SEPTEMBER 2022

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

California Legislature Passes Bill Regulating Data Processing on Websites "Likely To Be Accessed by Children"

California's legislature overwhelmingly passed (with veto-proof majorities) the California Age-Appropriate Design Code Act (AB 2273) to—at least in theory—regulate companies' processing of children's personal information. In this client alert, we recap key provisions of the bill, identify potential hardships operationalizing it, and provide practical tips for getting a jump start on compliance.

If Governor Newsom signs AB 2273 into law (or the California legislature overrides his veto), companies will face significant restrictions and obligations if they provide an online service, product or feature (each of which we call a "Site") *likely* to be accessed by a child—a person under 18 years old. (This is much broader than the Children's Online Privacy Protection Act, which focuses on companies *targeting* those under *13* years old.) Starting on July 1, 2024, companies subject to the law will need to understand the age of their users, adopt measures to protect children's privacy, and restrict how children's data is used. The Attorney General has exclusive enforcement ability, and he can seek civil penalties of up to $2,500 per child for each negligent violation (which increases to $7,500 for intentional violations). There is a 90-day cure period for companies who are in *substantial compliance*, and that cure period does not sunset.

Scope

The bill applies to a business, as that term is defined in the California Consumer Privacy Act. Once that threshold is met, the critical inquiry is whether a Site is "likely to be accessed" by a

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Josh Hansen
Associate
303.285.5306
jahansen@shb.com

child. A company must make that determination by evaluating whether it is "reasonable to expect" child access based on whether the Site:

- Is directed to children per the Children's Online Privacy Protection Act;
- Is routinely accessed by a significant number of children (based on competent/reliable evidence);
- Has advertisements marketed to children;
- Has design elements known to be of interest to children (e.g., certain games or cartoons); or
- Has a significant amount of its audience composed of children, per internal research.

There is no materiality threshold—the bill applies if your site is reasonably likely to be accessed by *any* number of children.

Key Requirements & Prohibitions

Among other requirements, businesses must:

- **Know Your Audience.** Estimate the age of child users or apply the child protections to all users.
- **Provide Transparency.** Provide legal terms (such as policies and terms of use) using language suited to the age of children likely to access the Site and, when parents can monitor a child's activity, provide the child an obvious signal their activity is being monitored by a parent.
- **Establish Strong Privacy Settings.** Assign default privacy settings to offer a high level of privacy, unless the company can demonstrate why a different setting is in the best interests of the child.
- **Conduct Data Protection Impact Assessments.** Conduct data protection impact assessments (DPIAs) for each Site, including any additions or changes, and review those assessments every two years. (More details on this are below.)

Along with other restrictions, businesses cannot:

- **Engage in Harmful Processing.** Cannot use a child's personal information in a way the business knows or should know is materially detrimental to a child's health or wellbeing.
- **Conduct Profiling.** Cannot profile (e.g., automated processing to evaluate individual) a child by default unless there are appropriate safeguards and it is either necessary to provide the Site or there are compelling reasons in the child's best interests.
- **Collect Unnecessary Information.** Cannot process a child's personal information that is not necessary to provide to the Site, unless there is a compelling reason in the child's

best interests.

- **Use Dark Patterns.** Cannot use dark patterns to encourage the child to provide more information.

Data Protection Impact Assessments

Each DPIA must (1) identify the purpose of the Site; (2) explain how the Site uses children's personal information and (3) assess the risks of material detriment to the child. Relevant considerations include:

- **Design.** Could the design harm children; cause them to experience or be exploited by harmful contacts on the Site; or permit them to witness, participate in or be subject to harmful conduct?
- **Algorithms.** Could the algorithms harm children?
- **Advertising.** Could targeted advertising cause harm?
- **Addiction.** How, if at all, does the company use system design features to increase, sustain or extend use (e.g., automatic playing of media and rewards for time spent)?
- **Sensitivity.** How and why (if at all) is sensitive personal information on children processed?

As part of the assessment, the company must document the risks to children and create a plan to mitigate/eliminate the risk *before* releasing the Site. Companies must perform their DPIAs for existing services by July 1, 2024.

Practical Considerations & Challenges

The bill presents a variety of operational challenges.

- **Verification.** Companies will likely need to collect additional personal information to verify consumer ages because the bill requires estimating children's ages (which cannot be done without knowing everyone's ages) or treating all consumers as children (which is impractical).
- **Transparency.** Companies must write policies for the youngest likely visitor (even if they are an outlier) because the bill requires the policies be suited to the age of the likely visitors.
- **Privacy Settings.** Companies generally will need to review (and potentially strengthen) their default settings to ensure children are initially assigned a "high" privacy setting.
- **Data Protection Impact Assessments.** Companies will need to perform DPIAs for essentially every new, existing or

updated component of their Site because (1) a service, feature or product can be very granular and (2) the requirement to assess any element likely accessed by the children is not a material limitation.

- **Harm.** Companies will need to change their service if any child, arguably even just one, would suffer harm as a result of processing because the bill prohibits processing any child's personal information if the company knows or has reason to know it will cause a risk of harm to a child. (And this is to say nothing of the fact that the bill doesn't define "harm.")

Compliance Preparation

Businesses will at least need to assess the ages of their Site's users. And most will likely need to comply with the rest of the requirements because, as written, the law applies regardless of how many children are likely to visit your site—a couple may be enough. So we suggest the following steps to prepare:

- **Evaluate Ages.** Develop a mechanism to assess the age of users.
- **Consider Age Restrictions.** Evaluate the costs/benefits of excluding children from the Sites.
- **Assess Dark Patterns.** Assess whether dark patterns are used to solicit personal information.
- **Review Policies.** Read any public-facing policies (not just privacy statements) to ensure they are written in a manner children can understand.
- **Identify Necessary DPIAs.** Evaluate which Sites are most likely to be accessed by children and begin conducting DPIAs for each of them.
- **Evaluate Privacy Settings.** Review your default privacy settings and determine whether (1) they are "high" (whatever that means) or (2) you have a compelling reason to use a lesser default.
- **Processing.** Identify what children's information is used, why it is used, and how it is used.

The choice of a lawyer is an important decision and should not be based solely upon advertisements.