



WHAT YOU SHOULD KNOW

- Through our increasing use of phones, devices, websites, apps and smart products, we are constantly creating data that reveals information about our lives.
- This data can reveal our location, who we are friends with, our sexual orientation, our political beliefs and the state of our health. It can also include biometric data, such as our fingerprints or the sound of our voice.
- This data is valuable to companies and governments who want to have a greater understanding of their customers or citizens.
- The data economy has given a small number of tech companies tremendous power and influence over our right to privacy.
- Complex privacy policies make it hard for individuals to understand how their privacy can be undermined.

Children and Online Privacy

Digital technology has changed the nature of privacy. This briefing outlines the key threats to children's privacy, the companies who influence it and UNICEF's view on what needs to be done.

Key drivers

- The global proliferation of digital devices: It is estimated that by 2020, there will be 24 billion connected devices.¹ These include smart household products, which are referred to collectively as the Internet of Things, and provide even more opportunities to gather our data.
- The birth of the data economy, dominated by a small number of tech companies: In 2015, it was estimated that the EU data economy alone was worth more than €285 billion.²

Key players

- Parents and schools who have created a demand for products that monitor children's online activity,

ostensibly to protect them from harmful content or threats such as cyber bullying.

- Companies who want to profit from the data they collect – for example by selling it or by analyzing it so they can understand how to market to their customers better.
- Companies, such as telecoms companies, who may be asked to provide data to governments.
- Actors in the advertising industry, who see children as a powerful consumer group: they are both the targets of marketing as well as influencers over their parents' buying choices.

¹ Business Insider Intelligence, 'There will be 24 billion IoT devices installed on Earth by 2020', United States, <www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-57r=US&IR=T>, accessed 04 March 2019.

² European Commission, 'Final results of the European Data Market study measuring the size and trends of the EU data economy', European Commission, Brussels, <<https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy>>, accessed 04 March 2019.

The Relevance for Children

Children's rights that are affected include:

■ Right to privacy and protection of personal information

- The collection, analysis and profiling of children's data can undermine children's rights to privacy and the protection of their personal information. These rights are also undermined by technologies that track, monitor and broadcast their Internet use.

■ Right to not be subjected to attacks on reputation

- When children's privacy is violated, it can affect their future. This right can be undermined by the publishing of information about them without their consent or a lack of mechanisms that enable children to control the data about them.

■ Rights should be protected in accordance with evolved capacities

- Privacy policies can be complex and children and parents may not understand what they are signing up to.

Opportunities for Positive Change

■ Responsible design of online goods and services

- Children's privacy is considered in the design of websites, platforms, products, services and applications designed for, targeted at or used by children.

■ Clear mechanisms for informed consent

- Consent mechanisms are designed in a way that parents and children can understand and provide their free and informed consent for the processing of their data. These should reflect the evolving capacities of children as they grow and develop.

■ Opportunities for redress when rights are violated

- Children and parents understand that children have rights and they are entitled to be able to address them if they are violated.

■ Responsible processing of data

- Children's data are processed in a manner that is fair, lawful and transparent, and compatible with the purpose for which the data were obtained. Where there are variations in regulations, companies should choose best practice options.

Integrate Children's Rights Into Corporate Policies and Practices

Some of the core ways that companies undermine children's privacy include:

- the collection of data, for example, in exchange for access to games, goods or services;
- the analysis and sale of children's browsing data;
- the collection of biometric data, for example, fingerprints or voice recordings;
- age verification techniques that can profile children;
- government surveillance that requires companies to share intrusive data; and
- parental controls that monitor children's Internet use.

UNICEF has developed five principles that companies should incorporate into their operations to protect children's rights:

- Children have the right to privacy and the protection of their personal data.
- Children have the right to freedom of expression and access to information from a diversity of sources.
- Children have the right not to be subjected to attacks on their reputation.
- Children's privacy and freedom of expression should be protected and respected in accordance with their evolving capacities.
- Children have the right to access remedies for violations and abuses of their rights to privacy and free expression, and for attacks on their reputation.

What UNICEF Is Doing

UNICEF believes that companies have a responsibility to protect children's right to privacy. We encourage companies across the tech and ICT sectors, as

well as those who provide goods and services to children, to make practical changes to their operations and ensure that children's rights are protected.

UNICEF is creating and advocating guidance that:

- integrates children's rights in corporate policies and the design and delivery of services;
- empowers companies to go beyond minimal legal compliance to best practice for data collection, processing and sharing;
- encourages children to be educated, informed and empowered to protect their personal data.

UNICEF RESOURCES FOR POLICYMAKERS

Privacy, Protection of Personal Information and Reputation

→ DISCUSSION PAPER MARCH 2017

- Identifies children's right to privacy under international law and the core online behaviours that threaten them.
- Identifies the responsibilities of the tech and ICT sector and the role that governments can play.

Children's Online Privacy and Freedom of Expression

→ INDUSTRY TOOLKIT MAY 2018

- Created for a wide range of companies across the digital environment, for example, telecoms providers, online platforms and the manufacturers of devices and smart products.
- Can be used by any company that collects, analyses or sells data or whose business affects the content that children can see.
- Identifies five principles that companies should adhere to and a checklist of recommendations that ground and shape decisions about children's online privacy.