common sense kids action

TO: Information Commissioner's Office
FROM: Common Sense
DATE: May 31, 2019
RE: Age Appropriate Design Code - Consultation Draft Response

Common Sense is an independent nonprofit organisation based in the United States dedicated to helping children and families thrive in a rapidly changing digital world. We are based in San Francisco, with offices in Los Angeles, New York, and Washington D.C. and will establish our first international office in the UK later this year. We are the leading organization in the United States that parents, teachers, and policymakers go to for unbiased information, trusted advice, and innovative tools to harness the power of media and technology as a positive force in all children's lives.

Since launching 15 years ago, Common Sense has helped millions of children and families think critically and make smart, responsible choices about the media they create and consume. Common Sense has over 108 million users and our award winning Digital Citizenship Curriculum is the most comprehensive K-12 offering of its kind in the education field; we have over 700,000 registered educators using our curriculum representing over half of schools in the United States. We also champion policy solutions that put children first, working with federal and state legislators and companies to craft rules and best practices that protect privacy, improve digital equity and connectivity, and promote the digital well-being of children and families.

Common Sense applauds the ICO and efforts to support children's rights in the digital environment through its Age Appropriate Design code. This Code embodies many of the principles and practices Common Sense has been seeking to bring to the United States for over a decade, and will serve as an excellent model of how government can encourage companies to design with privacy, child protections, and digital well-being in mind and from the start. We believe that companies should empower young people, and parents, to make better decisions online. One of our key privacy principles is that companies shall be transparent with families about their privacy and security practices, minimize personal information collection and retention, and appropriately safeguard any personal information they do collect. We believe this Code achieves that. We are pleased to offer comments in response to the consultation Code.

General Comment:

Types of Services Covered

We commend the ICO for recognizing that the code needs to apply to all ISS that are likely to be accessed by children, and that the burden is on the company to demonstrate it is not likely to be accessed by a child. In the U.S., where we have had the children's privacy law, COPPA,[1] for over 20 years, companies have evaded responsibility by claiming they are not directed or targeted to children or that they do not have "actual knowledge" of children. Some companies even make these statements to regulators, or try to hide behind the fine print of their policies which claim to not be for children, while at the same time telling advertisers they can reach tween audiences, or

[1] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505

knowing that polls show millions of children are signed up for their services. The ICO should prevent companies from being willfully ignorant of their services being used by children, and empirical evidence and market factors will be key to identifying offending ISS.

When assessing websites or services children are more likely to access, we recommend the United States Federal Trade Commission and its factors for analyzing if a website is directed to children: including subject matter, visual content, use of animated characters or children's activities or incentives, music content, the age of models, the presence of child celebrities or celebrities appealing to children, language used, and promotional materials about the site or service.[2] In addition, we recommend looking at empirical evidence regarding audience composition.[3]

Code Sections:

Section # 2 - Age-Appropriate Application

Code Summary: "Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children."

We applaud the ICO for recognizing that children pass through a range of stages and levels of comprehension and understanding. There is not a magic number at which kids suddenly understand privacy policies, the online ad ecosystem, or manipulative design. In the U.S., we have been educating companies and lawmakers on the benefits of a more transitional approach; an approach we see in the California Consumer Privacy Act, where parental consent is required for companies to sell information of under 13 year olds, and teen consent is required of under 16 year olds.[4] Similarly, the proposed updates to the Children's Online Privacy and Protection Act (COPPA), offered on a bipartisan basis by Senators Markey (D-Ma) and Hawley (R-Mo) would extend privacy protections to young teens but put them, not parents, in control.[5] The approach proposed by the ICO is even more granular and offers ways for services to meet children where they are, and gradually enable them to take effective control over their online experience.

We support the proposal that sites use robust age verification and make the default *no age verification* with strong protections in place. This will allow adults to to opt out of protections reduce incentives for children to lie about their ages. We believe what constitutes "robust age verification" will vary depending on the type of service and the impact it is likely to have on a user's fundamental rights including privacy. Sites that pose little risk to children should be able to use simpler mechanisms, which can enable adults to more easily "opt out" of the protective defaults. We would also caution against requiring or promoting government IDs as a premier type of age verification; that form of age verification can be privacy invasive and circumventable by a child. As the consultation Code notes, age verification tools are a developing area, and there is much innovation occurring in this space. Companies who now have incentives to approach age

[2] 16 CFR 312.2.
[3] Ibid
[4] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100– 1798.199
[5] COPPA 2.0 - Legislation to Update Children's Online Privacy Rules

verification in a robust, privacy protective (and also context dependent) way will no doubt continue to find new solutions.

On the possible concern that adults may be harmed if covered services treat all users like children because services cannot distinguish between users, we do not see this as limiting the rights of adults. What it may do is limit the amount of tracking and targeting adults face on services likely to be accessed by children, and perhaps limit the "relevance" of things that they see. (Again, if a site poses little risk, an adult can easily "opt out" of protections.) In our view, that something is "relevant" or "personalized" is not an unqualified positive. Individuals deserve the opportunity to learn new points of view and be exposed to new ideas.

Section #4 - Detrimental use of data

Code Summary: "Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice."

ISS should never use children's personal data in ways that are detrimental to their well-being, and well being should be broadly defined to encompass children's social, emotional, cognitive, and physical development. Because research on the effects of media and technology on children's well-being is limited, we expect what is deemed detrimental may change in the future.

We appreciate the consultation Code's calling out of strategies "used to extend user engagement." These are related to nudge techniques discussed further below. We believe that such practices have a largely detrimental and harmful effect on youth, and encourage a formal position stating so. In our conversations with children, they report feeling great anxiety over going on vacation and not being able to keep up with "Snap streaks" or of having designated offline time in the evening and not being able to respond immediately to friends' postings on social media. Kids believe they are "addicted" to technology[6]. These tech features create a sense of immediacy and "always on" feeling in children, and are designed to subvert user autonomy and choice and cultivate compulsive usage. In the US, the DETOUR Act, bipartisan legislation introduced by Senators Warner (D-Va) and Fischer (R-Neb), would prohibit a service from:

> "design[ing], modify[ing], or manipulat[ing] a user interface on a website or online service, or portion thereof, that is directed to an individual under the age of 13, with the purpose or substantial effect of cultivating compulsive usage, including video auto-play functions initiated without the consent of a user."[7]

Section # 6 - Default settings

[6] Common Sense Media, "The New Normal: Parents, Teens, and Devices Around the World," 2019
[7] Deceptive Experiences To Online Users Reduction (DETOUR) Act of 2019

Code summary: "Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child)."

We applaud the ICO for requiring that the defaults be strong. This is one of our key privacy principles, that children should have to actively opt in to sharing information. Studies show how few individuals take the time to change default settings, so putting in place strong defaults will ensure kids are protected. It will also ensure protections if children do not understand privacy policies or choices,[8] as in some instances individuals may take the time to study settings but still be unsure what option is best for themselves or their families.

Section #7 - Data minimisation

Code summary: "Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate."

We support the ICO's proposal that companies should only collect and retain what they need. This is an element that we believe is missing from current U.S. law, and one we have called for in future legislation. Data minimization is a key privacy principle that we support, and it is one we have asked Congress for in every U.S. federal privacy legislation.[9]

Section #8 - Data sharing

Code summary: "Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child."

We appreciate the ICO's guidance that the sale of children's information for commercial purposes is unlikely to be appropriate. We would suggest that the code go even further, and indicate that--at the very least in certain contexts, like the education context where children have very little choice--the commercial sale of children's information is *not* a compelling reason that would justify data sharing. Indeed, a landmark California student privacy law that we spearheaded, the Student Online Personal Information Protection Act, recognizes the unique vulnerabilities of children in the school setting, and flatly prohibits the sale or student's information in this context, as well as commercial profiling or use of such information for targeted marketing.[10]

Section # 9 - Geolocation:

Code summary: "Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, taking account of the best interests of the child), and provide an obvious sign for

[8] Arthur, Charles, "Why the default settings on your device should be right first time" 2013

[9] Jim Steyer's testimony at United States Senate Committee on Commerce, Science, and Transportation Hearing on "Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework," May 1, 2019

[10] Student Online Personal Information Protection Act of 2013

children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session."

We agree that geolocation tracking is a particularly invasive practice and applaud the ICO's suggestions to limit its use. We believe that the carve out for compelling reasons, taking into account the best interests of the child, allows for flexibility when a child is intentionally using a geolocation-focused app such as a map. We would note that there are additionally invasive tracking methods, such as via video camera or audio recording, and these should also be off unless a user intentionally turns them on (unless there is a compelling reason, taking account the best interest of the child),, and should always be paired with some obvious indication to the user that such recording is taking place. This type of tracking often comes up in connected devices, see below for additional comments regarding IoT.

Section # 11 - Profiling

Code summary: "Switch options which use profiling off by default (unless you can demonstrate a compelling reason for profiling, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing)."

We applaud the ICO's proposal to prevent profiling by default, absent a compelling reason. We believe that that certain profiling, such as commercial profiling used to target advertisements, will never be in the best interests of a child. We support bipartisan legislation introduced by Senators Markey (D-Ma) and Hawley (R-Mo), an update to COPPA, that would prohibit behaviorally targeted advertisements to kids under 13. It would also prohibit profiling based on race, ethnicity, or other proxies.[11]

In the U.S. and UK, we are working to improve the media landscape for kids including creating an environment where children are not fed information that is detrimental to their health or well-being. We need updated legislation to protect the well-being of kids and generations to come. We also believe that while it is important to protect children from harmful content, we should also seek to incentive enriching, positive content as well. We seek to inspire the creation of more educational programming that teaches our kids to be critical thinkers and life-long learners, and are working the the U.S. Congress and at the Federal Communications Commission to find ways to incentivize high quality children's content creation.

Section # 12 - Nudge techniques

Code summary: "Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off their privacy protections, or extend their use."

[11] COPPA 2.0 - Legislation to Update Children's Online Privacy Rules

We commend the ICO for recognizing that nudges can have multiple harmful effects on kids, including extracting personal information from them as well as encouraging compulsive usage. As mentioned, we support the DETOUR Act which would prohibit companies from design practices that encourage compulsive usage in kids. It would also prohibit companies from using design features and nudges that subvert user choice and autonomy, including those that trick people into giving more information.

Dark patterns refers to the use of design techniques that are intended to trick or subvert user choice. Companies build user interfaces using dark patterns that employ techniques based on extensive behavioral psychology research and often mislead users into agreeing to settings or practices. While adults fall prey to these techniques, children are especially vulnerable to platforms that employ dark patterns and could unknowingly make purchases, divulge information, or agree to an exploitative setting.

Oftentimes games will use beloved characters or hosts to shame children into purchase or extended gameplay. Games also create confusing interfaces where it's hard for children to discern the difference between content and advertising or a link to make a purchase. Platforms that automatically extend viewing by serving up unrequested content, sometimes even before the requested content is concluded, can trap families into extended viewing sessions. In some cases, designers engineer games with artificial difficulty curves to induce children to spend money on upgrades simply to progress. These games are often offered for free, enticing players to download and even offering them a false sense of progression upon initial download before artificially increasing difficulty to induce compulsive purchases. In other cases, designers create multiplayer games offering players who purchase paid upgrades competitive advantages over other players.

All of these techniques are design choices made to benefit the platform or app companies with purchases, data or extended use.

Section #13 - Connected toys and devices

Code summary: "If you provide a connected toy or device ensure you include effective tools to enable compliance with this code."

We are pleased to see the ICO recognize that specific protections and provisions are necessary for Internet Of Things/Connected Devices as much information collection is moving off of screens and into physical devices, immersing children and families often without their full realization, understanding, or awareness. These devices may be used by pre-literate children, and are often in sensitive locations (like physically on the body or in bedrooms) with potentially unlimited information gathering capabilities. Companies often are in a rush to market, with privacy and security being an afterthought. The combination of insecurity, interconnectedness, and massive (and often unexpected) information collection makes Connected Devices particularly concerning for children. We think it is especially critical for connected devices to provide information at the point of purchase--before an adult has purchased and opened a toy and may not be able to return it--as well as to minimize passive information collection and be clear with users about when

information collecting is occuring (such as lights or other indicators when microphones are working).

In fact, these are protections we sought in California for connected devices with SB 327,[12] which would, as initially proposed, have required disclosures of information collection practices (specifically whether the device collects personal or sensitive information, and how to obtain security updates) at the point of sale, user consent before the device could transmit information not needed for its state function, and requires manufacturers to equip devices with reasonable security features. The bill was narrowed due to industry pressure, but the reasonable security provisions made it into law. We have also worked on direct appeals to industry with partners such as Mozilla, asking for secure connected products[13] and for retailers to stop stocking insecure devices.

Education and Awareness is Critical

One final comment is how critical it is to educate companies, caregivers, and children themselves (to the extent it is age appropriate) about this code and about privacy and data protection. Families especially must be educated about online tools and parental controls, and what they can do to protect themselves and their children, as well as what companies complying with the code are doing to protect their children. By changing expectations, individuals will begin to demand more and--when companies meet these demands--trust more the sites and services that children are growing up with on a daily basis.

Additionally, because the media content children consume has a profound impact on their social, emotional, cognitive, and physical development, it is essential that children learn how to use media and technology safely and responsibly. That is why we encourage Digital Citizenship, a curriculum Common Sense developed, be taught in schools. We think all schools should have a dedicated curriculum that teaches core digital safety and resilience skills and habits of mind.

Conclusion

Increasingly, the lines between digital and analog are blurred--we no longer "go online" to get connected, we are connected as we move through spaces with sensors and interact with smart devices in our homes and schools. With the possibility and the risks of the offline world moving into the digital space, supporting and protecting our children is ever more critical.

Common Sense commends the ICO for efforts to support children's rights in the digital environment through its Age Appropriate Design code. We look forward to working with interested parties on actions and measures to promote and protect children's rights in and through the digital environment.

[12] Cal. Civ. Code §1798.91.04(a)(3)

[13] Mozilla, "This Valentines day all we want is products that meet minimum security standards," 2019