CLIENT ALERTS & INSIGHTS

New California Law Requires Enhanced Privacy By Default And Design For Users Under The Age of 18

SEPTEMBER 6, 2022

The bill, still awaiting likely signature from Gov. Newsom, will go into effect July 1, 2024 and apply to any business offering online services or products to children. The California Age-Appropriate Design Code Act recently passed both houses of the California legislature and is only a governor-signature away from imposing strict requirements on business that have online services, products, or sites that are targeted to children or that children are reasonably likely to access.

As a window into the intent of the bill, the bill states a legislative finding that businesses must consider the "best interests of children" when designing and developing websites, and that if a conflict arises between commercial interests and the best interests of children, the best interests of children prevail.

The new bill also sets forth some data protection requirements that are familiar to those businesses already subject to other data protection laws like the California Consumer Protection Act or the EU's General Data Protection Regulation. Those requirements include data protection impact assessments and data minimization.

Scope and Applicability

To analyze the full scope of the new bill, both the scope of what businesses are considered in-scope of the bills requirements and who is categorized as a child must be considered.

The bill does not provide a definition for what is considered an in-scope "business"; however, the scope of the requirements sweeps up any business that "provides an online service, product, or feature likely to be accessed by children." The bill includes some insight into what businesses could fall within this broad category.

According to the bill, the following types of businesses must comply with the bills requirements: any online service, product, or feature that (i) is directed at children; (ii) is routinely accessed by a significant number of children-based on competent and reliable evidence-or is substantially similar to such an online service; (iii) includes advertisements to children; (iv) is designed in a way to target children, including for example games, cartoons, music, etc.; or (v) has an audience significantly made up of children-as determined by internal company research.

This is a potentially broad category depending on how California authorities seek to interpret and enforce the law once in effect. Even if a business is not directly targeted at children or marketing to children, it could get swept up into the bill's requirements if it is "substantially similar to" an online service that is routinely accessed by a significant number of children.

The bill does have some expressed exemptions. Broadband internet service providers, telecommunication service providers, and deliveries of physical products, are all exempt from the bill's requirements.

Under the bill, a "child" or "children" is considered any consumer who is 18 years old or younger. This sweeps up a broader portion of the population than current data protection laws that govern the collection of children's personal information do.

For example, the U.S. Children's Online Privacy Protection Act considers anyone under the age of 13 to be a child and the California Consumer Privacy Act considers anyone under the age of 16 to be a child. The new bill expands on both and includes anyone who is 18 years old or younger.

Data Privacy Impact Assessment

Prior to making an online service, product, or feature available to the public (one that falls within the scope of "business" as described above), the business must conduct a Data Protection Impact Assessment ("**DPIA**").

Broadly, DPIA's must identify the purposes of their online service, product, or feature; how it uses children's personal information, and any identified risks.

Specifically, any DPIA must analyze the whether the online service, product, or feature could: (i) harm children or expose them to potentially harmful content (including its design); (ii) lead children to experience or be targeted by harmful or potentially harmful contacts; (iii) permit children to witness, participate in, or be subject to harmful or potentially harmful conduct; and (iv) allow children to be a party or exploited by harmful or potentially harmful contacts.

It is important to note that the above risks must be analyzed even when something could be "potentially harmful"; requiring companies to take a broad approach to the DPIA's risk analysis.

Additionally, the DPIA must consider whether: (i) algorithms used in the product, service, or feature could harm children; (ii) targeted advertising used in the product, service, or feature could harm children; (iii) the use of automatically playing media, rewards given for time spent on a service, and notifications can increase or sustain a child's use of the service; and (iv) the service, product, or feature collects or processes sensitive personal information of children.

At a high level, the DPIAs required under the new bill are not all that different from those required under the California Consumer Privacy Act, or that will be required under new state data protection laws. A business must analyze the purposes of their processing or activities and weigh them against the potential risks posed by such processing or activities. However, this bill sets forth specific categories of analysis that in-scope businesses must conduct-which sets it apart from other laws.

The DPIA is a prerequisite to any in-scope online service, product, and feature as businesses are prohibited from implementing such online products, services, or features without first conducting a DPIA. All Data Protection Impact Assessments required under the bill must be reviewed every other year after they are initially conducted.

Government Requests

Related to the DPIA, there are certain timing requirements that must be met when the California State Attorney General makes requests.

A business must, within 3 business days of a written request from the Attorney General, provide the Attorney General with a list of all DPIAs the business has conducted; and within 5 business days of a specific request, make any specific DPIA available to the Attorney General.

Affirmative Obligations

The bill also requires a set of affirmative obligations on in-scope businesses, all related to the principle of data minimization and privacy by designed and default.

1. All privacy settings for children users must be configured, by default to the highest level of privacy offered, unless the business can demonstrate an overriding interest (i.e., best interest of the child).
2. Privacy policies, terms of use, and other policies must be clearly and prominently posted on the site using language that is suited for the average age of those children accessing the service, product, or feature.
3. Prominent (i.e., clear and conspicuous) tools must be made available to help children exercise any applicable privacy rights.

Prohibitions

The bill also sets forth a number of prohibitions, restricting the activities and data processing of in-scope businesses. In-scope businesses are prohibited from:

1. Using a child's personal information in a manner the business knows or has reason to know is materially detrimental to the physical or mental health, or general well-being of the child;
2. Profiling a child unless the business can demonstrate (i) appropriate safeguards are in place; and (ii) either that the profiling is necessary and requested by the user or that the profiling is in the best interest of the child;
3. Collecting, selling, sharing, or retaining a child's personal information beyond what is absolutely necessary;
4. Using a child's personal information beyond the purposes it was originally collected for;
5. Collecting a child's precise geolocation information without providing an obvious sign to the child for the duration of the collection of that geolocation information; and
6. Using dark patterns (e.g., misleading designs, consents, automatic renewals, etc.).

The practical reality of these obligations and prohibitions is that any business that is or might be in the bills scope likely needs to set up some form of "age assurance" process to know what users are considered children, whether they make up a significant amount of the online services traffic, and how to ensure policies and procedures are in place to comply with the above obligations and restrictions.

But even age assurance procedures are limiting in the bill as business are prohibited from using any personal information collected for age assurance purposes for any subsequent purposes.

Penalties and Enforcement

The bills, once signed by Gov. Newsom and in effect, will be enforced by the California State Attorney General. There is no private right of action expressed in the bill that would allow consumers to sue for violations.

Any business that violates the bill can be subject to (i) an injunction; (ii) $2,500 fines per affected child for each negligent violation; or (iii) $7,500 fines per affected child for each intentional violation. The foregoing fines are the same totals of the per-violation fines for violations of the California Consumer Privacy Act.

Business with large volumes of traffic consisting of children (e.g., social media companies) could potentially face massive fines under the bill if found in violation.

As new laws and regulations come into effect that require enhanced data protection standards or defaults, including those related to the online activities of children, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.