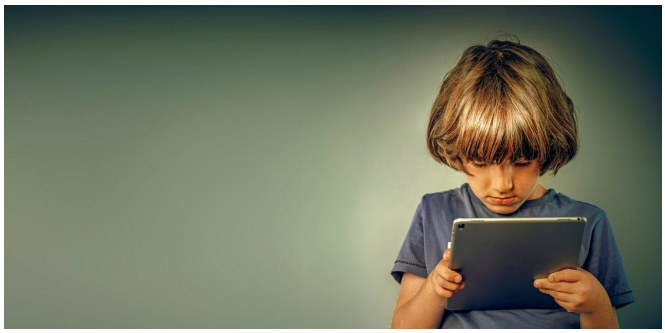
We street-proof our kids. Why aren't we data-proofing them?

30 September 2019, by Siobhan O'flynn



It's time to start data-proofing our children. Credit: Shutterstock

Google recently agreed to pay a US$170 million fine for illegally gathering children's personal data on YouTube without parental consent, which is a violation under the Children's Online Privacy Protection Act (COPPA).

The United States Federal Trade Commission and the New York State Attorney General—who together brought the case against Google—now require YouTube to obtain consent from parents before collecting or sharing personal information. In addition, creators of child-directed content must self-identify to restrict the delivery of targeted ads.

The $170 million fine is a pittance given Alphabet Inc.'s (Google's holding company) valuation of more than US$700 billion.

Our digital identities comprise data collected across our activities, making personal or identifying information irrelevant. Children today are subjugated to a scale of data collection and targeting that we cannot fathom. Right now, we also have no clue about the consequences, and regulatory protections to data-proof their futures are far from certain.

My ongoing research on how big tech and media conglomerates are using dark pattern design to bypass privacy regulations protecting personal information has revealed how vulnerable children are to data collection and how Canada's legislation in particular is failing them.

Incomprehensible scale

For adults and children, Google has access to everything from search queries to online purchases to any app and website associated with Gmail accounts - including deleted accounts - or linked via cross-browser finger-printing.

As a parent, you create a network of cross-connections when you input information to make purchases for your child online or set up accounts for your child on apps and websites. Added to this is all your child's activity on YouTube and YouTube Kids, search data to clicks on recommended videos to rewinds and duration of play time.

Then add cross-browser fingerprinting and most recently, Google's "GDPR workaround," secret buried web tracking pages that act as pseudonymous markers that track user activity across the web.

This latter violation of data privacy was revealed in a complaint to the Irish Data Protection Commission filed the same day Google's fine was made public.

We are talking about vast fields of data, the scale of which is difficult to comprehend; this data is used to feed Google's artificial intelligence recommendation algorithms that now steer everything from employment application processes to dating apps.

Children in the United States and Canada have another significant, persistent arena where information is being produced by them and collected by Google. Google entered the

educational sphere in 2012, and now dominates educational technology market in the U.S., giving Google unprecedented parent-sanctioned access to children's data through kindergarten to Grade 12.

Dominance in the educational sphere

Alphabet Inc. dominates child-directed and child-featured content online through YouTube Kids and has now colonized online educational spaces through Google Docs, G-Suite, Chromebooks and the associated Gmail accounts for children that are required for use.

This means that Google's access to children's data spans entertainment (YouTube and YouTube Kids), search and purchase histories (via associated parental accounts), and educational sectors.

The uptake numbers in the educational technology sphere are staggering. Between 2012 and 2016, Google Chromebooks went from less than one percent of the U.S. school market to over 50 percent —more than 30 million Chromebooks are currently being used in American classrooms.

By 2017, more than 58 percent of devices purchased for U.S. schools were Google devices; more than 80 million instructors and children use them globally.

Given Google's history of privacy violations, it's no surprise that Google's rollout of Chromebooks again violated children's data privacy. Initially, Google resisted complying with the federal Family Educational Rights and Privacy Act (FERPA), providing links to its security policies, which FERPA rejected.

In 2015, the Electronic Frontier Foundation (EFF) filed an FTC complaint because Chromebook default settings initially allowed Google to collect user data including "Web browsing histories, search-engine results, YouTube viewing habits and saved passwords."

Harry Brignull, a user experience specialist, coined the term "dark pattern" to describe a "user interface that has been carefully crafted to trick users into doing things, such as buying insurance with their purchase or signing up for recurring bills."

Gmail accounts for children remain a standard practice in schools today. Standard practice continues to be that children are enrolled by schools en masse into Gmail accounts, often without parental consent, using their full names, and "into other services that collect data without any notification." This data collection is presented as benign, optimizing your child's experience, enriching education, democratizing access to 21st century online resources.

Updating the laws

What Google has done is create a dynamic, adaptive system of data collection that has already colonized our children's futures, given what we now know of how ad targeting can manipulate behaviour . We have no way of knowing how this depth of data collection may be used in years to come.

In March 2019, U.S. senators Ed Markey and Josh Hawley introduced a bipartisan bill to update COPPA, banning targeting ads to children, extending privacy protections to 13- to 15-year-olds so data cannot be collected without user permission and an "eraser button" that would allow parents and kids to delete personal information.

This proposed update to COPPA is crucial legislation that Canadians should be studying—in addition to the European Union's General Data Protection Regulation - as again, there are multiple documented instances of Alphabet's subsidiaries failing to protect children's privacy.

This legislation, if passed, would have enormous impact on the revenue of the digital ad market for Google and Facebook, as digital ad revenue in the U.S. totaled $107 billion in 2018 We should anticipate sustained resistance from Alphabet's subsidiary companies and the other major platforms.

A focus on how we can ensure the consistent protection of the data privacy of children and youth must be central to our discussions of technology globally and to Justin Trudeau's proposed Digital Charter nationally in Canada.