common sense®

# PRIVACY RISKS AND HARMS

## The Common Sense Privacy Program

Common Sense is the nation's leading nonprofit organization dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in the 21st century.

common sense®

www.commonsense.org

# INTRODUCTION

The Common Sense *Privacy Risks and Harms* report identifies risks to children and students as they engage online and identifies ways for parents and educators to choose the products that best protect our youngest consumers from privacy intrusions and manipulation by third parties that could have long-term implications.

These decisions by parents and educators on which products to use at home and in the classroom need to be guided by resources backed by research and experts with informed analysis of the risks. Our easy-to-understand privacy evaluations from Common Sense include an overall score, display tier risks, and summarize privacy concerns to guide parents and educators in making informed choices. Information and communication technologies offer tremendous benefits to children, especially the most disadvantaged, but parents and educators need to be able to harness the power of the technology while at the same time limiting the harms in order to protect children. As parents, educators, and consumers, our main leverage in encouraging companies to make changes in how they collect and use personal information from kids is in our purchasing decisions, by us only buying products for kids that protect their privacy and avoiding products that do not.

Privacy has meant many things over time, but in the digital age the stakes are high, and the issue raises important questions about what personal information is collected from kids by the applications and services they use every day, how that information is used, and with whom it's shared and why. The understanding of the implications vary, and the choices we make for our children now can have ripple effects for decades to come. Many parents and educators say they are not concerned about the right to privacy and believe there are no real privacy risks or harms because they think their children and students have nothing to hide.

However, the choices kids make (and those their parents make on their behalf) with personal information are ultimately choices that define their online identities and profiles. When it comes to privacy, different people face different kinds of privacy risks and harms. Kids are especially susceptible to behavioral, social, emotional, physical, and financial risks that could create lifelong social and emotional harm. For example, when students take college entrance exams such as the PSAT, the ACT, or Advanced Placement exams, they are often asked to check off a box if they want to receive information from colleges or scholarship organizations. That simple act of checking a box to share a kid's personal information and their exam grades with third parties can be given without parental notice or consent and introduces privacy risks. Organizations like the College Board and ACT could use a student's personal information to create and market personal profiles to third parties. A student's personal information could also be combined with their online digital footprint to create detailed profiles that may be used by college admissions offices to determine acceptance based on statistical analysis of their data that takes into consideration the student's sex, race, and behavior on social media accounts.

With this report, we collect the best available information about ways consumers can arm themselves with information when choosing which technology tools to use. There is no one-size-fits-all solution for privacy, and so parents and teachers need to educate themselves with resources like ours and those offered by other trusted sources in order to best understand how to minimize the risk of harms to our youngest consumers based on the personal information collected from them, who has access to it, and how it is used.

The Common Sense Privacy Program

Common Sense is grateful for the generous support and underwriting that funded this report from the Michael and Susan Dell Foundation, the Bill and Melinda Gates Foundation, and the Chan Zuckerberg Initative.

## CREDITS

| | |
|---|---|
| Authors: | Girard Kelly<br>Jeff Graham<br>Jill Bronfman<br>Steve Garton |
| Suggested citation: | Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2019). *Privacy risks and harms*.<br>San Francisco, CA: Common Sense Media |

# TABLE OF CONTENTS

# PRIVACY RISKS

## What are the risks?

As applications and services collect more and more personal and behavioral information about children at home and students in an educational setting, it is imperative that the privacy of that information be protected from a wide range of potential risks. To begin with, information must be protected from potential misuse by third parties and from a data breach. However, kids also face unique privacy risks when trying to determine which applications and services are safer to use with countless websites and app store products all seeking their attention.

Companies often offer attractive free or low-cost apps with deceptive in-app purchases that are specifically targeted toward kids. These apps often have worse privacy practices—for the purposes of our evaluation process—because they use the information they collect, or the information of the parents, to engage in third-party marketing, advertising, and tracking technologies that could use the collected personal information to profile and target kids—as well as their parents and teachers—with advertisements outside of the product (Kelly, Graham, & Fitzgerald, 2018). These contextual or targeted advertisements may also influence kids across their devices and the internet over time. The type of risks that kids face depends on the type of personal information collected and for what purposes that information is used to cause intentional or unintentional harm.

> **“Research shows that children under the age of eight are unable to critically comprehend televised advertising messages and are prone to accept advertiser messages as truthful, accurate and unbiased” (American Psychological Association, 2004).**

Collection of personal information for the purposes of exerting influence over kids is an inherently deceptive process where kids learn at a young age about the principles of surveillance capitalism and that their information and its meaning has monetary value that can be exploited by others and exchanged for power (Christl, 2017; Zuboff, 2016; Zuboff, 2015). These advertising messages are intended to coerce kids into making choices they would not otherwise make. The choices that kids make in response to advertising-related messages may not always be in their best interests because advertising messages are designed to exploit kids' susceptibility and could be destructive to a kid's developing state of mental health. Advertising messages also serve to exploit kids' vulnerability in critical thinking because they are not always able to discern the difference between messages meant to convey truthful, accurate, and unbiased information and messages meant to influence and change their behavior (American Psychological Association, 2004; Nyst, 2017, pp. 8–9). Ultimately, these messages could distort kids' perception of reality, which could have negative consequences on their mental health and might affect their self-control and rational decision-making processes.

> **“There are also clear gaps in children's knowledge about risks online, and despite rapidly increasing usage among children and adolescents, many lack digital skills and the critical ability to gauge the safety and credibility of content and relationships they experience online” (Nyst, 2017, p. 9).**

The following examples illustrate some of the different types of behavioral, social, emotional, physical, and financial risks that can occur from the misuse or inadvertent disclosure of a child, student, parent, or educator's personal information:

- Behavioral risks include modified personality changes such as negative attitude, early or increased use of alcohol, parent-child conflict, loss of appetite or interests, inconsistent preferences or beliefs, attention deficits, sudden changes to characteristics, extreme opinions, irrational intentions, abandonment of established habits, and verbal cyberbullying or abuse of others (Livingstone, Mascheroni, & Staksrud, 2015).
- Social risks include modified professional or educational changes such as loss of employment, damage to reputation, social or emotional learning problems, poor learning outcomes at school, disciplinary actions, expulsion, criminal or civil charges, self-destructive relationships, running away, and separation from family or friends (Livingstone et al., 2015).
- Emotional risks include modified mental health changes such as negative body image, substance abuse, sexual deviance, anxiety, depression, low self-esteem, addiction, avoidance, isolation, aggression, and lack of empathy for others (Grabe, Ward, & Hyde, 2008).
- Physical risks include modified decision-making processes such as eating disorders, acts of verbal or physical violence toward family or friends, sexual assault, reckless endangerment, manslaughter, or self-harm such as cutting or suicide (Graafland, 2018).
- Financial risks include modified economic consumption changes such as impulsive in-app purchases, unexpected online purchases or gifts, extortion, credit fraud,

> large withdrawals, large purchases on credit, applications for more credit, maxed-out credit limits, loss of income, taking high-interest loans, theft from family or friends, sales of family or sentimental items, patterns of borrowing to make payments, food and housing insecurity, and unhealthy spending habits (Meyer, Adkins, & Yuan, 2019, January).

## Who is vulnerable to the risks?

Knowledge gaps of the risks are not surprising. Companies inform people incompletely, inaccurately, or not at all about their data practices with ambiguous, misleading, and often obfuscating language in their user interfaces and policies such as their privacy policies and terms of service. When assessing vulnerabilities of kids, it is important to take into account children's own attitudes about online risks—which often differ considerably from those of adults. Although there is a lack of research on some of the most marginalized communities and groups, Burton, as cited in Unicef (2017, p. 81), provided existing evidence that indicates "children who are most vulnerable to online harms include girls, children from poor households, children in communities with a limited understanding of different forms of sexual abuse and exploitation of children, children who are out of school, children with disabilities, children who suffer depression or mental health problems and children from marginalized groups."

> **"Digital technology and interactivity also pose significant risks to children's safety, privacy and well-being, magnifying threats and harms that many children already face offline and making already-vulnerable children even more vulnerable" (Unicef, 2017, p. 8).**

Also, how much children benefit from digital experiences has much to do with their starting points and opportunities in life. Research indicates "while those with strong social and familial relationships are likely to use the internet to bolster these relationships—leading to improved well-being—children experiencing loneliness, stress, depression or problems at home, for example, may find that the internet compounds some of these existing difficulties. Conversely, children who struggle with their social lives offline can sometimes develop friendships and receive social support online that they are not receiving elsewhere" (McKenna, Green, & Gleason, 2002, p. 9). These examples are not limited to kids—consider all the ways that marketers might be able to identify when parents break off a relationship, experience a significant health concern, start a new job, lose a job, or go through other events that create a habit-flexible, vulnerable moment that companies can exploit for their financial gain (Crain & Nadler, 2017).

For example, research from the American Medical Association (AMA) has found that most free apps designed to help people quit smoking or cope with depression share data with third parties for advertising purposes (Huckvale, Torous, & Larsen, 2019). Research indicates "behavioral science also suggests your mood, energy levels, and alertness can affect decision-making and biases in predictable ways. According to leaked internal documents, Facebook claims it can identify its teenage users' emotional states to give advertisers the means to reach those who feel 'insecure,' 'anxious,' or 'worthless.' Presumably the point is to pinpoint the exact moment a sales message is most likely to hit home" (Crain & Nadler, 2017). The types of risk that vulnerable kids face online can be categorized by: the content they are exposed to or share with others; the contact they have with trusted or untrusted individuals; and the conduct they display toward others that defines their identities.

## Three forms of risk: content, contact, and conduct

Researchers typically organize the wide range of privacy risks encountered online into the following three categories: content, contact, and conduct risks (Livingstone et al., 2015).

- Content risks: Where a child is exposed to unwelcome and inappropriate content. This can include sexual, pornographic, and violent images; some forms of advertising; racist, discriminatory, or hate speech material; and websites advocating unhealthy or dangerous behaviors, such as self-harm, suicide, and anorexia.
- Contact risks: Where a child participates in risky communication, such as with an adult seeking inappropriate contact or soliciting a child for sexual purposes, or with individuals attempting to radicalize a child or persuade him or her to take part in unhealthy or dangerous behaviors.
- Conduct risks: Where a child behaves in a way that contributes to risky content or contact. This may include children writing or creating hateful materials about other children, inciting racism, or posting or distributing sexual images, including material they have produced themselves.

While it is relatively easy to categorize various forms of risk in general, it is much harder to determine the risk relationship between a particular online image or activity and an individual child. The following table describes these types of risks and the resulting harms (Nyst, 2017, p. 73):

| | Content: child as recipient (mass productions) | Contact: child as participant (adult-initiated activity) | Conduct: child as actor (perpetrator or victim) |
|---|---|---|---|
| Aggressive | • self-abuse and self-harm<br>• suicidal content<br>• discrimination<br>• exposure to violent content | • radicalization<br>• ideological persuasion<br>• hate speech<br>• stalking | • cyberbullying<br>• stalking<br>• harassment<br>• violent peer activity |
| Sexual | • unwanted/harmful exposure to pornographic content | • sexual harassment<br>• sexual solicitation<br>• sexual grooming | • child sexual abuse<br>• production of child abuse content<br>• child-product indecent images |
| Values | • racism<br>• biased or misleading information | • self-harm<br>• unwelcome ideological persuasion | • potentially harmful user-generated content |
| Commercial exploitation | • embedded marketing and advertising<br>• online gambling | • violation and misuse of personal data<br>• hacking<br>• fraud and theft<br>• sexual extortion | • livestreaming of child sexual abuse<br>• sexual trafficking and exploitation of children |

PHOTO: MARCUS KWAN

## What digital footprints do kids leave?

As children come of age in today's digital society, the digital footprints they leave behind has been shown to have a measurable impact on their lives as adolescents and adults (Martin, Wang, Petty, Wang, & Wilkins, 2018). Research shows that, over the last few years, there has been "a significant increase in Internet usage by 0-8 year olds, partly because children start using digital devices at younger ages. On average across Organization for Economic Co-operation and Development ('OECD') countries with access to digital technologies, 18% of students in 2015 accessed the internet for the first time before reaching the age of 6, an increase of 3 percentage points since 2012" (Graafland, 2018, p. 10). In addition, parents can be a potential source of children's data misuse. Parents increasingly start building digital footprints for their children, even before they're born (e.g., parents announcing the mother's pregnancy on social media platforms and apps tracking the movement and heart rate of the fetus). Many hospitals even offer access to third-party professional photographers to take newborn baby photos with the mother and her baby only mere hours after birth. Unknown to most mothers is that those intimate photographs may be used to market professional photography services to other parents and hospitals for the rest of that child's life.

Research has shown that 81% of children under age 2 currently have some kind of digital footprint, with images of them posted online (AVG Technologies, 2015). In the U.S. that percentage rises to 92%, while for the EU the figure is 73% (AVG Technologies, 2015). When it comes to digital skills for kids 2 to 5 years old, "more small children can open a web browser (25%) than swim unaided (20%), and most 6- to 9-year-olds and almost half [of] 6- to 7-year-olds spend more than two hours a week online" (AVG Technologies, 2015). Kids reach digital maturity by the time they're 11, because that is when they establish their own online identities, or begin to participate in their online identities created by their parents and graduate onto mainstream social networks like Facebook, Instagram, Snapchat, and Twitter (AVG Technologies, 2015). Research has shown that 21% of children have encountered websites containing potentially harmful user-generated content such as sites containing hate messages, anorexia/bulimia sites, sites promoting self-harm, or sites that discuss taking drugs. In separate studies in 2011 and 2018, approximately 9% of children age 11 to 16 experienced some form of personal data misuse (Graafland, 2018; Livingstone, Haddon, Görzig, & Ólafsson, 2011, *Risks and safety*). The most common misuses reported were that someone had used their password or pretended to be them (7%); personal information abuse (4%); and that they had lost money by being cheated online (1%) (Livingstone, Haddon, Görzig, & Ólafsson, 2011, *EU kids online*).

> **"The act of going online can dismantle the traditional protections most societies try to place around children, exposing them to unacceptable content, unacceptable behaviour and potentially dangerous contacts with the outside world" (Unicef, 2017, p. 71).**

Traditional protections were established by adults to protect children in real time, either with live adult supervision or structurally, to substitute for adult supervision. In a pre-internet era, adults held the remotes for live channel changing when inappropriate content came onto the television, which was situated in a centrally located living room. Even when an adult was not physically present, parents could assume they set a channel or program and could walk away from the television and the selected program would be appropriate for their kids. Furthermore, time-slot programming prevented younger children, many of whom were likely to be in bed by 9 p.m., from seeing mature content. With each technological innovation, these traditional protections broke down. First, there were multiple television screens in private rooms, then recording devices to time-shift programming, then internet-accessible television programming available at all hours, on multiple devices, and to any user. Similar transitions occurred with regard to relying on adult playground supervision to break up physical fights and classroom teachers reminding students to keep their eyes on the board. Now bullying can occur online outside of adult supervision or knowledge, and students communicate and learn via a variety of technologies, not all of which are a communal experience under the control of a single classroom teacher.

The more time kids spend online, the greater their exposure to online opportunities and risks and also the greater their digital footprints. Research indicates these go hand in hand, as children must encounter and explore online risks in order to learn and develop digital skills. Attempts to minimize risks can limit children's online opportunities, while efforts to maximize opportunities can also increase digital risks (Livingstone et al., 2011, *EU kids online*). As kids start to reach 14 to 17 years old, their online activities are often completely unsupervised. Research shows that 40% of 17-year-olds secretly access their Facebook accounts without parental knowledge when told not to use their devices, which is partly due to adolescents being increasingly worried about the number of likes, favorites, or retweets they get on their posts (AVG Technologies, 2015). Adolescents often delete their recent photos or posts that do not have a large number of likes or favorites in order to support the impression that all of their content and social interactions are popular, which further maintains their online persona, social reputation, and status among peers. Accordingly, approximately 40% of 13- to 17-year-olds in the United States reported feeling pressured to only post popular or flattering content (Lenhart, 2015). This is not surprising, as receiving "one-click" feedback (such as likes or pokes) activates the part of the brain that is involved in explicit pleasure and addiction (Sherman, Payton, Hernandez, Greenfield, & Dapretto, 2016). The developing adolescent brain is more easily able to create pathways of addiction that involve several factors and processes, as described in Winters, as cited in Nestler & Malenka (2004), that include the neurobiology of addiction, environmental factors, genes, vulnerabilities, and disorders. Research about adolescent brain development provides insights into and additional clues as to why adolescence might be a particularly vulnerable period for developing a substance use disorder or internet addiction to receiving "one-click" feedback (such as likes or pokes) (Casey, Jones, & Hare, 2008; Winters, 2009; Felt & Robb, 2016).

However, this behavior can be harmful, as receiving "one-click" feedback is associated with reduced well-being (e.g., lower self-esteem, increased anxiety and depressed feelings) among adolescents (Burke & Kraut, 2016; Kross et al., 2013). Digital footprints also allow advertisers to learn which content a child does or does not favorite or like, which allows advertisers to specifically target messages to kids they know are more likely to be influenced and also to spread viral content through their peer groups. A Pew Research Center survey showed that 81% of parents of 13- to 17-year-olds surveyed in the United States reported being concerned about how much information advertisers can learn about their child's online behavior (Madden, Cortesi, Gasser, Lenhart, & Duggan, 2012).

**"Adolescents have real concerns about the place of digital technology in their everyday lives. They are sensitive to the tensions created when their desire to engage online has to be weighed against their need to protect themselves, their responsibilities to themselves and others, and the responsibilities of adults to help them live and grow well in the digital age" (Nyst, 2017, p. 83).**

Digital baggage, or the digital footprint that has accumulated since birth, can cause additional risks for adolescents as they move into adulthood where "over a quarter (27%) admit to there being 'inappropriate' photos of them online, while almost half (46%) say that there are photos on the Internet of them that they wish they could remove" (AVG Technologies, 2015). As kids transition to being working adults, the privacy risks continue to cause concern both at home and at work, where "of those that agreed social media has eroded their privacy at work, nearly a quarter (24%) now avoid posting on social networks that have caused them privacy concerns, while 23% limit their posts and more than half (53%) are more careful about what they post" (AVG Technologies, 2015).

A recent survey found that "more than half of employers have said they have not hired a candidate because of content they found on social media, but a similar number said if they can't find an applicant online, they are less likely to call that person in for an interview" (Quraishi, 2019). This leaves young people who are trying to participate in educational and vocational opportunities in a quandary. If they have no online presence, they may not only not be able to communicate with friends, but they also may not be able to access online assignments for college classes or job applications available through social media sites. Yet if they have an expansive online presence, such as a paid influencer, video content creator, or controversial blogger, their online persona may clash with the job opportunity offered by a company that does not want to be associated with such content. Needless to say, social content that indicates that the young job applicant has used drugs or participated in any illegal activity would be a disincentive for an employer. Even deleted posts or posts with a limited shelf life may come back to haunt the young job applicant.

As kids reach adulthood and enter the job market at age 18 to 25, they are presented with new types of risks. As adults, today's children and adolescents will be subject to a scrutiny and historical digital footprint record that we cannot begin to imagine. For example, "while most of us were, blessedly, able to forget, reimagine or reinvent part of our early lives, loves, jobs, thoughts, deeds, comments and mistakes, today's children will be in a very different spot. A single stupid comment can lead to decades of disdain and cyberbullying. A single stupid action can be reviewed by authorities, voters or employers decades later" (Unicef, 2017, p. 94).

Misuse or disclosure of personal information can also increase the risk of being cyberbullied or of engaging in self-deprecating behaviors, which can have a significant impact on an individual's psychological and physical health, potentially decreasing life satisfaction and increasing depression and drug and alcohol use among the victim. Marginalized groups face even greater risks of online harassment based on their race, ethnicity, or sexual orientation. A 2013 study of 5,907 internet users in the United States age 13 to 18 found that those who self-identified as lesbian, gay, bisexual, or transgender were disproportionately at risk of online sexual harassment (Mitchell, Ybarra, & Korchmaros, 2014).

# What type of personal information is at risk?

The tremendous amount of personal information collected from and about kids by applications and services includes a wide range of internal, external, financial, social, technological, and political information. The more personal information collected from, and about, a child or student, the greater the content, contact, and conduct risks and magnitude of any resulting harm.

Personal information is generally defined as any information that identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular child, student, or household. This means that when a kid downloads an app or logs in to a service and provides their information, that information is likely personal information that could be used to cause them intentional or unintentional harm in the future. In addition, the nature of collecting personal information from kids, through shared technology devices and applications and services used at home and in the classroom, easily allows for the association of a specific child to a household and their parents and a student to their school, classroom, and educator (Christl, 2017). This can lead to information asymmetry, where companies, organizations, and governments through their data-collection, data-association, and data-recombination processes can have better intimate knowledge about a kid's social and emotional behaviors and idiosyncrasies than the kid or parent/teacher does.

The following list of categories of personal information represent details that may be misused, used to target or bully, or used to manipulate a kid's behavior, potentially increasing the content, contact, and conduct risk exposure. This additional risk exposure increases the likelihood of intentional or unintentional harm if the respective personal information is not adequately protected. Due to these increased risks and potential harms, there is an increased need to ensure that information collected is not used, or not disclosed in a context other than the context or purpose for which it was collected.

## Internal information

- "Knowledge and beliefs" describes information about what a person knows or believes, such as their religious beliefs or their private thoughts.
- "Authentication" describes information used to authenticate a person with an application or service with something they know, such as a username and password or an answer to a secret question.
- "Preferences" describes information about a person's unique opinions, interests, or intentions that direct their actions.

## External information

- "Identification" describes information that uniquely identifies a specific person based on their characteristics such as their name, unique identifier, photograph, or biometric data.
- "Ethnicity" describes information about a person's origins or lineage such as their race, national origin, or languages spoken.
- "Sexual identity" describes information about a person's gender identity, sexual orientation, preferences, proclivities, and history with their partners.
- "Behavioral information" describes a person's knowledge, traits, personality, and activities that direct their actions.
- "Demographic" describes information about a person's characteristics that they share with a group of other persons such as age, race, gender, education, and geographic location.
- "Health" describes information about a person's medical conditions or health care records including information about their physical and mental health, drug tests, disabilities, fertility, family history, blood type, DNA, biometric data, surgeries, and drug prescriptions.
- "Physical characteristics" describes information about a person's unique physical characteristics such as their height, weight, age, hair and eye color, skin tone, and gender.

## Financial information

- "Accounts" describes information that identifies a person's financial accounts such as their credit or debit card number, bank account number, or other monetary account number.
- "Property" describes information about tangible and intangible things a person has rented, borrowed, licensed, or owned/owns such as a car, a house, land, digital items, or personal possessions.
- "Transactions" describes information about a person's financial activities such as their purchases, sales, credit, income, loans, taxes, and spending habits.

- “Credit” describes information about a person’s reputation with lending sources such as their earning potential, spending data, and history paying back money owed to others through credit reports, credit scores, credit availability, and credit worthiness.

## Social information

- “Professional” describes information about a person’s professional job or career such as their job title, salary, work history, subordinates, yearly evaluations, references, interviews, certifications, complaints, and disciplinary actions.
- “Criminal and civil” describes information about a person’s criminal activity such as arrest records, trial proceedings, convictions, probations, and pardons as well as civil lawsuits with settlements and details of the dispute.
- “Education” describes information about a person’s educational records as a student such as their contact information, family contact information, schools, teachers, classes, subjects, grades, assignments, and scholarships, as well as disciplinary actions taken against them.
- “Public” describes information about a person’s public identity such as their character, reputation, social status, marital status, religion, political affiliation, interactions, and community affiliations.
- “Family” describes information about a person’s family relationships such as family structure, marriages, divorces, adoptions, siblings, offspring, and inheritance.
- “Social network” describes information about a person’s friends or connections that include their associations, their group memberships, and the history of the connections.
- “Communication” describes information about a person’s messages or communications to others such as voice recordings, electronic mail correspondence, attachments, and instant messages sent through other technology platforms. Information about end-to-end encrypted communications may still describe communication metadata such as the platform used to send a message, the time the message was sent and received, the identification of the sender and receiver, and the amount of message data sent and received.

## Technological information

- “Devices” describes information about the devices with unique identifiers a person uses to access digital content, such as a mobile device, tablet, laptop, personal computer, TV, or internet-connected smart device.
- “Software” describes information about which operating systems and versions of applications and services a person uses, such as games and apps for communication, browsers to access websites, apps for collaboration with friends, services for content creation, and services that deliver media entertainment or news.
- “Subscriptions” describes information about the free or paid plans for services a person uses to access technology, such as a broadband internet plan, mobile voice and data plan, television channel plan, or software access subscription plan.
- “Tracking” describes information about the history of the content a person accesses and includes the device or software they access the content from, what content they accessed before and after that content, at which location they accessed it, when they accessed it, how long they accessed it, how they interacted with it, how much they paid for access, who else interacted with it, and what other content is connected to it.

## Political information

- “Speech” describes information about the type and content of political messages or opinions a person provides to others and that is meant to persuade, influence, or polarize their knowledge or beliefs.
- “News” describes information about the type and source of political content or opinions that a person receives and that is meant to inform their knowledge or beliefs.
- “Misinformation” describes information about the veracity and source of political content or opinions that a person receives and that is meant to persuade or influence their knowledge or beliefs.
- “Contributions” describes information about monetary gifts or other forms of value a person provides to a particular candidate, political party, ballot measure, or political action fund.
- “Activism” describes information about the type and content of political activities a person participates in such as rallies, marches, protests, demonstrations, candidate events, signature gathering, and civil disobedience.

# PRIVACY HARMS

## What are the harms?

Even though children and students might encounter online privacy risks similar to those of parents and educators, they can experience very different outcomes in terms of harms (Fau & Moreau, 2018). It is important for parents and educators to understand both the privacy risks, which include the selling of data, third-party marketing, behavioral advertising, third-party tracking, and the creation of advertising profiles, as well as the privacy harms, which include loss of attention, poor mental health, broken relationships, and a threat to our democracy ("Privacy Program," 2019; Center for Humane Technology, 2019). Once a kid downloads an app or logs in to a service that does not respect their privacy, it's often too late to protect their privacy and minimize their future risk of exposure or the impact of any harms. If a kid provides their personal information to a product that does not respect privacy, then that kid's information can be collected, used, and shared with third parties who can continue to use that kid's data to influence their decisions for the rest of their lives. Even if a kid deletes their data or removes the app, the harm does not go away; it only stops the spread of additional harm with that application or service. The potential harm keeps spreading. The impact of deleting a kid's data is only relative to the application or service to which they provided their data in the first place, because deletion does not stop the information from spreading to third parties with access to the data. Children and students typically have no ability to protect their privacy or exert control over how third parties use their data once it has been collected and shared (Carpenter v. United States, 2018).

**After a kid's data has been shared with third-party companies, those same companies can still use their own copies of the data for their own purposes.**

This harm is further exacerbated in the event of data breach. For example, if a kid's personal information is publicly disclosed to third parties in a data breach, then it is difficult or impossible to stop it from being shared indefinitely, and there is no simple way to stop the potential harm from spreading, even if the kid were to delete all of their data from the company that had the data breach after the fact ("K-12 Cybersecurity Resource Center," 2019). In addition, the potential harm to a kid is proportional to the type and amount of sensitive personal information disclosed. More sharing of personal and intimate details about a kid amplifies both the potential and magnitude of inappropriate use and harm. Unlike in a home burglary where you will not likely ever see your stolen physical possessions again, personal information of a kid lost in a data breach is often sold or recombined with other information about that kid by third parties who use the information to target advertisements or steal the identity of that kid, their parents, or their educators, for the rest of their lives.

**You can turn off a non-age-appropriate movie, but you can't turn off an app that doesn't respect privacy.**

Companies and schools may use products that collect extremely detailed and sensitive information about children and students, including family financial information, health information, real-time location, biometrics such as palm prints or fingerprints, Social Security numbers, and behavioral and disciplinary records. There are immediate risks to the collection and storage of this sensitive personal information, such as the disclosure of students' behavioral or special education records, which can lead to reputational and emotional harm and potential bullying (Nyst, 2017, p. 9).

Research indicates "whereas in previous generations, children being bullied could escape such abuse or harassment by going home or being alone, no such safe haven exists for children in a digital world. Carrying a mobile phone, laptop or other connected device means that texts, emails, chats and social media posts can arrive anytime, day or night. And online bullying carries on, spreading widely among peers and inflicting reputational harm whether the child is online or off" (Unicef, 2017, p. 74). If a child's real-time location is obtained by a "bad actor," such as deceptive advertisers, abusive (ex)partners of a parent, or child groomers, they could pose direct physical and safety concerns. Even if the number of children suffering severe harm is relatively low, when harm does occur to a child, according to review of evidence in this area, its impact on the child can be significant and justifies the allocation of substantial resources and attention to prevent the harm (Slavtcheva-Petkova, Nash, & Bulger, 2015). First of all, simply counting the number of children who report that they personally have been bullied does not capture all of the harm that occurs as the result of online bullying. While the number of children who are bullied, especially the percentage of those affected who report being bullied, may be small as a percentage of overall users, the culture of online bullying hurts everyone. Bullying and other negative communication online affect children who see it, hear about it, read about it, and live it. It is a culture of fear. Parents and educators need to better understand the privacy risks and potential harms of applications and services so they can make informed decisions about which apps their children and students should use before they download or log in to them, not afterward, because the harm will have already occurred.

## Social and emotional harms

A kid's information can also be misused to create lifelong social and emotional harm. Sensitive personal information about a child's anxieties, fears, secrets, knowledge, and beliefs were traditionally kept private in a diary or shared only in confidence with very close family, friends, or adults they explicitly trusted such as their parents or educators. This sensitive personal information often defines an individual's innermost secrets and sense of self-worth and security (Nyst, 2017, p. 91).

Sharing this information in confidence can help build that kid's foundation of trust and safety. Sharing this information online, however, turns social media, which by its name suggests a public function, into the publishing of a private diary. There are two basic methods that place the private diary in public hands: One, children with little understanding of how privacy or technology work "voluntarily" share this information online, expecting just a friend or small circle of close acquaintances to see the material. Two, sensitive personal information can be collected knowingly or unknowingly by a company through that kid's use of an application or service at home or in the classroom and used at any time to exploit their vulnerabilities.

We cannot, nor should we, eliminate all risks, but the most vulnerable are those most exposed to risk and therefore the most likely to suffer the harms. It is critically important to understand why risk can translate into actual harm for certain children and not for others. Some children may be unaffected by luck of the draw, in that their data isn't chosen or used inappropriately. Other children may be victimized, especially if they fall into a particularly vulnerable category as discussed in this report's section "Who is vulnerable to the risks?" (pg. 2).

> **"It opens our eyes to the underlying vulnerabilities in the child's life that can place him or her at greater risk in the digital age. By better understanding and addressing these vulnerabilities, we can better protect children both online and offline, and better enable them to enjoy the opportunities that come from being connected in the digital age" (Unicef, 2017, p. 71).**

If sensitive personal information is used to target children, students, or their parents or educators with behavioral advertisements, those targeted advertisements could cause harm to a kid if the information in the message was also disclosed to that kid's family, friends, or peer groups. We don't need a data breach or a bad actor for things to go wrong. Simple commercialization of kids' private data can result in harm to children. In a now famous example of embarrassing disclosure, Target analyzed a teenage girl's data and decided she was pregnant and disclosed this information to her father (Hill, 2012).

Research shows that behavioral advertising that uses personal information to target online ads to specific behaviors, as well as other advertising techniques, can contribute to the growing commercialization of childhood (Palfrey, Gasser, & boyd, 2010). For example, disclosure of sensitive personal information could cause social harms such as loss of a parent or educator's money or employment status if the information contained negative remarks about that parent or educator's company, supervisors, or colleagues. For example, the former head of a private preparatory school in Miami, Florida, lost an $80,000 confidential discrimination settlement after his daughter boasted about it on Facebook (Stucker, 2014).

In addition, a kid may experience reputational harm or cyberbullying if their sensitive personal information is intentionally or unintentionally disclosed to others at their school; that information can include their private messages, education records, intimate details, or explicit photos. A research survey of parents in the U.S. found that 26% reported that their child was a victim of cyberbullying in 2018 (Cook, 2018). Inadvertent disclosure of sensitive information to a kid's peer groups could lead to cyberbullying and extreme social changes such as social or emotional learning problems in the classroom, poor learning outcomes with students repeating grades, disciplinary actions, or even expulsion (Tokunaga, 2010).

For example, for months, 12-year-old Mallory Grossman received taunts in text messages, Instagram posts, and Snapchats from classmates that said "why don't you kill yourself?" The taunts, her parents say, took a toll on the lively young cheerleader and gymnast. At school, Mallory's grades deteriorated, and at home, she complained of constant headaches and stomach pain. Mallory begged to stay home from school, and then on June 14, 2017, she took her own life (Schmidt, 2017). There are also real-word consequences for the perpetrators of cyberbullying. In another example, more than a dozen students were expelled from Boulder Preparatory High School in Boulder, Colorado, after being involved in posting rape memes, messages championing "white power," and comments to their classmates about wanting to kill black and Jewish people in a group called the 4th Reich Official Group Chat on Facebook (Levin, 2016).

In the *American Sex and Tech* survey from 2008, 39% of 13- to 19-year-olds reported that they had sent or posted sexually suggestive messages, 20% reported that they had sent or posted nude or seminude photos of themselves, and 38% reported that the act of sexting someone made dating or hooking up with that person more likely (Kosenko, Luurs, & Binder, 2017). Disclosure of this sensitive information either intentionally or unintentionally could cause irreparable behavioral, emotional, physical, or social harm to a kid that could result in sudden changes to their mood or personality and in extreme cases lead to self-harm, such as cutting, or increased risk of suicide (Nixon, 2014; Kowalski & Limber, 2013; Centers for Disease Control and Prevention, 2018).

> **"Strong evidence shows that girls face much greater pressure to send sexually explicit images and suffer much harsher judgements when those images are shared beyond the intended recipient" (Livingstone & Mason, 2015, p. 10; boyd, Ryan, & Leavitt, 2011).**

Sexual blackmail has affected very young teens. For example, "when Amanda Todd, a Canadian adolescent, was about 13, a man she met in a video chat room convinced her to expose her breasts on camera. He captured the image and used it to blackmail her, threatening to send the image to her friends and family. She ignored the threat and over the next two years was subject to bullying (both online and offline), harassment and physical assault. Despite her efforts to escape the torment—she moved both schools and cities—the attacks continued, both by the online offender and by her classmates. During this time, she struggled with depression, drug and alcohol abuse, isolation, loneliness and self-harm. Two years later, in October 2012, at 15, Amanda committed suicide" (Nyst, 2017, p. 74). While for boys, possessing and exchanging explicit images of girls adds to their reputation and status among peers. However, for girls, participating in sending explicit images or "sexting" raises concerns about the potential risks to their sexual reputation among peers (e.g., being called a "slut") (Ringrose, Harvey, Gill, & Livingstone, 2013).

## Surveillance harms

Parents and schools that use technology to monitor a kid's daily activities can automatically collect all the information a kid generates on applications or services, which can include sensitive personal information. This collection practice can serve to normalize surveillance technologies for children and students at a young age and can change the way they regard their private information. Children with resulting lower expectations of privacy may then assume that all technologies are engaged in the same type of surveillance activities, which can lead them to download apps that also do not respect their privacy (Unicef, 2017, p. 9). In addition, research shows that when people know they are being constantly monitored, they change their behavior in response to the surveillance, which can produce chilling effects on forms of action or expression (Shaw, 2017; Christl, 2017).

Children and students who change their minds and wish to keep their sensitive personal information private and who choose to opt out of providing their personal information to apps that do not respect their privacy, or who refuse to opt in and subject themselves to surveillance and monitoring technologies, are often seen as rejecting social norms and are excluded from school and peer activities. However, these choices mean that students may not be able to take advantage of educational technology used in the classroom and at home to complete assignments, which may put them at risk for lower test scores and at a learning disadvantage compared to their peers. At the same time, children and students have ever fewer options to resist the power of this data ecosystem; opting out of pervasive tracking and profiling has essentially become synonymous with opting out of much of modern life (Christl, 2017). This social harm can result in increased social isolation and a cycle of exclusion from peer groups that can lead to anxiety and depression. Ultimately, peer pressure to use normalized surveillance technologies in order to participate in social activities results in children and students reluctantly using products that do not respect their privacy to try to conform to societal norms.

For example, kids have reported that when they know all their online activities are being monitored at home or at school by surveillance technologies, they change their behavior in response and are less likely to engage in conversations or take risks to learn something new or explore controversial ideas that may get them into trouble. As a result, children and students have been found to be less likely to engage in critical thinking, participate in political activism, vote, or question news or authority figures (Brown & Pecora, 2014). Cambridge Analytica, a data-analysis firm, exfiltrated data on 50 million Facebook users in early 2014 to build a system that could profile individual U.S. voters to target them with personalized political advertisements and influence their critical thinking and voting behavior (Cadwalladr & Graham-Harrison, 2018). Research indicates "Cambridge Analytica sought to identify mental and emotional vulnerabilities in certain subsets of the American population and worked to exploit those vulnerabilities by targeting information designed to activate some of the worst characteristics in people, such as neuroticism, paranoia and racial biases" (Written statement to the United States Senate Committee on the Judiciary, 2018). Surveillance technologies with marketing interests have also steered the development of digital networks toward maximizing their consumer surveillance capacities, which fertilized the soil for political manipulation (Crain & Nadler, 2017).

PHOTO: JEN SISKA

### Ideological harms

Rather than simply collect personal information to match consumers with products that fit their existing interests, mass consumer surveillance technologies have led to sophisticated efforts to modify behavior, engineer consumer habits, and intervene upon intimate decision-making processes (Crain & Nadler, 2017). Personal information collected from children and students and their parents over time can be used to influence their decision-making processes now or in the future, which ultimately causes harm to our society and democracy when it results in behavior modifications that change, for example, voting preferences and election outcomes (Epstein & Robertson, 2015). Political participation can be broken down into units of specific behaviors. It's at this granular level where nudges, emotional triggers, and carefully designed choice architecture can exert significant influence at critical steps (Crain & Nadler, 2017).

In a 2010 study published in *Nature*, Facebook reported an experiment involving over 61 million Facebook users who were randomly selected to see different types of messages or no message about voting in their Facebook News Feed on Election Day. The authors of the study found that the Facebook messages likely brought an extra 340,000 people to the poll that day (Talbot, 2012). However, Facebook also used "distributed targeted political ads apparently sponsored by Russian operatives. Most of the ads made no reference to specific candidates. Rather they appeared to focus on amplifying divisive social and political messages across the ideological spectrum—touching on topics from LGBT matters to race issues to immigration to gun rights" (Crain & Nadler, 2017). Political polarization of social issues through ads can be used to make individuals question their strongly held knowledge or belief systems, which can lead to voter suppression if individuals feel they no longer understand the issues or that their vote doesn't matter.

> **"If data-driven targeting and behavioral science can be used to increase voter turnout, it can also be used to suppress it. Here, the task is to identify marginal voters leaning toward an opponent and figure out what behavioral intervention might nudge them not to vote" (Crain & Nadler, 2017).**

Information that affects voter turnout could be really simple, like real or fake information about the weather, the lines at the polls, and/or the possible outcome of the election. None of this has anything on its face that has to deal with choosing a candidate but might be even more effective because it is subtle and less likely to raise alerts. The recipients of such information may not even be able to identify it as influential in their choices (Menn, 2018).

## Who poses a risk of harm to kids?

Research shows that kids value their privacy online and they see risks to their privacy coming from both outside their personal circle, such as from companies and governments, and from within their own circle, such as from overprotective parents, nosy parents, and parents, friends or siblings who spy (Third, Bellerose, Dawkins, Keltie, & Pihl, 2014).

### First- and third-party companies

A kid's personal information is inherently at risk when it's collected by a company that they have a first-party relationship with, such as an app the kid downloads or a website they log in to. These companies may use that same personal information to indirectly influence or modify the behavior of the kid or directly influence the behavior of the kid's parent or educator through first- and third-party marketing and advertising. This influence can be positive in nature, in that useful information about products is transmitted. Still, in the case of marketing to children, we need to be careful in what we allow children to see and to buy. In-app purchases are especially problematic as kids may not realize they are buying with real money rather than playing a game. Moreover, many of the privacy protections afforded to children under 13 years of age with the Children's Online Privacy Protection Act (COPPA) do not apply to children over 13 (Children's Online Privacy Protection Act, 2012). Teens' personal information is at an even greater risk of misuse, because it can be collected and disclosed to third parties without their knowledge or their parent's consent (Felt & Robb, 2016).

First-party companies then may use the information gathered by the direct relationship and share that information with third-party companies that have no relationship with the original underage user. Children or trusted adults can be influenced to purchase other products from that first-party company or, for the children and students, products from other third-party companies. With good intentions of keeping individual privacy intact, many companies monetize data collected from children and students by so-called de-identifying or anonymizing the personal information and building personality or user profiles of children and students to sell to other third-party companies or to license the data for targeted advertising (General Data Protection Regulation, 2018). A kid's de-identified or anonymized data may also be reidentified or aggregated later by any of the third parties along the line once the data has left the care of the first-party company with a direct legal or contractual obligation to maintain the privacy of kids' data. Often, data provided to one application or service that is not considered personal information may still be shared and combined later with other data from a particular kid from another third-party application or service in order to create valuable personal information that can be used to re-identify that kid or link them to separate data sets (Nyst, 2017). This reidentification of a kid's information is often performed without the child, student, parent, or educator's knowledge or consent.

A kid's personal information may also be used by companies that provide banking, housing, or insurance to discriminate against that kid or their parents (Dreyfuss, 2019). Historically, companies used a now-illegal practice called "redlining," which used the personal information and ZIP codes of communities of color to deny them access to housing or banking services. However, personal information provided from a kid about themselves or their parents such as criminal history, credit history, education level, economic status, or even ZIP code could still be used by companies to deny them bank accounts, car loans, access to credit, or rental applications or result in the charging of higher insurance or interest rates. Companies today use as much personal information as they can collect about a child or their parent in their proprietary algorithm decision-making process to determine whether to accept or deny services, or even to determine whether advertisements will be displayed for better opportunities. These decisions are often based on thousands of data points and weighted factors, which makes determining whether illegal discrimination occurred nearly impossible.

The U.S. Department of Housing and Urban Development determined that the social media giant Facebook violated the Fair Housing Act because it "allows landlords and home sellers access to advertising tools that limit which prospective buyers or tenants can view certain online ads based on race, religion, sex, disability and other characteristics" (Booker, 2018). For example, Linda Bradley of Franklin County, Ohio, lost her job at a call center and had been searching for work through Facebook, but Bradley and other female members of the union discovered they were routinely denied the opportunity to receive job ads and recruitment opportunities on Facebook that "similarly situated male Facebook users ... received" (Tiku, 2018).

Companies have access to more personal information about children and their parents than ever before. Technological advancements have enabled companies to use that data to discriminate against vulnerable populations by engaging advertising-targeting technology to exclude them from seeing better opportunities in or information about housing, jobs, education, or credit (Booker, 2018).

## Organizations

A kid's personal information may also be used by organizations such as educational institutions or employers for discrimination. However, the Civil Rights Act of 1964 prevents discrimination in educational facilities and public workplaces for specific protected classes of personal information. Under that act and other federal and state antidiscrimination laws, a person may not be discriminated against based on any of the following: age, pregnancy status, national origin, race, ethnic background, religious beliefs, or sexual orientation (Civil Rights Act of 1964).

Despite these laws, a kid's personal information that is not protected could still be used as a proxy for discrimination if it provides information about themselves, their parents, or their educators. Organizations can easily purchase personal information about children, students, and their parents or educators from third-party companies and data brokers. Although discrimination can exist within all types of classes, there are certain classes of personal information that are not protected under antidiscrimination laws:

- citizenship status
- credit history
- criminal history
- economic class
- education level
- membership in organizations
- physical characteristics
- ZIP code

Regardless, organizations subject to the Civil Rights Act can still serve or not serve advertisements based on protected classes of personal information if the advertisements are not discriminatory. Organizations can still use personal information not protected under antidiscrimination laws to deny children or their parents acceptance into higher educational programs, deny children internship opportunities, deny their parents or educators employment opportunities, or offer better pricing to some groups or individuals.

## Governments

A kid's personal information is also at risk when it's collected by or shared with the U.S. government. Any personal information a kid shares with a company or organization also can be shared with the government at any point they request it for the rest of that kid's life. It is common for a company's policies to allow them to easily share a kid's information with the government for any purpose that they believe is necessary to protect the safety of their company or their users. However, some companies' policies state they will only share a kid's personal information with the government if a government agency presents a subpoena for the information based on probable cause that a crime has been committed and the kid's information must be disclosed as part of the investigation (Cardozo et al., 2018).

**"If governments are able to link individual profiles with data intercepted by mass surveillance, as many believe feasible, this would allow authorities to build and maintain records of children's entire digital existence" (Nyst, 2017, p. 15).**

However, governments do not always need to request that companies or organizations provide them with personal information from children or students that they have collected, because many governments already implement their own sophisticated data-collection surveillance technologies that automatically intercept and collect personal information from its citizens and citizens of other countries for national security purposes without their knowledge. Research indicates "governments can collect vast amounts of online personal data on children, a type of surveillance largely unimaginable in the pre-internet era. Often neither lawful nor publicly acknowledged, mass surveillance now forms a key part of national security efforts in many countries. Not only does it undermine basic notions of privacy, it also threatens other basic human rights, such as freedom of expression, and opens the door to potential abuses of state power" (Brown & Pecora, 2014, p. 202).

**Facial-recognition and other image-recognition tools will soon be able to make this data much, much more useful to law enforcement and other government entities, but it is still prone to errors (Singer, N., 2018; Sengupta, 2013).**

Depending on the type of personal information disclosed to a government and that government's laws, there is a wide range of risks and possible harms that could result. Many governments when investigating a crime may collect and analyze huge volumes of personal information about its citizens, such as mobile app and device phone calls, messages, photos, geolocation histories, emails, and even health information such as familial DNA that could be used to prosecute related family members. Governments may also routinely collect data through a system of contracts with private companies, such as asking a private company to install cameras on city streets. Since the data is collected by a private company rather than the government directly, important legal safeguards established to protect citizens from government overreach may be completely ignored. It is possible that the only thing protecting our privacy at this point in time is that the sheer quantity of video images gathered by these cameras and other data-collection methods is too difficult to use, but that is just for now.

Personal information from a kid could even be used against them or their parents by a foreign government to persuade them to act as an undercover agent or informant against others to avoid prosecution. Other foreign governments that obtain sensitive personal information from children or students could even use that information to blackmail or persuade them or their parents to engage in espionage or treason against their own government to avoid prosecution or even worse consequences by their own government if the sensitive personal information were publicly disclosed. In extreme cases in some countries around the world, a kid's personal information that has been collected or shared with a repressive foreign government about their political activism, homosexual identity, or atheist religious beliefs could lead to the most extreme type of harms against them or their parents such as imprisonment, public stoning, or the death penalty (Ohlheiser, 2013; Lamb, 2019; Bearak & Cameron, 2016).

## Bad actors

Children and student's personal information can also be used by other individuals with bad intentions to cause them intentional physical or emotional harm. Family members, relatives, family friends, acquaintances, neighbors, or even strangers can collect and use personal information from children and students to gain specific and intimate knowledge about them and use that knowledge for their own personal gain and objectives. Research indicates that children and teens consider meeting a stranger online an opportunity to meet new people or even develop romantic relationships, while parents see meeting a stranger online as one of the most dangerous things that could happen to their child on the internet. (Phyfer, Burton, & Leoschut, 2016; Mascheroni & Cuman, 2014). Research examining studies between 1990 and 2016 found that approximately 20% of youth had been exposed to unwanted sexual content online and 11% experienced unwanted online sexual solicitation, with 25% of youth reporting being "extremely" bothered by these experiences (Madigan et al., 2018). Intimate knowledge learned about a child can give bad actors a power differential that allows them to influence a kid's actions as well as influence their family or friends.

"Advances in technology allow offenders to remain anonymous, cover their digital tracks, create false identities, pursue many victims at once, and monitor their whereabouts. The increased use of mobile devices and greater access to broadband internet have made children more accessible than ever through unprotected social media profiles and online game forums. Offenders often begin grooming their victims on these platforms, where they gain a child's attention or trust, before moving the communication to video- and photo-sharing platforms, which can lead to content-driven or financially driven extortion or meeting offline" (Nyst, 2017, p. 76).

Extremist groups can also use digital and communication technologies to collect personal information about kids in order to make contact, radicalize them, and persuade them to take part in unhealthy or dangerous activities, such as striking targets with whatever weapons are available, such as knives or crude bombs (Faiola & Mekhennet, 2017). For example, personal information about a kid's first and last names, their parent or educator's names, their birthday, and their home address could be used by non-parents to impersonate that kid's parent, family member, or educator to persuade others to contact or give over custody of the kid in order to kidnap them or cause them harm. The more personal information a bad actor can collect about a kid the more reputational influence and persuasion they have over others entrusted with the care of those children and students (Bilich, n.d.). For example, the recent documentary *Abducted in Plain Sight* showed how a sexual predator collected and used personal information over time to become an acquaintance and torment an Idaho girl, and her family, for years ("Abducted in Plain Sight," 2017).

Bad actors can also engage in physical or emotional abuse such as physiological abuse, blackmail, kidnapping, child molestation, exploitation, or sex trafficking. Research indicates that "even as information and communication technology has made it easier to share knowledge and collaborate, so, too, has it made it easier to produce, distribute and share sexually explicit material and other illegal content that exploits and abuses children. Such technology has opened new channels for the trafficking of children and new means of concealing those transactions from law enforcement. It has also made it far easier for children to access inappropriate and potentially harmful content—and, more shockingly, to produce such content themselves" (Unicef, 2017, p. 8). Applications and services that collect and share specific personal information about children and students such as their geolocation or status update information over time present a unique risk. If this specific personal information is made publicly available or accessed directly or indirectly by bad actors, the data could be used to stalk a kid over time and learn intimate details about their home and school addresses, routines, and friends or even the best time of day to confront them alone.

Children's and students' information can also be abused by fraudsters peddling fake scholarship opportunities. Social Security numbers and other background information can be stolen and used by identity thieves to open up new lines of credit, creating serious problems for children and parents who often don't discover they have been victimized until a number of years have passed; the ease of obtaining a child's information plus delayed discovery, combined with clean credit reports, are reasons children are particularly susceptible to identity theft. Research has shown that children are 35 times more likely to be victims of identity theft because they don't have a credit history and their Social Security number isn't active, according to the Division of Consumer Protection of the New York Department of State (Singer, P., 2018).

## How parents and educators can make a difference

Privacy is complicated, and protecting kids online, regardless of the particular privacy risks and harms they face, requires a holistic and coordinated response that takes into account all the circumstances of a child's life. Risk is specific to each kid's unique situation, and safeguards and protections will need to be adjusted as kids come of age. Understanding the risks will also help minimize the potential harms and maximize the positive outcomes. Parents, teachers, companies, organizations, governments, and kids themselves all have a part to play in keeping kids safe. These recommendations can make a difference in outcomes for kids:

1. **Read high-quality evaluations about which online technologies protect kids' privacy**. As parents, educators, and consumers, we can help encourage companies to make changes in how they collect and use personal information from kids by only purchasing products for kids that protect their privacy and avoiding products that do not. Parents and educators can also use the easy-to-understand privacy evaluations from Common Sense. Privacy evaluations include an overall score, display tier risks, and summarize privacy concerns to help parents and educators make informed choices about the products they use at home and in the classroom ("Privacy Program," 2019). With the Common Sense Privacy Evaluations, anyone can confront privacy concerns before they start. That's why the Common Sense Privacy Program was created: to champion child and student privacy and to support parents, educators, schools, and communities on a path toward a more secure digital future for all kids.

2. **Require commitments to safeguard kids' privacy**. Parents and educators should be able to harness the true power of information and communication technologies to benefit all children, especially the most disadvantaged children, while at the same time limiting the harms to protect those children who are most vulnerable (Nyst, 2017, pp. 11, 84). How-

ever, digital technologies pose significant risks to children's safety, privacy, and well-being. The harms that many children already face offline can make already vulnerable children even more vulnerable (Nyst, 2017, p. 8). Today's surveillance technology and data footprints allow for children's data to be combined and reused in both amazing and alarming ways. Kids deserve a much greater commitment by private companies, organizations, and governments to protect their data and a shared agreement not to misuse or exploit kids' data for their own purposes. Practices that take advantage of kids' susceptibility, developing mental capacity, and inability to discern whether advertising messages are truthful, accurate, and unbiased should be off-limits to kids. Parents and educators also need to teach children by example how to protect themselves from threats to their own privacy and identity (Unicef, 2017, p. 11).

Parents and educators can begin by choosing privacy-protective products and then continue role-modeling by using privacy protections for themselves and refusing to offer their children's information to social media and other products that may use their information for purposes outside of the context in which the information was originally offered. Ultimately, with support from government and industry, parents and educators can make a real difference in safeguarding their kids' privacy by ensuring that digital technologies use kids' personal information in ways that support the rights of the child to:

- keep them safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse;
- protect and support their health and well-being;
- protect and support their physical, psychological, and emotional development;
- protect and support their need to develop their own views and identity;
- protect and support their right to freedom of association and play;
- recognize the role of parents in protecting and promoting the best interests of the child; and
- recognize the evolving capacity of the child to form their own view, and give due weight to that view (Information Commissioner's Office, 2019).

3. **Teach digital literacy and digital well-being**. Kids need to understand the risks of content creation and sharing information online, including learning how to protect their privacy and personal data with privacy settings (Information Commissioner's Office, 2019). In addition, kids need to understand the many ways in which communicating online is different from traditional communication because of its lack of verbal and facial clues to give meaning and its potential for anonymity (Nyst, 2017, p. 129). Social-emotional learning and the teaching of empathy helps develop kids' online resilience and helps to diminish online abuse and hateful language. Check out the Common Sense Digital Citizenship Curriculum for more resources to take on timely topics for school communities, support teachers with improved classroom tools, and prepare kids to take ownership of their digital lives ("Digital Citizenship," 2019).

# CONCLUSION

With this report, we collect the best available information about ways consumers can arm themselves with information when choosing which technology tools to use. There is no one-size-fits-all solution for privacy, and so parents and teachers need to educate themselves with resources like ours and those offered by other trusted sources in order to best understand how to minimize the risk of harms to our youngest consumers based on the personal information collected from them, who has access to it, and how it is used. Our work at the Common Sense Privacy Program steps into the space between what we need to do to protect our kids and the technology that has permeated every aspect of their lives. Now is a pivotal moment in our ability to stop and examine what we have created, evaluate how the technology does and does not protect kids' privacy, and demand better products and services for our kids.

# REFERENCES

Abducted in Plain Sight. (2017). Retrieved from **https://www.imdb.com/title/tt3444312/**

American Psychological Association. (2004, February 23). *Television advertising leads to unhealthy habits in children; says APA task force*. [Press release]. Retrieved from **https://www.apa.org/news/press/releases/2004/02/children-ads**

AVG Technologies. (2015). *The AVG 2015 digital diaries*. Retrieved from **https://www.scribd.com/document/123136168/AVG-Digital-Diaries**

Bearak, M., & Cameron, D. (2016, June 13). Here are the 10 countries where homosexuality may be punished by death. *The Washington Post*. Retrieved from **https://www.washingtonpost.com**

Bilich, K. (n.d.) *Child abduction statistics for parents*. *Parents*. Retrieved from **https://www.parents.com**

Booker, B. (2018, August 19). *HUD hits Facebook for allowing housing discrimination*. Retrieved from **https://www.npr.org**

boyd, d., Ryan, J., & Leavitt, A. (2011). Pro-self-harm and the visibility of youth-generated problematic content. *A Journal of Law and Policy for the Information Society*, *7*(1), 40.

Brown, D., & Pecora, N. (2014). Online data privacy as a children's media right: Toward global policy principles. *Journal of Children and Media*, *8*(2), 201–207. **https://dx.doi.org/10.1080/17482798.2014.893756**

Burke, M., & Kraut, R. (2016). The relationship between Facebook use and well-being depends on communication type and tie strength. *Journal of Computer-Mediated Communication*, *21*(4), 265–281. **https://dx.doi.org/10.1111/jcc4.12162**

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved from **https://www.theguardian.com**

Cardozo, N., Crocker, A., Gebhart, G., Lynch, J., Opsahl, K., & York, J. C. (2018, May 31). *Who has your back? Censorship edition 2018*. Retrieved from **https://www.eff.org**

Carpenter v. United States, 138 S. Ct. 2206 (2018).

Casey, B. J., Jones, R. M., & Hare, T. A. (2008). The adolescent brain. *Annals of the New York Academy of Sciences*, *1124*, 111–126. **https://dx.doi.org/10.1196/annals.1440.010**

Centers for Disease Control and Prevention. (2018). *Youth risk behavior surveillance — United States, 2017* (Morbidity and Mortality Weekly Report). Retrieved from **https://www.cdc.gov/healthyyouth/data/yrbs/pdf/2017/ss6708.pdf**

Center for Humane Technology. (2019). Ledger of harms. Retrieved from **https://ledger.humanetech.com**

Children's Online Privacy Protection Act, 16 C.F.R. Part 312 (2012).

Christl, W. (2017). *Corporate surveillance in everyday life: How companies collect, combine, analyze, trade, and use personal data on billions*. Retrieved from Cracked Labs website: **http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf**

Civil Rights Act of 1964, 42 U.S.C. § 2000d et seq. (1964).

Cook, S. (2018, November 12). *Cyberbullying facts and statistics for 2016-2018*. Retrieved from **https://www.comparitech.com**

Crain, M., & Nadler, A. (2017, September 27). *Commercial surveillance state: Blame the marketers*. Retrieved from **https://nplusonemag.com**

Digital Citizenship. (2019). Retrieved from **https://www.commonsense.org/education/digital-citizenship**

Dreyfuss, E. (2019, March 9). Facebook changes its ad tech to stop discrimination. *Wired*. Retrieved from **https://www.wired.com**

Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. *Proceedings of the National Academy of Sciences of the United States of America*, *112*(33), E4512–E4521. **https://dx.doi.org/10.1073/pnas.1419828112**

Faiola, A., & Mekhennet, S. (2017, February 11). They're young and lonely. The Islamic State thinks they'll make perfect terrorists. *The Washington Post*. Retrieved from **https://www.washingtonpost.com**

Fau, S., & Moreau, Y. (2018). *Managing tomorrow's digital skills: what conclusions can we draw from international comparative indicators?* Retrieved from UNESCO Digital Library website: **http://unesdoc.unesco.org/images/0026/002618/261853e.pdf**

Felt, L. J., & Robb, M. B. (2016). *Technology addiction: Concern, controversy, and finding balance*. Retrieved from Common Sense website: **https://www.commonsensemedia.org/sites/default/files/uploads/research/csm_2016_technology_addiction_research_brief_0.pdf**

General Data Protection Regulation (GDPR), Recital 38, Regulation (EU) 2016/679.

Graafland, J. H. (2018). *New technologies and 21st century children: Recent trends and outcomes*. Retrieved from Organisation for Economic Cooperation and Development website: **https://www.oecd-ilibrary.org/education/new-technologies-and-21st-century-children_e071a505-en**

Grabe, S., Ward, L. M., & Hyde, J. S. (2008). The role of the media in body image concerns among women: A meta-analysis of experimental and correlational studies. *Psychological Bulletin*, *134*(3), 460–476. **https://dx.doi.org/10.1037/0033-2909.134.3.460**

Hill, K. (2012, February 16). How Target figured out a teen was pregnant before her father did. *Forbes*. Retrieved from **https://www.forbes.com**

Huckvale, K., Torous, J., & Larsen, M. E. (2019). Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *The Journal of the American Medical Association Network Open*, *2*(4). **https://dx.doi.org/10.1001/jamanetworkopen.2019.2542**

Information Commissioner's Office. (2019). *Age appropriate design: A code of practice for online services*. Retrieved from **https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf**

The K-12 Cyber Incident Map. (2019). Retrieved from **https://k12cybersecure.com/map**

Kelly, G., Graham, J., & Fitzgerald, B. (2018). *2018 state of edtech privacy report*. Retrieved from Common Sense website: **https://www.commonsense.org/education/sites/default/files/tlr-blog/cs-state-of-edtech-privacy-report.pdf**

Kosenko, K., Luurs, G., & Binder, A. (2017). Sexting and sexual behavior, 2011-2015: A critical review and meta-analysis of a growing literature. *Journal of Computer-Mediated Communication*, *22*(3). **https://dx.doi.org/10.1111/jcc4.12187**

Kowalski, R. M., & Limber, S. P. (2013). Psychological, physical, and academic correlates of cyberbullying and traditional bullying. *Journal of Adolescent Health*, *53*(1), S13–S20.

Kross, E., Verduyn, P., Demiralp, E., Park, J., Seungjae, D. L, Lin, N., ... Ybarra, O. (2013). Facebook use predicts declines in subjective well-being in young adults. *PLoS ONE*, *8*(8). **https://dx.doi.org/10.1371/journal.pone.0069841**

Lamb, K. (2019, April 3). Brunei brings in stoning to death for gay sex, despite outcry. *The Guardian*. Retrieved from **https://www.theguardian.com**

Lenhart, A. (2015). *Teens, technology and friendships*. Retrieved from Pew Research Center website: **http://www.pewinternet.org/2015/08/06/teens-technology-and-friendships**

Levin, S. (2016, October 14). Students expelled after Facebook group calls for 'execution' of Jews, black people. *The Guardian*. Retrieved from **https://www.theguardian.com**

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *EU kids online: final report*. Retrieved from London School of Economics and Political Science website: **http://eprints.lse.ac.uk/39351/1/EU_kids_online_final_report_%5BLSERO%5D.pdf**

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*. Retrieved from London School of Economics and Political Science website: **http://eprints.lse.ac.uk/33731/**

Livingstone, S., Mascheroni, G., & Staksrud, E. (2015). *Developing a framework for researching children's online risks and opportunities in Europe*. Retrieved from London School of Economics and Political Science website: **http://eprints.lse.ac.uk/64470/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU%20Kids%20Online_Developing%20framework%20for%20researching_2015.pdf**

Livingstone, S., & Mason, J. (2015). *Sexual rights and sexual risks among youth online: A review of existing knowledge regarding children and young people's developing sexuality in relation to new media environments*. Retrieved from London School of Economics and Political Science website: **http://eprints.lse.ac.uk/64567/1/Livingstone_Review_on_Sexual_rights_and_sexual_risks_among_online_youth_Author_2015.pdf**

Madden, M., Cortesi, S., Gasser, U., Lenhart, A., & Duggan, M. (2012). *Parents, teens, and online privacy*. Retrieved from Pew Research Center website: **https://www.pewinternet.org/2012/11/20/parents-teens-and-online-privacy/**

Madigan, S., Villani, V., Azzopardi, C., Laut, D., Smith, T., Temple, J. R., ... Dimitropoulos, G. (2018). The prevalence of unwanted online sexual exposure and solicitation among youth: A meta-analysis. *Journal of Adolescent Health*, *63*(2), 133–141. **https://dx.doi.org/10.1016/j.jadohealth.2018.03.012**

Martin, F., Wang, C., Petty, T., Wang, W., & Wilkins, P. (2018). Middle school students' social media use. *Journal of Educational Technology & Society*, *21*(1), 213–224. Retrieved from **https://www.j-ets.net/ETS/journals/21_1/19.pdf**

Mascheroni, G., & Cuman, A. (2014). *Net children go mobile: Final report (with country fact sheets). Deliverables D6.4 & D5.2*. Retrieved from Net Children Go Mobile website: **http://netchildrengomobile.eu/reports/**

McKenna, K., Green, A., & Gleason, M. (2002). Relationship formation on the internet: What's the big attraction? *Journal of Social Issues*, *58*(1), 9–31. **https://dx.doi.org/10.1111/1540-4560.00246**

Menn, J. (2018, October 15). *Exclusive: Facebook to ban misinformation on voting in upcoming U.S. elections*. Retrieved from **https://www.reuters.com**

Meyer, M., Adkins, V., Yuan, N., Weeks, H. M., Chang, Y., & Radesky, J. (2019). Advertising in young children's apps: A content analysis. *Journal of Developmental & Behavioral Pediatrics*, *40*(1), 32–39. Retrieved from **http://childrenstech.com/files/2018/11/Advertising_in_Young_Children_s_Apps___A_Content.99257.pdf**

Mitchell, K., Ybarra, M., & Korchmaros, J. (2014). Sexual harassment among adolescents of different sexual orientations and gender identities. *Child Abuse and Neglect*, *38*(1), 43–71. **https://dx.doi.org/10.1016/j.chiabu.2013.09.008**

Nestler, E. J., & Malenka, R. C. (2004). The addicted brain. *Scientific American*, *290*(3), 78–85, Retrieved from **http://sites.oxy.edu/clint/physio/article/theaddictedbrain_sciam.pdf**

Nixon, C. L. (2014). Current perspectives: The impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics*, *5*, 143–158.

Nyst, Carly. (2017). *Privacy, protection of personal information and reputation*. Retrieved from Unicef website: **https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf**

Ohlheiser, A. (2013, December 13). There are 13 countries where atheism is punishable by death. *The Atlantic*. Retrieved from **https://www.theatlantic.com**

Palfrey, J. G., & Gasser, U., & boyd, d. (2010). *Response to FCC notice of inquiry 09-94: Empowering parents and protecting children in an evolving media landscape* (Berkman Center Research Publication No. 2010-02). Retrieved from **https://cyber.harvard.edu/publications/2010/Re_Empowering_Parents_Protecting_Children**

Phyfer, J., Burton, P., & Leoschut, L. (2016). *South African kids online: Barriers, opportunities & risks. A glimpse into South African children's internet use and online activities*. Retrieved from Global Kids Online website: **http://globalkidsonline.net/wp-content/uploads/2016/06/GKO_Country-Report_South-Africa_CJCP_upload.pdf**

Privacy Program. (2019). Retrieved from **https://privacy.commonsense.org**

Quraishi, H. (2019, April 13). *Under employers' gaze, gen Z is biting its tongue on social media*. Retrieved from **https://www.npr.org**

Ringrose, J., Harvey, L., Gill, R., & Livingstone, S. (2013). Teen girls, sexual double standards and 'sexting': Gendered value in digital image exchange. *Feminist Theory*, *14*(3), 305–323. **https://dx.doi.org/10.1177/1464700113499853**

Schmidt, S. (2017, August 2). After months of bullying, her parents say, a 12-year-old New Jersey girl killed herself. They blame the school. *The Washington Post*. Retrieved from **https://www.washingtonpost.com**

Sengupta, S. (2013, October 13). Privacy fears grow as cities increase surveillance. *The New York Times*. Retrieved from **https://www.nytimes.com**

Shaw, J. (2017, January/February). The watchers: Assaults on privacy in America. *Harvard Magazine*. Retrieved from **https://harvardmagazine.com**

Sherman, L., Payton, A., Hernandez, L., Greenfield, P., & Dapretto, M. (2016). The power of the like in adolescence. *Psychological Science*, *27*(7), 1027–1035. **https://dx.doi.org/10.1177/0956797616645673**

Singer, N. (2018, July 26). Amazon's facial recognition wrongly identifies 28 lawmakers, A.C.L.U. says. *The New York Times*. Retrieved from **https://www.nytimes.com**

Singer, P. (2018, August 29). Kids 35 times more likely to be identity theft victims. Here's how to avoid it. *The Democrat & Chronicle*. Retrieved from **https://www.democratandchronicle.com**

Slavtcheva-Petkova, V., Nash, V., & Bulger, M. (2015). Evidence on the extent of harms experienced by children as a result of online risks: Implications for policy and research. *Information, Communication & Society*, *18*(1), 48–62. **https://dx.doi.org/10.1080/1369118X.2014.934387**

Stucker, M. (2014, March 2). *Girl costs father 80,000 dollars with 'SUCK IT' Facebook post*. Retrieved from **http://www.cnn.com**

Talbot, D. (2012, September 12). How Facebook drove voters to the polls. *MIT Technology Review*. Retrieved from **https://www.technologyreview.com**

Third, A., Bellerose, D., Dawkins, U., Keltie, E., & Pihl, K. (2014). *Children's rights in the digital age: A download from children around the world*. Retrieved from Western Sydney University website: **https://www.uws.edu.au/__data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf**

Tiku, N. (2018, September 18). ACLU says Facebook ads let employers favor men over women. *Wired*. Retrieved from **https://www.wired.com**

Tokunaga, R. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, *26*, 277–287. **https://dx.doi.org/10.1016/j.chb.2009.11.014**

Unicef. (2017). *The state of the world's children 2017: Children in a digital world*. Retrieved from **https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf**

Winters, K. C. (2009). Adolescent brain development and alcohol abuse. *The Journal of Global Drug Policy and Practice*, *3*(3). Retrieved from **https://www.dfaf.org/wp-content/uploads/2018/11/Vol-3-Issue-3.pdf**

Winters, K. C., & Arria, A. (2011). Adolescent brain development and drugs. *The Prevention Researcher*, *18*(2), 21–24. Retrieved from **https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3399589/**

Written statement to the United States Senate Committee on the Judiciary, in the matter of Cambridge Analytica and other related issues, 115th Cong. 22 (2018) (testimony of Christopher Wylie).

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75–89. **https://dx.doi.org/10.1057/jit.2015.5**

Zuboff, S. (2016, May 3). Wie wir Googles Sklaven wurden. [The secrets of surveillance capitalism]. *Frankfurter Allgemeine Zeitung*. Retrieved from **https://publicpurpose.com.au/wp-content/uploads/2016/04/Surveillance-capitalism-Shuboff-March-2016.pdf**

## OUR OFFICES

**San Francisco Headquarters**
650 Townsend Street, Suite 435
San Francisco, CA 94103
(415) 863-0600

**Los Angeles Office**
1100 Glendon Avenue, 17th Floor
Los Angeles, CA 90024
(310) 689-7535

**New York Office**
575 Madison Avenue
New York, NY 10022
(212) 315-2138

**Washington, D.C. Office**
2200 Pennsylvania Avenue NW
4th Floor East
Washington, D.C. 20037
(202) 350-9992

common sense®

**www.commonsense.org**

PHOTO: JEN SISKA