Young people are the most surveilled and tracked generation ever. Their personal information, activities, hobbies, and networks are exposed — and often for sale — from birth, enabling companies and others to form detailed dossiers that can determine children's futures and extend beyond parents’ and kids’ control.

Why are kids particularly at risk?
While access to powerful technology from birth gives kids access to new opportunities, it also means that devices at home, at school, and everywhere in between collect information about them constantly. As kids’ brains are still developing, they lag behind adults in conceptualizing privacy, comprehending online data ecosystems, understanding terms of service, and distinguishing between ads and other content.

- **AT HOME** Kids are early adopters of new technology, including cheap, insecure apps and IoT devices that lack security updates and protective features. This vulnerability is passed on to parents when home networks are exposed.

- **IN SCHOOL** Kids must go online, often on school devices and networks, to receive an education. Resource-constrained schools have limited ability to vet products and services that collect highly sensitive educational information.

- **IN OUR COMMUNITIES:** Kids' online activity is largely on mobile devices, meaning their location, activities, and conversations are tracked. And with an increase in community cameras, bluetooth trackers, and other sensors, kids are watched wherever they go.

What do families want? ¹

- **More than 9 in 10** parents and teens think it’s important that websites clearly label what data they collect and how it will be used.

- **97% of parents and 93% of teens** think it’s important that sites ask permission before selling or sharing data.

- **82% of parents and 68% of teens** are concerned about how social networking sites use their data to allow advertisers to target them with ads.

In a recent survey of 1000 U.S. parents, **98%** were concerned about their kids’ digital privacy. And this was despite many lacking awareness about how companies could commercially exploit children’s information or target them with advertisements.²

---

¹ Privacy Matters: Protecting Digital Privacy for Parents and Kids (June 2018)
² https://www.startpage.com/privacy-please/privacy-awareness/2020-parents-privacy-survey-startpage. 36% did not know companies could "exploit their children's data for commercial gain" and 33% did not know companies could "use their children's digital footprint to target inappropriate ads."
What should Congress and the FTC do to protect kids’ privacy?

Pass a comprehensive privacy law that provides a strong floor.
- With some protections for everyone, inadvertent gaps in kid-specific laws will be less problematic, ensuring some coverage wherever children and teens are.
- The law should be stronger than current state laws, encourage data minimization, and enable meaningful enforcement. The onus should be on companies to protect individuals.

Update COPPA to protect teens and better protect children.
The CPRA and the GDPR already offer additional protections for teenagers, as do recent child-specific rules like the UK’s Age Appropriate Design Code and Ireland’s proposed guidance on a child-oriented approach to data processing. Teens are specifically vulnerable, as their brains are still developing and they are more likely to engage in risky behavior. Further, teens’ apps have been shown to seek more data from users and contain more third party trackers.

- Congress should pass a strong children’s privacy law that:
  ➔ does not let sites and apps turn a blind eye to young people using their services.
  ➔ empowers teens to make decisions for themselves, recognizes their developing autonomy, and requires companies use age-appropriate controls and language.
  ➔ offers special protections to young children, such as prohibiting behavioral marketing.
  ➔ broadly defines personal information to ensure all personal information is protected.
  ➔ beefs up enforcement, ideally through a private right of action and/or also a better-resourced FTC.

Overhaul student privacy laws, including FERPA, to reflect 21st century learning and data practices.
As more learning takes place online and more sensitive information is collected—ranging from students’ homes to health information—it is critical that student privacy laws keep pace.

- Congress should update FERPA to ensure:
  ➔ Protected educational records should include online data created by students such as web browsing, searching, and other online activity.
  ➔ The law must close outdated directory information loopholes, narrowing the definition, making sharing opt-in, and giving parents more granular choices as to which third parties they wish to share directory information with.
- Congress must also pass legislation that holds companies directly accountable for students’ personal information. E.g., companies must be prohibited from using students’ personal information for profit.
- More money is needed for trained privacy and data security professionals in schools.

Ensure that federal privacy regulators understand the children’s tech market and are resourced to robustly enforce COPPA.
- Tech companies hide problematic practices behind trade secrets and opaque algorithms and models that are hard for the public to understand. Some seek to punish third party researchers who attempt to collect this information. And the FTC has acknowledged budget shortfalls that limit its work.
- Congress should fund the FTC to hire staff equipped to take on big tech. For equivalent staffing to European privacy regulators -- average of 5 staff per 1 million -- the FTC would need ~1600 staffers for a population of 320 million.
- Congress should encourage the FTC’s 6(b) platform study, require regular briefings and updates during the study, and encourage the FTC to look at the ed tech market with ED.
- Congress should enhance the FTC’s enforcement powers to ensure it can meaningfully punish bad actors.

Questions? Contact Amina Fazlullah: afazlullah@commonsense.org or Danny Weiss: dweiss@commonsense.org.