Statement of

Laura Moy, Associate Professor of Law, Georgetown University Law Center

before the Subcommittee on Oversight and Investigations of the
Energy & Commerce Committee, U.S. House of Representatives

Hearing on "Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy"

April 19, 2023

Chairman Griffith, Ranking Member Castor, and distinguished members of the Subcommittee, thank you for inviting me here today. I am Laura Moy, an associate professor of law at Georgetown University. I appreciate the opportunity to testify on the important subject of data brokers. I represent nonprofit clients on various policy matters before federal agencies, including on matters related to data brokers,[1] but I appear today in my individual capacity.

In 2018, CNN published a story about a man named Kip Koelsch who noticed that his 84-year-old father was receiving hundreds of pieces of scammy mail every week. Mr. Koelsch realized the problem was more than just a lot of junk mail when, one day, his dad called to tell him that he had won a Mercedes and a million dollars. A look at his dad's checkbook revealed that his dad had been succumbing to scams and solicitations in the mail for years. There were records of more than 3,000 checks totaling more than $10,000 a year over several years in response to both scams and manipulative solicitations from sketchy charities and political groups.[2]

Mr. Koelsch's father's problems likely started when he somehow ended up on a "suckers list" maintained by a data brokers. After a person falls for one scam, they often

[1] Last year my colleagues and I represented the Council on American-Islamic Relations urging the Federal Trade Commission to investigate alleged unfair and deceptive trade practices by multiple actors in the location data industry. https://www.cair.com/wp-content/uploads/2022/04/FTCcomplaint.pdf. This year my colleagues and I represented Just Futures Law, joined by a number of other organizations, urging the Consumer Financial Protection Bureau to use the full force of its authority under the Fair Credit Reporting Act to rein in the data broker industry. https://epic.org/wp-content/uploads/2023/02/2023-02-08-Coalition-Letter-to-CFPB.pdf.

[2] Blake Ellis and Melanie Hicken, *How to Get Off a Scammer's Suckers List*, CNN, Aug. 7, 2018, https://www.cnn.com/2018/08/07/world/data-broker-suckers-lists-invs.

end up on other suckers lists categorized by areas of vulnerability, such as people who appear to love sweepstakes or people who are highly responsive to solicitations.[3]

This is not an isolated incident. This type of widespread troubling behavior of unscrupulous data brokers was the subject of recent cases brought by the Department of Justice against multiple brokers.[4] The Justice Department alleged that over the course of several years, multiple data brokers gathered, refined, and sold lists of millions of elderly and otherwise vulnerable individuals to scammers. In one instance, executives of the company were aware that some of its clients were scammers in the business of defrauding people, including Alzheimer's patients, and that some clients had been investigated or even stopped by authorities for fraudulent practices.[5] Despite this information, the company continued to sell lists of vulnerable individuals to some of the very scammers it had been warned about.[6]

I hope this story has your attention as we talk about data brokers here today. Now I'd like to highlight there are three main points as this Subcommittee considers whether and how to take action to rein in the data broker industry:

- First, data brokers hold tremendously detailed information about all of us.
- Second, Congress must act because individuals cannot address the data broker problem on their own. And they are frustrated about this.
- Third, the booming data broker industry does real harm to real people.

My testimony here today expands on these three points.

I. Data brokers hold tremendously detailed information about all of us.

The amount and depth of information held by data brokers about us is simply out of control. This is not a new problem. It has been known and written about for many years.

For many people, when they think of the information held by data brokers, they imagine simple lists of names and addresses, and assume that there is no reason to be too concerned about this type of information as long as they are personally aware of and able to defend against the risk of being scammed. But even historical address data can be incredibly revealing. If someone has a list of every address you've lived at and when you lived there—and the same information about everyone else—they can learn

---

[3] *Id.*

[4] Alistair Simmons & Justin Sherman, *Data Brokers, Elder Fraud, and Justice Department Investigations*, Lawfare, July 25, 2022, https://www.lawfareblog.com/data-brokers-elder-fraud-and-justice-department-investigations.

[5] https://www.justice.gov/civil/case/file/1326376/download at ¶¶ 8–12.

[6] *Id.*

all about your personal history, as well as your history of relationships with people you've lived with, such as family members, romantic partners, and close friends.

In fact, the information held by data brokers runs much deeper than this. A Senate report published over nine years ago explained that even at that time, data brokers were known to collect:

- Specific purchase and transaction information, including detailed information obtained directly from retailers about items purchased, purchase history, and transaction medium alongside personal information such as name, physical address, and email address.[7]

- Health information, including about individuals' specific conditions and attributes, such as particular diagnoses and household members' weights.[8]

- Behavioral information that many people would find private, such as whether an individual uses laxatives or yeast infection products, the number of visits to the gynecologist within the past year, and the number of whiskey drinks consumed within the past month.[9]

And as the Federal Trade Commission explained in a 2014 report that it issued on data brokers, brokers do not just collect detailed individualized information and repackage it, they also "combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences."[10] Consumers are often assigned to categories identified by data brokers for the purpose of facilitating targeted solicitations. For example, the FTC described categories that highlight individuals' age, such as the "Rural Everlasting" category for single men and women over the age of 66 with low education levels, and the "Married Sophisticates" category for upper-middle class couples in their 30s with no children. According to the FTC, some categories are health-related, such as "Expectant Parent" or "Diabetes Interest." Others focus on

---

[7] U.S. Senate, Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Staff Report: A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes (2013) at 13, 16, https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a [hereinafter 2013 Senate Report].
[8] *Id.* at 13–14.
[9] *Id.*
[10] U.S. Fed. Trade Commission, Data Brokers: A Call for Transparency and Accountability (2014) at 47, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter 2014 FTC Report].

ethnicity and income, such as categories that contain a disproportionate share of low-income Latine and Black individuals.[11]

More recently, Joanne Kim of the Duke University Sanford School of Public Policy published research indicating that "some data brokers are marketing highly sensitive data on individuals' mental health conditions on the open market, with seemingly minimal vetting of customers and seemingly few controls on the use of purchased data."[12]

Data brokers also deal in highly revealing location data. In 2018, a team of journalists at *The New York Times* acquired and reviewed a database containing historical location data from more than a million phones in the New York area—presumably location data that was collected and shared by apps installed on those phones.[13] Using that location data, the journalists were able to identify individual people. They also explained how location data could be analyzed to learn intimate details about those people's private lives, such as where they worked, where they lived, and when they spent the night at another person's home. Last fall, investigations by the Electronic Frontier Foundation and Associated Press found that one broker that collects cell phone location data claims to have "billions" of data points pertaining to "over 250 million" devices.[14]

II. Congress must act to address this problem, because individuals cannot address it on their own.

Congress must take action to address data brokers. Most people are extremely dissatisfied with the status quo, but in light of the amount of information now generated in daily life, individuals are no longer able to combat this problem on their own, without government intervention.

Most people are aware that they can no longer avoid sharing massive amounts of information about themselves with unknown third parties in their normal conduct. The FTC found almost nine years ago that "data brokers collect and store billions of data

---

[11] *Id.*

[12] Joanne Kim, Data Brokers and the Sale of Americans' Mental Health Data (2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf.

[13] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times, Dec. 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[14] Bennett Cyphers, *Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police*, EFF Blog (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police.

elements covering nearly every U.S. consumer."[15] According to research conducted by Pew, 81% of adults now say they have very little or no control over the data collected about them by companies.[16] As Justice Sotomayor remarked when the Supreme Court decided the landmark Fourth Amendment case *U.S. v. Jones*, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[17] That was in 2012—some 11 years ago—and the situation since then has only gotten worse.

Even though they feel they cannot change this situation on their own, people are not okay with the status quo. On the contrary, individuals overwhelmingly express dissatisfaction regarding this lack of control. According to the same body of research by Pew, a staggering 79% of adults say they are somewhat or very concerned about how companies are using the data it collects about them.[18]

Even if persistent and well-informed individuals wanted to attempt to remove their own information from data brokers, as a practical matter, it is nearly impossible to do so. The data broker industry is opaque and generally not consumer-facing. In 2020, journalist Seth Fiegerman of *CNN Business* wrote about his efforts to eliminate his information from people-search websites the previous winter. He reflected,

> As I would learn through my brief, manic campaign in December to scrub as much of my personal data as possible and start the new year with a clean digital slate, it's hard not to feel like you're just scratching the surface of an impossibly large data industrial complex. By the end of my experiment, I felt even worse off about my ability to wrestle back control of my data than when I started.[19]

Journalist Mara Hvistendahl of *Consumer Reports* had a similar experience when she attempted to opt out of people-search services to protect herself from the possibility of harassment. She explained that even when services offer an opt-out option, "each has a uniquely labyrinthine process that's often hard to find out about, much less navigate. It

---

[15] 2014 FTC Report, *supra* note 10 at iv ("For example, one of the nine data brokers has 3000 data segments for nearly every U.S. consumer.").

[16] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, Americans & Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information at 6 (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf.

[17] United States v. Jones, 565 U.S. 400, 417, 132 S. Ct. 945, 957, 181 L. Ed. 2d 911 (2012) (Sotomayor, J., concurring) (internal citations omitted).

[18] Auxier et al., *supra* note 16 at 8.

[19] Seth Fiegerman, *I Tried to Delete Myself from the Internet. Here's What I Learned*, CNN Business, May 21, 2020, https://www.cnn.com/2020/05/21/tech/deleting-personal-data-online/index.html.

is far easier to buy the criminal records of all your neighbors than it is to scrub your personal details from these sites."[20]

Making matters worse, in the current legal and factual landscape, a great deal of information collected by data brokers will never go away. Data brokers routinely obtain information from the same sources and share information with each other.[21] This means that once an individual's information has been collected by one party, it may be virtually impossible to eliminate completely from all entities. According to the FTC's 2014 report, "Some of the data brokers store all data indefinitely, even if it is later updated, unless otherwise prohibited by contract."[22]

In light of the unavoidable nature of information sharing with data brokers, and the fact that individuals both cannot protect their own information and are deeply dissatisfied with the status quo, Congress should act. Indeed, throughout the history of U.S. law, Congress has repeatedly seen fit to establish privacy protections for information that individuals share in the course of daily life. For example, as far back as 1931, leading up to the passage of wiretap legislation, Representative Beck raised the essential and unavoidable nature of interpersonal communications, referring to wiretapping as an "indefensible violation of the ordinary decencies of private life," describing the ability of an agent "to listen to everything you may say, messages of love and affection and of sacred confidence, or of the most intimate, confidential business."[23] In 1974, when Senator Buckley pitched the legislative amendment that would eventually become the Family Educational Rights and Privacy Act, he argued that "[t]he sense of a loss of control over one's life and destiny . . . seems to be increasingly felt by parents with respect to the upbringing of their own children."[24] And in 1974, when Congress was contemplating financial privacy following the Supreme Court's decision in *United States v. Miller*,[25] leading up to the passage of the Right to Financial Privacy Act, Representative Cavanaugh lamented that, "the changing patterns of life took the possession of information about himself out of the control of the individual."[26]

---

[20] Mara Hvistendahl, *I Tried to Get My Name Off People-Search Sites. It Was Nearly Impossible*, Consumer Reports, Aug. 20, 2020, https://www.consumerreports.org/personal-information/i-tried-to-get-my-name-off-peoplesearch-sites-it-was-nearly--a0741114794/

[21] 2014 FTC Report, *supra* note 10 at 16 ("All of the responding companies reported obtaining information from other data brokers either by purchasing or under sharing arrangements.").

[22] *Id.* at 48

[23] Cong. Rec. House 2902 (Jan. 22, 1931) (remarks of Rep. Beck).

[24] 120 Cong. Rec. Senate 14,580 (May 14, 1974) (remarks of Sen. Buckley).

[25] *United States v. Miller*, 425 U.S. 435 (1976).

[26] Safe Banking Act hearings 3 at 1451 (Sept. 20, 1977) (remarks of Rep. Cavanaugh).

III. The booming data broker industry does real harm to real people.

The wealth of information collected by data brokers, our virtual powerlessness as individuals to avoid them, and the eternal nature of digital data certainly may be enough to persuade most lawmakers that something must be done about this problem. But in addition, data broker practices do real harm to real people in a multitude of ways that I have attempted to describe here.

Data brokers fuel scammers. As discussed above in the story of the Koelsch family, scammers use data from brokers to fuel mass scams. In addition, sophisticated fraudsters can use data from data brokers to target specific people for the purpose of stealing their identity or gaining access to their accounts.[27] For example, a scammer with access to detailed information about an individual and her finances could persuasively impersonate a representative of her bank in order to get her to give up information about her account over the phone. Alternatively, a scammer with detailed historical biographical information about an individual could use that information to guess the answers to an individual's security questions for the purpose of directly gaining access to one of his accounts.[28]

Data brokers enable predatory marketing. The types of lists held by data brokers described above, which frequently categorize individuals by sensitive attributes, can also be used to market predatory products that might not be considered to be outright scams but are nevertheless harmful. For example, lists containing contact information for low-income people, disproportionately low-income people of color, could be used to market predatory high-interest payday loans, sub-prime auto loans, or debt relief programs of questionable legitimacy.[29]

---

[27] Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, Vice Motherboard (Mar. 27, 2018), https://www.vice.com/en/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection; Scott Ikeda, *Major Data Broker Exposes 235 Million Social Media Profiles in Data Leak*, CSO Online, Aug. 28, 2020, https://www.cpomagazine.com/cyber-security/major-data-broker-exposes-235-million-social-media-profiles-in-data-leak/ (explaining that data leaked by data brokers online can be used in fraud and social engineering attempts).

[28] Grauer, *supra* note 27 ("'If you can get information on someone online, you might be able to impersonate them or use their credit history, or perhaps get into a password protected website if you can answer security questions about people,'" said Paul Stephens, Director of Policy and Advocacy at Privacy Rights Clearinghouse.")

[29] 2013 Senate Report, *supra* note 7 at 7; Upturn, Civil Rights, Big Data, and Our Algorithmic Future 8 (2014), https://bigdata.fairness.io/wp-content/uploads/2015/04/2015-04-20-Civil-Rights-Big-Data-and-Our-Algorithmic-Future-v1.2.pdf.

Data brokers facilitate stalking and harassment. Stalkers and abusers have also been known to make use of data brokers for the purpose of tracking down their victims and their victims' family members.[30] Even when an individual moves out of their home to escape a person who is pursuing them, they may find that their abusers are able to locate them by tracking down their relatives using data broker services.[31]

Data brokers help law enforcement agencies circumvent constitutional protections. Law enforcement agencies sometimes go to data brokers to make an end-run around the Fourth Amendment, purchasing private information that they have insufficient grounds to obtain through lawful order.[32] For example, a few years ago a journalist at the *Wall Street Journal* revealed that the IRS had been purchasing access to precise location data.[33] And last fall, investigations by the Electronic Frontier Foundation and Associated Press found that one broker that collects cell phone location data claims to have "billions" of data points pertaining to "over 250 million" devices,[34] sold access to that location data to nearly two dozen agencies.[35]

Data brokers facilitate exclusionary decision-making. For a variety of important eligibility decisions—including those about housing and employment—decision-makers sometimes rely on information obtained by data brokers that collect and aggregate records from court records databases and credit report furnishers.[36] Landlords and employers sometimes rely on reports from these brokers without even

---

[30] *See Klobuchar, Murkowski Urge FTC to Protect Domestic Violence Victims' Information Online*, Mar. 4, 2021, https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=9F40D7AE-B9C2-4363-915F-E0AF23AE6A87.

[31] *See* Mara Hvistendahl, *I Tried to Get My Name off People-Search Sites. It Was Nearly Impossible*, Consumer Reports, Aug. 20, 2020, https://www.consumerreports.org/personal-information/i-tried-to-get-my-name-off-peoplesearch-sites-it-was-nearly--a0741114794/ ("Victims of stalking or domestic violence can't even find safety by fleeing to a relative's house, because many people-search sites publish the names and addresses of family members.").

[32] David McGarry, *The Feds Are Buying Their Way Around the 4th Amendment*, Reason, Feb. 14, 2023, https://reason.com/2023/02/14/the-feds-are-buying-their-way-around-the-4th-amendment/.

[33] Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, Wall St. J., June 19, 2020, https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815

[34] Cyphers, *supra* note 14.

[35] Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget'*, Associated Press, Sept. 2, 2022, https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef

[36] *See* Comments of Upturn Re: Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security (Commercial Surveillance ANPR, R111004), Nov. 21, 2022, at 37–38, https://www.upturn.org/static/files/Upturn-FTC-ANPR-Comment-20221121.pdf.

knowing precisely what information they entail, and as a result may disproportionately lock people out of important job and housing opportunities due to historical data that is colored by discrimination. Similarly, data brokers furnish information to health insurance companies, including information on race, education, marital status, financial health, social media, bill payments, and more for the purposes of profiling individuals and making predictions about their future healthcare costs.[37]

Data brokers disseminate inaccurate information. Data brokers also often hold records that are not just detailed, but contain errors—and sometimes inaccuracies in data can result in harms to individuals. For example, inaccurate information could be relied upon by potential employers making decisions about job applicants, resulting in improper denial of employment opportunities.[38] And harms flowing from data inaccuracies may not fall equally on all people—for example, inaccuracies due to name mismatches disparately impact racialized communities, who often face a higher likelihood of these types of mismatches because of "clustering" of common surnames.[39]

Data brokers increase data breach vulnerabilities. Finally, data brokers' collection of massive amounts of private information leaves that information vulnerable to exposure by security failures. We all recall when Equifax was compromised in 2017, exposing the information of more than 147 million Americans, including social security numbers, dates of birth, home addresses, and driver's license numbers.[40] Indeed, that single breach was the subject of a number of hearings in Congress, including one held by a subcommittee of this committee.[41] The FBI later charged four Chinese military-backed attackers in connection with the Equifax breach.[42]

---

[37] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And it Could Raise Your Rates*, NPR, July 17, 2018, https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.
[38] *See* Joseph Jerome, *Ninth Circuit Issues Ruling on Spokeo: Inaccuracies Create Concrete Harms*, Center for Democracy & Technology blog (Aug. 16, 2017), https://cdt.org/insights/ninth-circuit-issues-ruling-on-spokeo-inaccuracies-create-concrete-harms/.
[39] Sarah Mancini, Kate Lang & Chi Chi Wu, *Mismatched and Mistaken*, Justice in Aging 21 (Apr. 14, 2021), https://justiceinaging.org/wp-content/uploads/2021/04/SSADataReport.pdf.
[40] AnnaMaria Andriotis & Ezequiel Minaya, *Equifax Reports Data Breach Possibly Affecting 143 Million U.S. Consumers*, Wall St. J., Sept. 8, 2017, https://www.wsj.com/articles/equifax-reports-data-breach-possibly-impacting-143-million-u-s-consumers-1504819765.
[41] Oversight of the Equifax Data Breach: Answers for Consumers, Hearing before the Subcommittee on Digital Commerce and Consumer Protection of the Committee on Energy and Commerce, U.S. House of Representative, Oct. 3, 2017, https://www.govinfo.gov/content/pkg/CHRG-115hhrg27462/html/CHRG-115hhrg27462.htm.
[42] *Chinese Military Hackers Charged in Equifax Breach*, U.S. Fed. Bureau Investigations, Feb. 10, 2020, https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020.

The Equifax breach was not an isolated incident—in the past several years, data brokers have repeatedly been responsible for breaches exposing millions of people's private information.[43] Some of this information has ended up on the dark web, for sale to fraudsters.[44] In 2020, when Social Data, a data broker that scraped social media profiles, exposed hundreds of millions of profiles through an unsecured database, a journalist at *CSO Online* explained, "this is the sort of data that scammers collate into larger 'combo files' (often traded on the dark web) as reference for elements of authenticity when engaging in attempts at fraud or social engineering."[45]

Data brokers put minors at risk. Data brokers collect information about minors. For example, researchers at the Fordham Center on Law and Information Policy looked into student data brokers several years ago and found, among other things, one data broker that claimed to be "the nation's premier provider of student marketing data" for over 40 years, with a database containing mailing addresses of over 5 million high school students, and another broker offering data on students as young as two years old.[46] In a recent data breach, the leaked information reportedly included the number, age, and gender of people's children.[47] And in 2021 it was revealed that a family safety app was selling kids' and their families' location data to approximately a dozen data brokers.[48]

As with other information held by data brokers, minors may find that that information effectively lives forever. And although the Children's Online Privacy Protection Act (COPPA) places particular obligations on operators of sites and online services that collect information from children under 13, and some companies that have

---

[43] *See* Justin Sherman, *Data Brokers and Data Breaches*, Duke Sanford School of Public Policy Blog, Sept. 27, 2022, https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/; Andy Greenberg, *Marketing Firm Exactis Leaked a Personal Info Database With 340 Million Records*, WIRED, June 27, 2018, https://www.wired.com/story/exactis-database-leak-340-million-records/ (In 2018, Exactis exposed information about millions of people, including details like religion, interests, and children's details).

[44] *Id.*; Scott Ikeda, *Major Data Broker Exposes 235 Million Social Media Profiles in Data Leak*, CSO Online, Aug. 28, 2020, https://www.cpomagazine.com/cyber-security/major-data-broker-exposes-235-million-social-media-profiles-in-data-leak/.

[45] Ikeda, *supra* note 44.

[46] N. Cameron Russell, Joel R. Reidenberg, Elizabeth Martin, & Thomas B. Norton, *Transparency and the Marketplace for Student Data*, 22 Virg. J. Law & Tech. 107, 114 (2019).

[47] Andy Greenberg, *Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records*, WIRED, June 27, 2018, https://www.wired.com/story/exactis-database-leak-340-million-records/.

[48] Jon Keegan & Alfred Ng, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users*, The Markup, Dec. 6, 2021, https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.

collected children's information have been found in violation of COPPA,[49] this law does not extend either to information about older minors or to information that data brokers have collected from sources other than directly from children, such as information collected from parents about their children.[50]

IV. Conclusion

I appreciate the Subcommittee's attention to this very important issue. I am grateful for the opportunity to present this testimony. I look forward to your questions.

[49] Of particular relevance to this hearing, in 2021 the Federal Trade Commission reached a settlement with advertising platform OpenX regarding allegations that it collected personal information, including location, from children in violation of COPPA. *Advertising Platform OpenX Will Pay $2 Million for Collecting Personal Information from Children in Violation of Children's Privacy Law*, U.S. Fed. Trade Commission, Dec. 15, 2021, https://www.ftc.gov/news-events/news/press-releases/2021/12/advertising-platform-openx-will-pay-2-million-collecting-personal-information-children-violation.

[50] 15 U.S.C. §§ 6501–6506.