BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION?
PROJECT NO. P145406

COMMENTS OF COMMON SENSE MEDIA

August 15, 2014

I. Introduction & Overview

Common Sense Media, a nonpartisan, nonprofit organization dedicated to helping kids and families thrive in a world of media and technology, respectfully submits these comments in response to the Federal Trade Commission's request for comment in advance of its upcoming workshop, "Big Data: A Tool for Inclusion or Exclusion?" We applaud the Commission for examining big data and its impact on consumers.

As the FTC explores big data's ability to include or exclude, the public discourse ought to include one of our nation's most important and vulnerable groups: youth. The FTC has long been the leader in protecting kids' privacy. Now more than ever, the agency's expertise is needed to protect children and teens in a big data world.

Today's digital world offers young people limitless opportunities to create, communicate, connect, and learn in new and impactful ways. At the same time, our highly interconnected online ecosystem aggregates little bits of data into "big data" that may be used by unintended audiences in unexpected ways, and can deprive individuals of their right to self-determination. Data is amassed into extremely detailed profiles, which are used to label and steer individuals. Such ubiquitous data collection and profiling is disconcerting for everyone, but is particularly troubling for young people, who are growing up, developing, experimenting and learning in a digital world. Big data combines digital footprints into a full body scan, which can then be used to grant or deny their admission to future opportunities.

The FTC's recent Data Broker Report confirmed what many have suspected – that data brokers and other big data players are collecting, storing, mining, and sharing information about virtually every consumer – ***including children and teens.***[1] As the FTC and others have recognized, children's and teens' personal information is particularly sensitive.[2] Accordingly, we need further investigation of data brokers' practices and the ramifications of big data on children and teens. While we understand the September workshop will appropriately focus on big data's inclusionary and exclusionary impact on low-income and underserved communities, any discussion of big data is not complete without considering our nation's youngest consumers. The FTC should investigate the impact of big data on kids in this or future

---

[1] FTC, *Data Brokers: A Call for Transparency and Accountability* 21 (May 2014) ("FTC Data Broker Report").
[2] FTC, *Protecting Consumer Privacy in an Era of Rapid Change* 47, 60 (Mar. 2012) ("FTC 2012 Privacy Report"). (stating that when sensitive data such as "children's information is involved … the likelihood that data misuse could lead to embarrassment, discrimination, or other harms is increased," and that, "companies that target teens should consider additional protections."). *See also* FTC Data Broker Report at 55 (noting that principles underlying the Children's Online Privacy Protection Act may apply equally in offline contexts, and that teens often fail to appreciate long-term consequences of posting data online).

proceedings. We also need clear rules that recognize that personal information about children and teens is a sensitive data category presenting unique risks and deserving special protections in a big data world. We respectfully urge the Commission to clarify this in its legislative recommendations for data brokers.

Simply put, big data should not label and limit kids.

Imagine this:

- A student from a less affluent zip code, who can't afford a private tutor, struggles with a math-tutoring app and is labeled as "financially vulnerable."
- A child with an interest in extreme sports (discovered through web browser histories, YouTube searches, and book purchases) is categorized as a "risk-taker."
- A teenager, frequently home late (logged by the "smart" home monitoring system), who is friends with a popular crowd on social media and shares posts about parties, is categorized as an alcohol user and "socially influenced" (even if the teen doesn't drink).

Normal child and teen behavior can categorize, affecting educational options and admissions, employment opportunities, and product offers and pricing. Children and teens may suffer differential treatment, and be included or excluded, on the basis of collections of data points they do not understand and may not even know exist.

In its Data Broker Report, the Commission proposed legislation that would increase the transparency and accountability of data brokers. It recommended that consumer-facing companies obtain affirmative express consent before sharing sensitive information with data brokers for marketing products. The FTC also suggested as a "best practice" that data brokers "implement better measures to refrain from collecting information from children and teens, particularly in marketing products."[3] Given the special sensitivity of children's and teens' data (like financial and health information, and precise geolocation), collection and sharing of information from and about children and teens should—*as a matter of law*—require affirmative express consent either from parents (for children under 13) or from teens themselves. Legislation should address the unique issues presented by young people's age and level of understanding to ensure transparency and individual control over their personal information, and to safeguard against the unexpected consequences of big data used beyond the context in which it was collected.

Common Sense Media has called for legislation that builds on the Children's Online Privacy Protection Act ("COPPA") protections for personal information collected from children under 13, extends parallel protections to teens, and broadens the FTC's legislative recommendation that companies obtain affirmative express consent before sharing sensitive information with data brokers.[4] Specifically, data brokers and their sources should provide the following heightened protections before profiling children and teens:

---

[3] FTC Data Broker Report, *supra* note 1, at 55.

[4] *See* Common Sense Media, *Comments on Big Data and the Consumer Privacy Bill of Rights* (Aug. 5, 2014), *available at* http://www.ntia.doc.gov/files/ntia/common_sense_media_0.pdf.

- Consumer-facing entities that share personal information about children or teens with third parties, such as data brokers, should provide notice to their customers and should obtain affirmative express consent from either a parent (for children under 13) or the teen before they collect or share their personal information.

- If a data broker knows or reasonably should know it is collecting information from or about a child under 13, it should stop collecting, until and unless it has affirmative express parental consent.
    - To the extent data brokers collect information from or about children, it should be used only to safeguard the child, such as prevention of fraud and identity theft.

- If a data broker knows or reasonably should know it is collecting information from or about a teen, it should stop collecting, until and unless it has the teen's affirmative express and informed consent.

These recommendations are consistent with Common Sense Media's long-standing belief that online companies should provide special protection for kids and teens, and get affirmative express consent from either parents (for children under 13) or teens before collecting their personal information or geolocation, or targeting them with behavioral ads.

Children and teens should be able to explore and express themselves freely, at home, in school, and everywhere in between. They should be given the space to discover and define themselves, before big data does it for them. Failure to safeguard their personal information, coupled with widespread concern about ubiquitous corporate and government surveillance, could jeopardize the collective trust in digital technology. Users may start to self-censor their thoughts, temper their online exploration, and withhold information. This could ultimately chill the right to free expression and squelch opportunities for youth.

Strong safeguards for personal information from and about children and teens would help create a more trusted online environment, where kids can enjoy the benefits of technological innovation without fear of jeopardizing their future.

II. The FTC Should Further Examine How Big Data Is Tracking Children and Teens

A. Children and Teens are Providing Increasing Amounts of Data

A number of factors put children and teens uniquely at risk in a big data world. More data will be collected from today's youth than from any generation before. They are the first to have a digital trail spanning the length of their entire lives, if not longer.[5] They are avid adopters of new technology. And they are particularly heavy users of mobile devices,[6] which can collect

[5] A quarter of children have an online presence before being born. *See, e.g.*, Business Wire Press Release, *Digital Birth: Welcome to the Online World – AVG Study Finds a Quarter of Children Have Online Births Before Their Actual Birth Dates* (Oct. 6, 2010), http://www.businesswire.com/news/home/20101006006722/en/Digital-Birth-Online-World.

[6] Twice as many young children used mobile in 2013 than just two years prior, and 38% of toddlers under age two have used a mobile device in the last two years. *See* Common Sense Media, *Zero to Eight: Children's Media Use in America 2013* 11 (Oct. 28, 2013), *available at* https://www.commonsensemedia.org/file/zerotoeightfinal2011pdf-

sensitive data (such as geolocation) anytime and anywhere. As the FTC has recognized, mobile apps on such devices collect a plethora of information—sometimes in compliance with current law, sometimes not.[7] In school, the proliferation of educational technology and digitization of school records and activities—from nurse visits to student keystrokes—means digital dossiers that are lengthier and stickier than any paper file.

Young people seem wired to share more information. Children may not appreciate the sensitivity of what they are sharing. And teens live in a culture that promotes sharing,[8] with no signs of abatement.[9] Teens also tend to act impulsively without fully thinking through the consequences.[10] Young people often do not understand what data they are sharing and with whom it will be shared afterwards.[11]

Moreover, young people are being monitored not only in their free time, but also in school and while completing their homework. Schools are integrating more laptops and tablets in the classroom and experimenting with educational learning platforms, fingerprint-purchased meals, and digitized student records stored in the cloud. Educational technology, used wisely, has the potential to positively transform America's schools, enhancing student learning and improving school efficiency. At the same time, it brings a host of privacy concerns. As the White House's recent Big Data Report recognizes, student data can be very personal.[12] Student data can reveal academic progress, health information, disciplinary records, and even eligibility for free or reduced price meals. Thus, "[t]he big data revolution in education … raises serious questions about how best to protect student privacy as technology reaches further into the classroom."[13] The relentless tracking of students exacerbates the privacy problems already faced by children and teens.

B. Data Brokers Are Collecting Data About Young People, Online and Offline

The FTC Data Broker Report has begun to shed some light on data brokers' treatment of information about kids and teens. The FTC Report confirmed that some data brokers include information about children and teens in products they sell to their clients.[14] Others "suppress" the information related to children and teens and do not include it in their products—but

---

0/download. One in four teens are cell-mostly Internet users, versus the 15% of adults overall, and among teen smartphone owners, that number is one in two. Pew Research Center & Berkman Center for Internet & Society, *Teens and Technology 2013* (Mar. 13, 2013), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_TeensandTechnology2013.pdf.

[7] FTC Staff, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012).

[8] Ninety percent of teens have used social media. Common Sense Media, *Social Media, Social Life: How Teens View Their Digital Lives* 9 (June 26, 2012), *available at* https://www.commonsensemedia.org/file/socialmediasociallife-final-061812pdf-0/download.

[9] A recent research study found that teens' use of Facebook increased in the last two years. Reed Albergotti, *Survey: Teens Say They Are Using Facebook More,* Wall St. J. Digits Blog (June 24, 2014, 6:00 AM), http://blogs.wsj.com/digits/2014/06/24/survey-teens-say-they-are-using-facebook-more/.

[10] FTC 2012 Privacy Report, *supra* note 2, at 70.

[11] Pew Research Center & Berkman Center for Internet & Society, *Teens, Social Media, and Privacy* 2 (May 21, 2013), *available at* http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.

[12] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (May 2014) ("White House 2014 Big Data Report").

[13] *Id.* at 25.

[14] The only stated purpose of such inclusion was for fraud prevention. FTC Data Broker Report, *supra* note 1, at 21.

apparently make no effort to stop collecting, storing, and perhaps even mining, such data. And some data brokers simply rely on their sources to "suppress" information about children and teens, turning a blind-eye to whether or not they are collecting such information or including it in their products.[15]

Importantly, "suppression" does not mean deletion. Neither data brokers nor their sources have said what they do with the data when a teen turns 18. But it seems likely that they start using it then (if they haven't already). Otherwise, why keep it at all?

One rationale given for collecting or providing information about children and teens is to prevent fraud. This in itself cannot justify unlimited collection or use of child and teen personal data. Indeed, data brokers acknowledge this implicitly in instances when they "suppress," or rely on their sources to "suppress," such information for a minor.[16]

Recent reports have explained how data brokers combine data from hundreds or thousands of data points, creating an incredibly detailed profile. Even the most innocuous seeming data can end up contributing to a rich and potentially incriminating individual profile. As the White House Report explains, "integrating diverse data can lead to what some analysts call the 'mosaic effect,' whereby personally identifiable information can be derived or inferred from datasets that do not even include personal identifiers, bringing into focus a picture of who an individual is and what he or she likes."[17]

This picture becomes even more focused when data brokers combine online data with offline data. Marketers admit to using "onboarding" to target consumers online based on their offline behavior. And they appear to be doing the reverse as well—targeting people offline based on browsing patterns online.[18] We can expect more of such data merging and marketing across online and offline platforms in the future.[19]

Offline data is expected to expand exponentially with the growth of wearables, facial recognition technology, and the internet of things. As offline data collection moves from the credit-card reader to the street camera or the smartwatch, more offline data will be collected from

---

[15] *Id.*

[16] Data brokers' sources are myriad and opaque. It is doubtful that all sources are "suppressing" information related to children and teens, especially given the vast number of third-party trackers that are targeting children for advertising and profiling. For instance, in May of 2014, TRUSTe found 1,110 third-party trackers, including 644 unique tracking organizations, on the top 40 websites used by kids. TRUSTe found an average of two dozen trackers on preschool and education sites, and even more on kids' entertainment and gaming sites. Press Release, TRUSTe, New Study Finds 644 Unique Third Party Trackers (Jun. 19, 2014), http://www.truste.com/about-TRUSTe/press-room/news-study-finds-644-unique-third-party-trackers. It is unclear if these trackers provide their information to ad networks, data brokers, or both; regardless, they are all part of a sharing ecosystem. *See, e.g.*, Display Advertising Technology Landscape, LUMA Partners LLC (Dec. 31, 2010), http://cdn.theatlantic.com/static/mt/assets/science/display_advertising_ecosystem_011011-1024x741.png

[17] White House 2014 Big Data Report, *supra* note 12, at 8.

[18] FTC Data Broker Report, *supra* note 1, at 29.

[19] *See, e.g.,* Kate Kaye, *Acxiom Acquires LiveRamp to Boost Offline-to-Online Data Capability*, Advertising Age (May 14, 2014), *available at* http://adage.com/article/datadriven-marketing/acxiom-buys-liveramp-offline-online-data-capability/293212/.

children and teens. This trove of offline data will be combined with ever-more online data[20] into even more detailed and potentially intrusive personal profiles at even younger ages.

The personal and sensitive data collected about young people may include everything from social media posts (anonymous or not) to geolocation, the content of emails and texts, the hours spent on various devices, online videos, newspapers, and books, school research interests, educational app progress, metadata, in-school grades, nurse visits, food choices, health and biometric information, in-store and online purchases, friends and family, and economic background.

Given the exponentially increasing amount of data created, collected, and combined, online and offline, coupled with the dwindling amounts it costs to store and mine such data, there are few practical constraints on big data brokers. Thus, legal, ethical and other constraints are needed to ensure that young people can grow up free of constant surveillance, free of digital labeling and related limitations. These topics are ripe for further FTC examination.

C. Big Data Is Labeling and Limiting Minors in Ways That Will Have Long-Term and Little-Understood Consequences

Big data has the power to determine and decide. In addition to the FTC Data Broker Report, recent scholarship demonstrates the extent to which individuals are being scored and categorized.[21] They are labeled as everything from allergy sufferers to sports enthusiasts to unlikely to pay the bills.[22] This ranking is not limited to adults. First-graders may be labeled as drop-out risks, elementary students are being counseled on certain careers, and teens are identified as pregnant.[23]

Labeling and predictions of future behavior can occur not just on the basis of past behavior, but on the basis of algorithmic inferences. As Chairwoman Ramirez has explained, big data can label people "not because of what they've done, or what they will do in the future, but because inferences or correlations drawn by algorithms suggest they may behave in certain ways that make them poor credit or insurance risks, unsuitable candidates for employment or admission to schools or other institutions, or unlikely to carry out certain functions." She terms this "data

---

[20] Ninety-percent of data was created in the last two years. *See* Edith Ramirez, Chairwoman, FTC, Speech at the Media Institute: Protecting Consumer Privacy in a Big Data Age (May 8, 2014).

[21] *E.g.*, Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014); Pam Dixon & Robert Gellman, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future* (Apr. 2, 2014), *available at* http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf.;
Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations Majority Staff, *A Review of the Data Broker Industry* (Dec. 18, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577.

[22] Dixon, Gellman, *supra* note 21, at 8; FTC Data Broker Report, *supra* note 1, at 21.

[23] Sarah Sparks, *Data System Flags Dropout Risks by 1st Grade*, Education Week (Aug. 6, 2013), *available at* http://www.edweek.org/ew/articles/2013/08/07/37firstgrade-2.h32.html; Stephanie Simon, *Big Brother, Meet the Parents,* Politico (June 5, 2014), *available at* http://www.politico.com/story/2014/06/internet-data-mining-children-107461.html; Charles Duhigg, *How Companies Learn Your Secrets,* N.Y. Times Magazine (Feb. 16, 2012).

determinism," and has expressed concerns about "discrimination by algorithm" and "arbitrariness-by-algorithm."[24]

Other scholars have argued that algorithms are worse than arbitrary -- they are ***biased***. This is because "human beings program predictive algorithms," so "their biases and values are embedded into the software's instructions."[25]

Arbitrary and biased labeling can be extremely limiting, and have both a social and economic impact on young people's current and future lives. Predictive algorithms may show only news articles from a certain point of view. Search results may provide medical information based on a computer's assessment of likely ability to afford treatment. College pamphlets or career guides might make their way into some postal and e-mail boxes, but not others. What's more, big data and scoring systems "have the potential to take a life of their own, contributing to or creating the situation they claim merely to predict."[26] Data collectors have the power to steer people's lives and drive individual decisions in ways that are opaque and not understood. Big data's most pronounced effect surely will involve kids and teens. Data may be collected during every moment of their lives, including key formative years during their childhood and adolescence, when exploration is encouraged and desirable. Data will also be collected as they research and develop in school. As students learn, big data will be learning about them. While this can have positive benefits in the individualized education context, it is difficult to ignore the risks. This data could be viewed by unintended audiences and may result in unexpected consequences.

Imagine if a grade school student struggles with a math app. She is also clocked at turning in every test at the very end of class, always taking the full time. She is labeled as a slow learner, and put in remedial classes the next year. The school's "career counselors" come to remedial classes to talk about trade schools, not college. The ads she sees online, and the informational materials she receives in her email box and at her house all trumpet the same message. She does not go to college. She does not end up in a high-paying job.[27]

Big data knows more and more about us with each passing day, and can channel our choices, our decisions, and even our emotions, without our knowledge. For example, earlier this year we learned that in January 2012, Facebook had intentionally altered news feeds of hundreds of thousands of its users (including teens) to make them happy or sad. Who knows what other secret experiments Facebook, or a data broker the public has never heard of, has conducted on users?

Young people need to be able to safely explore and express themselves without fear of being labeled or pigeonholed by invisible, automated decisionmakers. They need the freedom to make mistakes, try new things, and find their voices, unencumbered by the looming threat of a permanent digital record.

---

[24] Edith Ramirez, Chairwoman, FTC, Keynote Address at the Technology Policy Institute Aspen Forum: Privacy Challenges in the Era of Big Data: A View from the Lifeguard's Chair (Aug. 19, 2013); Ramirez, *supra* note 20.
[25] Citron, Pasquale, *supra* note 21, at 4.
[26] *Id*. at 33.
[27] Citron and Pasquale describe another frightening scenario involving a recent college graduate: she can't get a job after graduation, gets a low "employability" score on this basis, finds only part-time work which reduces her credit score, and then suffers more because of her low credit score, never finding a full-time job. *Id.* at 32.

III. Legislative Recommendations Addressing "Big Data" Should Include Extra Safeguards for Sensitive Child and Teen Data

In order to reap the benefits of big data while also responding to its risks, we must enact laws that reflect the unique sensitivity of child and teen data and create a trusted environment for today's youth, with transparency and individual control over commercial tracking, targeting and profiling. The FTC has rightly recognized that children's and teens' personal information is sensitive and deserving of extra protections and precautions.[28] The FTC has also recognized that consumers need more transparency and control over commercial tracking, targeting, and profiling.[29] We are calling for legislation that explicitly provides more protection and control to children and teens, because of the inherent sensitivity of their personal information.

A. The Public Supports Safeguards to Rein In Corporate Tracking of Kids

There is deep public concern about this issue. Eighty-seven percent of consumers with a child in the household avoid doing business with companies they do not believe protect their privacy.[30] Eighty-nine percent of Americans believe it is extremely or very important to keep personal information about their kids private from corporate tracking.[31] And almost eight out of ten believe that companies should get permission from teens aged 13 to 15 before collecting personal information about them or sending them targeted advertisements.[32]

This public concern is beginning to translate into political consensus. There is bipartisan agreement that children should not be tracked without their parents' consent or even their knowledge, and growing bipartisan support for the notion that teens deserve similar protections.[33] And there is bipartisan agreement that student data should be used to improve

---

[28] FTC 2012 Privacy Report, *supra* note 2, at 59-60; FTC Data Broker Report, *supra* note 1, at 55. *See also* The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 15 (Feb. 2012); and White House 2014 Big Data Report, *supra* note 12, at 25.

[29] *See, e.g.*, legislative and best practice recommendations in FTC Data Broker Report, *supra* note 1.

[30] 2014 TrustE Kids Privacy Index, *supra* note 16. This is particularly problematic because not a lot of consumers *do* believe companies protect their privacy. A recent Gallup poll found that only 1 in 5 consumers has a lot of trust that businesses will protect their privacy. *See* John Fleming & Elizabeth Kampf, *Few Consumers Trust Companies to Keep Online Info Safe* (June 6, 2014), http://www.gallup.com/poll/171029/few-consumers-trust-companies-keep-online-info-safe.aspx.

[31] Memorandum from Anzalone Liszt Grove Research, Americans Concerned about Privacy from Corporate and Government Surveillance (Mar. 31, 2014), *available at* http://media.wix.com/ugd/c4876a_e8f4ee3b207344d9aac9a3403118ca9c.pdf.

[32] *Id*. By requiring teens' permission as the default, companies can allow teens to pause, consider consequences, and get more information. As the FTC has explained, setting more privacy-protections by default "can function as an effective 'speed bump' for this audience and, at the same time, provide an opportunity to better educate teens about the consequences of sharing personal information." FTC 2012 Privacy Report, *supra* note 2, at 60.

[33] *See* Do Not Track Kids Act of 2013, introduced by Senators Edward J. Markey (D-Mass.) and Mark Kirk (R-Ill.) and Representatives Joe Barton (R-Texas) and Bobby L. Rush (D-Ill.), S. 1700 and H.R. 3481. This bill would require that websites and online services directed to teens ages 13 to 15, or who know they are collecting personal information from teens aged 13 to 15, obtain their consent before collecting their personal information, including geolocation. The bill would also allow children and teens to remove personal information via an "eraser button."

education, not to sell products or amass permanent profiles.[34] Common Sense Media supports the principles that kids and teens should be free of tracking, and that affirmative express consent should be required before their personal information, including geolocation, is collected, or before profiles are created about them and behavioral advertisements served.

B. Privacy Legislation Should Require Data Brokers To Limit Collection from and about Children and Teens

The FTC Data Broker Report notes that data brokers are collecting information about minors, and the one plausible explanation for such collection is to prevent fraud. The use of a child's or teen's data for fraud prevention purposes is one thing. But in order to flag a purchase for fraud, all that is necessary to know is the age associated with the purchaser (or device or ID) making the transaction. It is not necessary to know that the purchaser is also partial to cowboy cartoons, has recently asked puberty-related questions on a health site, or is progressing in an interactive book well behind grade-level expectations, indicating a likelihood of a learning disability. Nonetheless, this information may be collected.[35]

Legislation should require data brokers to refrain from collecting personal information from or about children and teens without affirmative express, informed consent. The principles underlying COPPA, which requires parental consent before online collection of personal information from children under 13, should apply equally to information collected offline from children and information collected and compiled by data brokers from or about children.[36] Teens, likewise, deserve the opportunity to opt-in to data brokers collecting, compiling, and profiling their personal information.

Accordingly, Common Sense Media proposes the enactment of privacy legislation, enforceable by the FTC, that incorporates the following principles:

1) Consumer-facing entities that share child or teen data with third parties such as data brokers should provide notice to their customers, and should obtain affirmative, express opt-in consent from either a parent (for children under 13) or a teen before they collect or share information from or about a child or teen.[37] This is consistent with the FTC Data Broker Report's legislative recommendation that customer-facing

---

[34] *See* Protecting Student Privacy Act of 2014, introduced by Senators Edward J. Markey (D-Mass.) and Orrin Hatch (R-Utah), and co-sponsored by Senators Mark Kirk (R-Ill.) and John Walsh (D-Mont.), S. 2690.

[35] If onboarding is occurring, the device profile might also include information about local ice cream store preferences, or matinee movie visits.

[36] *Cf.* FTC Data Broker Report, *supra* note 1, at 55.

[37] The FTC Data Broker Report recommended legislation requiring that consumer-facing sources obtain affirmative express consent before they collect sensitive information, "such as certain health information." FTC Data Broker Report, *supra* note 1, at 52. Relatedly, Chairwoman Edith Ramirez and Commissioner Julie Brill also recommended that data brokers should take reasonable steps to assure themselves that their sources obtained data with notice and choice, "including express affirmative consent for sensitive data." *Id.* at 52 n.91. And Commissioner Brill separately supported "[a] requirement that the sources of data broker information used for marketing purposes provide consumer control over collection—express affirmative consent for sensitive information collection, notice and choice for other information… ." Statement of Commissioner Julie Brill, *Data Brokers: A Call for Transparency and Accountability* C-4 (May 27, 2014).

sources obtain "express affirmative consent" from consumers before sharing their sensitive information with data brokers for marketing purposes.[38]

2) If a data broker knows or reasonably should know it is collecting information from a child under 13, it should stop collecting, until and unless it has affirmative, express parental consent. This is consistent with COPPA's framework, and would prevent any backdoor methods of collecting personal information, including persistent identifiers, "finger prints," or other methods that allow for highly detailed profiles of children. To the extent data brokers collect information from or about children, it should be used only to safeguard the child, such as prevention of fraud and identity theft.

3) If a data broker knows or reasonably should know it is collecting information from a teen, it should stop collecting, until and unless is has the teen's affirmative express and informed consent.

IV. Conclusion

Big data shapes our lives in ways both large and small. It brings numerous benefits and efficiencies. But it should not be used to label or limit kids. We thank the FTC for considering how big data is categorizing consumers, and the inclusionary and exclusionary impacts of big data, in its workshops, reports, and recommendations. The particularly powerful impacts that big data may have on children and teens should be further explored and considered in these proceedings. We look forward to working with the FTC and other policymakers and stakeholders to ensure that children and teens can reap the benefits of big data while avoiding its risks.

Respectfully submitted,

James P. Steyer
CEO and Founder
Common Sense Media

[38] *See* Supplement to Statement of Commissioner Julie Brill (May 27, 2014) (summarizing Commission legislative recommendations), *available at* http://www.ftc.gov/system/files/documents/public_statements/311541/140527databrokerrptbrill.pdf