Articles + Publications | September 23, 2021

New UK Standards for Children's Digital Services Take Effect — Provides Framework for New US Law

WRITTEN BY

Molly S. DiRago | Timothy A. Butler | Ronald Raether, Jr. | Ashley L. Taylor, Jr.

Earlier this month, the U.K.'s Age-Appropriate Design Code (referred to as the "Children's Code") took effect. The Children's Code is not a law per se, but rather a set of 15 flexible standards that apply to online services, such as apps, online games, and web and social media sites, likely to be accessed by children in the U.K. The Children's Code is meant to assist businesses in creating and maintaining age-appropriate services and fairly processing children's data consistent with the GDPR.

U.S. lawmakers have urged online businesses, such as Epic Games, Microsoft, Walt Disney, and Nintendo, to comply with the Children's Code within the United States. Rep. Kathy Castor recently introduced an updated Protecting the Information of Our Vulnerable Children and Youth Act (the Kids PRIVCY Act), which incorporates key elements of the Children's Code to amend the Children's Online Privacy Protection Act (COPPA). Notably, the Kids PRIVCY Act creates a protected class of teenagers beyond COPPA's application (*i.e.*, children ages 13-17) and applies to all sites "likely to be accessed by children and teens," not just "child-directed" services. If enacted, the Kids PRIVCY Act would also repeal safe-harbor regulations allowing for industry self-regulation.

The 15 standards established by the U.K. Children's Code are as follows:

1. Best Interests of the Child. Organizations must consider the needs of child users. While there is no "one-size fits all" when determining the best interests of a child, the Children's Code cautions that "[i]t is unlikely … that the commercial interests of an organisation will outweigh a child's right to privacy."

2. Data Protection Impact Assessments (DPIA). A DPIA — a defined process to help identify and minimize data security risks to children — should be embedded into the design of a particular digital service. An organization's DPIA should be "flexible and scalable," and it is good practice to publish it.

3. Age-Appropriate Application. Organizations must consider the different needs of children at different ages and stages of development. This also requires organizations to establish the age of a user through methods deemed fit by the organization for their particular service, including third-party age verification services, self-declaration, or artificial intelligence.

4. Transparency. Information provided to users must be concise, clear, prominent, and presented in a child-friendly way, taking the child's age into account. Such information should be delivered in "bite-sized"

explanations at the point at which use of personal data is activated.

5. Detrimental Use of Data. This requires that organizations do not use children's personal data in ways shown to be detrimental to their wellbeing or that go against industry codes of practice, other regulatory provisions, or government advice.

6. Policies and Community Standards. Published terms, policies, and community standards must be adhered to.

7. Default Settings. Default settings must be set to "high privacy" because many children just accept whatever default settings are provided. It is not enough to merely allow children to activate high privacy settings.

8. Data Minimization. Organizations must collect and retain only the minimum amount of personal data needed to provide the service in which a child is actively and knowingly engaged. This also requires that children are given separate choices over which service elements they wish to activate.

9. Data Sharing. Under this standard, children's data cannot be disclosed unless there is a compelling reason to do so, taking into account the best interests of the child. "Disclosure" can include sharing data between different parts of one organization.

10. Geolocation. Geolocation options must be turned off by default. There must be an obvious sign when location tracking is active and should be switched back to the default (*i.e.*, off) at the end of each session.

11. Parental Controls. Children must be provided with age-appropriate information about parental monitoring. If the online service allows parents to monitor their child's online activity or track their location, the service must provide an obvious sign to the child when he/she is being monitored.

12. Profiling. Profiling must be turned off by default and permitted only when appropriate measures are in place to protect the child from any harmful effects (in particular, being fed content detrimental to his/her health or wellbeing).

13. Nudge Techniques. Organizations should not use "nudge techniques" to lead or encourage children to provide unnecessary personal data or turn off privacy protections. Nudge techniques are design features that lead or encourage users to follow the designer's preferred paths in the user's decision making. Below find two examples set forth in the Children's Code:

14. Connected Toys and Devices. Children's toys and other devices connected to the internet must adhere to the Children's Code. The Children's Code does not apply to devices that collect personal data, but only store it within the device itself.

15. Online Tools. Organizations must provide "prominent and accessible tools" to help children exercise their

data protection rights and report concerns simply and easily.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber