of users.

GDPR and CCPA are merely the beginning. As more states and countries adopt similar legislation, it is imperative for the industry to stay ahead of these mandates. It will be far too costly, in terms of statutory damages, customer mistrust, and brand identity, to fall behind.

[Courtland Brooks has brought this information together as an initial advisory. We are not lawyers. Please consult a lawyer.]

1 California Legislature. (2020). Retrieved from http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=