

Protection of Children's Personal Data

23 Apr 2021

Children, due to their limited life experience and propensity for risk taking relative to adults, are generally considered particularly vulnerable to online personal data intrusions and theft. Data from the National Center for Education Statistics of the United States indicate that 94% of US children between the ages of 3 and 18 have regular internet access: 88% via a home computer and 6% via smartphone^[1]

Children are generally considered legally incompetent and without power alone to enter into binding agreements. However, under certain circumstances and with the consent of a parent or adult guardian a child may do so.

In light of the innate vulnerability of children, the trade in their data is ethically troubling to say the least. The United Nations International Children's Emergency Fund ("**UNICEF**") has addressed the issue of child privacy in the UNICEF Papers^[2] which spotlighted the divergent interests of children and business when it comes to data privacy. Indeed, children represent a large chunk of the online marketplace and their personal data is a valuable, marketable asset of particular interest to advertisers in placing targeted online ads directed at children.

Apart from this in the legal sphere, there is the Children's Online Privacy Protection Act of 1998 ("**COPPA**"), which is a pioneering regulation in United States ("**US**"), and the General Data Protection Regulation ("**GDPR**"), which regulates children's personal data in European Union ("**EU**").

It is beyond dispute that children and their privacy - including data privacy - must be protected. As technology continues its rapid advance, governments around the world struggle to enact effective privacy protection legislation in a veritable cat-and-mouse game. With respect to children's data privacy and protection, ethical and normative concerns compete with massive business interests. On all fronts, strict compliance with applicable law is a must. Accordingly, this article will lay down the international conjecture and discuss Turkey's current situation regarding privacy of children.

United States

COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age; and makes it unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates COPPA.

Under COPPA operators must:

- (a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information,
- (b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children,
- (c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance,
- (d) Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and
- (e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

In December 2018, the United States Department of Justice agreed to settle COPPA violation charges against Oath - *the ad-tech parent of AOL and Yahoo and a division of Verizon Communications, Inc.*; with Oath paying a record fine of \$5M. YouTube and Google are currently under investigation by the U.S. Department of Justice for COPPA violations.

In response to an increasingly strict regulatory environment, some online providers now incorporate express parental consent for use of services by and collection of data on children, or, as Google now does, prohibit personalized ads directed at and the collection of personal data on children.

European Union

COPPA has no analogue amongst EU directives. However, the GDPR, though it lacks COPPA's age specification, recognizes children as vulnerable and in need of specific protections; and Member States, except for the few that implement COPPA's age provision, generally consider 16 years as the age of adulthood. Some of the EU countries determined the age limit as 13, as similar to the US, but this is not the general principle.

Recital 38 of the GDPR states:

"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."

Notably under GDPR, where express parental consent to processing a child's personal data is lacking, a data controller must demonstrate that reasonable efforts were made to obtain it.

In September 2020, the Data Protection Commission of the Republic of Ireland (**"DPC"**) initiated investigations of Facebook and its subsidiary Instagram in connection with child data processing in violation of GDPR. The DPC is looking into whether Facebook has a legal basis for processing of children's personal data and, if it does, whether it implements adequate measures to protect children using Instagram; whether Facebook meets transparency requirements; and whether Instagram profile and account settings adequately protect children.

Turkey

Like the EU, Turkey has no statutory analogue to America's COPPA. However, Turkey's Data Protection Law ("**DP Law**"), enacted in April 2016, is substantially similar to EU Directive 95/46/EC which predates and is superseded by the GDPR. Personal data of adults and children are protected equally by the DP Law though it contains no specific definition of a child.

The DP Law requires, subject to certain exceptions, express consent of a data subject before personal data may be processed.

Turkish law does not specifically define a child. Article 11 of the Turkish Civil Code numbered 4721 ("**TCC**"), however, defines an adult as a person 18 years of age or older, or as otherwise provided under applicable law or adjudication. Similarly, the United Nations Convention on the Rights of the Child defines a child as everyone under 18 unless "*under the law applicable to the child, adulthood is attained earlier.*"

Under Turkish Law, Children are generally considered legally incompetent and without power alone enter into binding agreements. However, under certain circumstances and with the consent of a parent or adult guardian a child can enter into a legal binding agreement.^[3]

Certain TCC provisions, however, provide that a mentally competent child - itself an opaque term - may, in exercising strictly bound rights, legally bind themselves without guardian consent. Under Turkish law, strictly bound rights are those so intertwined with one's person that they are considered integral and neither transferrable nor exercisable by third parties - e.g., the right to marry, divorce, change one's name^[4] This of course begs the question of whether the right to data privacy and protection is strictly bound.

In a decision dated 11.08.2020, and numbered 2020/622, Turkey's Personal Data Protection Board ("**Board**") appears to have recognized as strictly bound the right to privacy when it stated therein that "*personal rights are rights that a person has on his tangible and emotional self and economic integrity and privacy.*" However, in the same decision the Board went on to state that the right to privacy - inclusive of data privacy ostensibly - is not absolutely strictly bound and a guardian may seek independently to protect a child's privacy rights^[5]

Following the only decision to date made by the Board on children and attributed above, the Board recently published guidelines which include some limited recommendations on processing children's personal data including data minimization, stricter compliance with the DP Law, implementation of reliable age confirmation measures and child-appropriate privacy notices. These guidelines published by the Board are similar in content to COPPA.

According to the Human Rights Action Plan published in March 2021, the DP Law will be brought into line with EU standards and the GDPR within two years at the latest. Therefore, it is expected to have a data privacy regulatory framework regarding children's data in Turkey, soon.

[1] https://nces.ed.gov/programs/coe/indicator_cch.asp

[2] https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

[https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression\(1\).pdf](https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf)

[3] <https://hukuk.deu.edu.tr/wp-content/uploads/2019/09/CANAN-ERDOGAN.pdf>

[4] <https://www.kvkk.gov.tr/Icerik/6816/2020-622>

[5] <https://www.kvkk.gov.tr/Icerik/6816/2020-622>

Related Practices

- [Privacy and Data Protection](#)