CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the House Judiciary Committee

"Digital Dragnets: Examining the Government's Access to Your Personal Data"

A Testimony by:

Caitlin T. Chin

Fellow, Strategic Technologies Program, CSIS

July 19, 2022

2141 Rayburn House Office Building

Chairman Nadler, Ranking Member Jordan, and distinguished Members of the Committee:

Thank you for inviting me to submit written testimony in advance of this week's hearing on "Digital Dragnets: Examining the Government's Access to Your Personal Data." My name is Caitlin T. Chin, and I am a Fellow at the Center for Strategic and International Studies (CSIS) in Washington, D.C. As CSIS does not take institutional policy positions, the views in this statement are my own and do not represent those of my employer.

The notion of privacy from the U.S. government is engrained within the Bill of Rights. The Fourth Amendment protects individuals from "unreasonable searches and seizures," and requires government entities to obtain a warrant with "probable cause" to infringe upon their "persons, houses, papers, and effects." To determine what constitutes an "unreasonable" search, courts have drawn a line where individuals may possess a "reasonable expectation of privacy."[1] In this manner, the three branches of federal government have struck an ever-evolving balance between the country's interest in protecting national security and an individual's right to privacy.

But in recent years, this balance has fundamentally changed. Now, I observe two major trends that have materially enlarged the reach of government surveillance—without a comparable modernization in privacy legal protections.

First, technological advancements have enabled private companies to collect an extremely invasive scope of personal data from individuals, including precise geolocation, internet history, communications, audio and visual footage, and biometrics. In turn, many of these details could either directly reveal or could be used to infer sensitive information related to a person's health, finances, race, religion, gender identity, sexual orientation, familial status, and more. Society, too, has shifted online, accelerated by the COVID-19 pandemic which has normalized virtual education, employment, shopping, and social, cultural, and religious activities.[2] As a result, many individuals now utilize dozens of websites, mobile apps, and internet-connected devices each day, reaching a point where it is not possible for most Americans to access basic information or societal functions without leaving a digital trail.

Second, U.S. law enforcement and intelligence agencies have become increasingly reliant on data obtained from the private sector—both through compelled and voluntary mechanisms. Apple, Google, Facebook (now Meta), and Microsoft together received approximately 125,000 U.S. legal requests for data from January to June 2021, involving around 248,000 accounts—an increase from about 39,000 U.S. data requests, affecting 72,000 accounts, from January to June 2015.[3] But an even more problematic tendency is for U.S. law enforcement entities to circumvent the judicial process altogether by purchasing, instead of compelling, the disclosure of personal information.

[1] *Katz v. United States*, 389 U.S. 347 (1967).
[2] Caitlin Chin and Mishaela Robison, "This cuffing season, it's time to consider the privacy of dating apps," The Brookings Institution, November 20, 2020, https://www.brookings.edu/blog/techtank/2020/11/20/this-cuffing-season-its-time-to-consider-the-privacy-of-dating-apps/.
[3] Microsoft Law Enforcement Requests Report, accessed July 8, 2022, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report; Meta Government Requests for User Data, accessed July 8, 2022, https://transparency.fb.com/data/government-data-requests/country/US/; Google Global Requests for User Information, accessed July 8, 2022, https://transparencyreport.google.com/user-data/overview; Apple Transparency Report, accessed July 8, 2022, https://www.apple.com/legal/transparency/us.html.

By entering voluntary contracts with data brokers, without a court order or probable cause warrant, U.S. law enforcement and intelligence authorities are moving in a direction that enables monetary purchases of bulk data troves from private information aggregation services with significantly less judicial oversight and public transparency.

Taken together, these trends compound the need to reassess the appropriate boundaries of the U.S. government's access to personal information held by private companies. I will devote the remainder of my statement to the latter challenge—the voluntary disclosure of personal information by private companies—and ways to strengthen public transparency, judicial oversight, and privacy and civil liberties safeguards.

Warrantless Surveillance in the Private Sector

In 2018, the Supreme Court held in *Carpenter v. United States* that U.S. law enforcement authorities must obtain a Fourth Amendment warrant—not just a subpoena—to access a person's cell site location information (CSLI) over seven days, rejecting the government's argument that individuals who voluntarily disclose "business records" to third-party wireless carriers do not hold a "reasonable expectation of privacy" in that information. But the *Carpenter* decision was narrow; the Court did not comment on whether commercial data transactions, "conventional surveillance" such as security cameras, or data collection involving foreign affairs could also fall under the scope of a Fourth Amendment search.[4]

That lack of legal instruction has contributed to the current status quo: a largely underregulated environment for data brokers to voluntarily package and sell both domestic and international geolocation and other personal information to government agencies without first requesting a warrant.[5] The Department of Homeland Security (DHS) and Defense Intelligence Agency (DIA) have reportedly each issued memos which concluded that the government does not require a warrant to purchase cell phone data from private corporations, with the latter stating that: "DIA does not construe the *Carpenter* decision to require a judicial warrant endorsing purchase or use of commercially available data for intelligence purposes."[6]

In its January 2021 memo, DIA confirmed that it had funded the purchase of bulk smartphone geolocation data pertaining to individuals both within and outside the United States, and that the agency had searched the geolocation database of U.S. individuals, without a warrant, on five separate occasions in the previous 2.5 years. Meanwhile, DHS, particularly Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), has reportedly contracted

[4] Lower courts have seen divisions over the application of *Carpenter* to surveillance in other contexts. Demonstrating this ambiguity, last month the U.S. Court of Appeals for the First Circuit split 3-3 over whether *Carpenter* would require the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) to obtain a warrant to conduct pole camera surveillance outside an individual's home over an eight-month period. *See, e.g., United States v. Moore-Bush*, No. 19-1582 (1st Cir. Jun. 9, 2022).

[5] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, " Legal loopholes and data for dollars: How law enforcement and intelligence agencies are buying your data from brokers," Center for Democracy & Technology, 2021, https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

[6] Hamed Aleaziz and Caroline Haskins, "DHS authorities are buying moment-by-moment geolocation cellphone data to track people," BuzzFeed News, October 30, 2020, https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation; "Memo on Clarification of information briefed during DIA's 1 December briefing on CTD," Defense Intelligence Agency, January 15, 2021, https://www.wyden.senate.gov/imo/media/doc/011521%20CTD%20Discussion%20RFI%20Response_redaction.pdf.

the smartphone location aggregator Venntel to identify activity along the U.S.-Mexico border.[7] In fact, many federal agencies including, but not limited to, the Federal Bureau of Investigation (FBI), Secret Service, Internal Revenue Service (IRS), Drug Enforcement Agency (DEA), and U.S. Special Operations Command (USSOCOM) have purchased aggregated smartphone location data from a number of data brokers like Venntel, X-Mode, and Babel Street, which they have reportedly used for a wide range of investigatory actions related to tax fraud, immigration, and more.[8]

Apart from smartphone geolocation data, private data aggregators have also compiled and licensed extensive facial recognition databases and algorithms to government agencies, also without requiring a probable cause warrant. For example, Clearview AI has reportedly been awarded contracts with over 3,000 U.S. federal, state, and local government agencies—including the Central Intelligence Agency (CIA) and FBI—to search for and identify individuals in photos. In this manner, the private sector has significantly enlarged the range of government facial recognition surveillance; Clearview claims to have scraped over 10 billion images from CCTV surveillance cameras, social media platforms, and other public forums, while the FBI reportedly only maintains approximately 640 million photos in its internal database.[9] Most individuals are not notified that their images are collected or shared with U.S. government entities, nor that law enforcement authorities do not require a warrant to access such information.

Because data aggregation allows for an almost unprecedented range of surveillance, we must also seriously consider new boundaries on warrantless data collection in traditionally public places. For example, companies like Vigilant Solutions and Thomson Reuters sell vehicle location information through license plate imagery—inevitably sweeping up incidental data from millions of individuals who drive or park in public areas, even those who are unassociated with any particular crime or investigation.[10] On social media platforms, data miners like Palantir and Giant Oak offer commercial services that automatically scan and analyze billions of user-generated posts for keywords or other proxy variables that could help DHS and other government entities detect the small percentage that might indicate even minor illegal activity such as visa overstays, despite concerns over accuracy and impact.[11]

---

[7] Sara Morrison, "A surprising number of government agencies buy cellphone location data. Lawmakers want to know why." Vox, December 2, 2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel.

[8] Charlie Savage, "Intelligence analysts use U.S. smartphone location data without warrants, memo says," The New York Times, January 22, 2021, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html; Joseph Cox, "How the U.S. military buys location data from ordinary apps," Vice, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Bennett Cyphers, "How the federal government buys our cell phone location data," Electronic Frontier Foundation, June 13, 2022, https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data; Joseph Cox, "The IRS is being investigated for using location data without a warrant," Vice, October 6, 2020, https://www.vice.com/en/article/qj479d/irs-investigation-location-data-no-warrant-venntel.

[9] Will Knight, "Clearview AI has new tools to identify you in photos," Wired, October 4, 2021, https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/; Eli Watkins, "Watchdog says FBI has access to more than 641 million 'face photos'," CNN, June 4, 2019, https://www.cnn.com/2019/06/04/politics/gao-fbi-face-photos/index.html.

[10] "Thomson Reuters brings Vigilant license plate recognition data to CLEAR investigation platform," Thomson Reuters, June 18, 2017, https://www.thomsonreuters.com/en/press-releases/2017/june/thomson-reuters-brings-vigilant-license-plate-recognition-data-to-clear-investigation-platform.html; Conor Friedersdorf, "An unprecedented threat to privacy," The Atlantic, January 27, 2016, https://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/.

[11] Max Rivlin-Nadler, "How ICE uses social media to surveil and arrest immigrants," The Intercept, December 22, 2019, https://theintercept.com/2019/12/22/ice-social-media-surveillance/; "Social media surveillance by Homeland Security Investigations: A threat to immigrant communities and free expression," Brennan Center for Justice, November 15, 2019, https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-homeland-security-investigations-threat.

Lastly, I would like to call attention to the ways in which data brokers can reinforce racial profiling in government surveillance, building upon a well-documented history of bias in both the domestic law enforcement and national security context.[12] As recently as 2020, defense contractors that worked with U.S. military commands, including USSOCOM, reportedly purchased geolocation data from at least five smartphone apps targeted to Muslim individuals, including Muslim Pro and Salaat First, through data brokers like X-Mode and Predicio.[13] Another data aggregator, Mobilewalla, collected geolocation data from approximately 17,000 individuals who attended Black Lives Matter protests in mid-2020, sparking concerns that law enforcement officials could utilize this information to target racial equity activists.[14] In addition, ICE and CBP's partnership with Venntel, as referenced earlier, has tracked geolocation data from individuals arriving from Central or South America along the U.S.-Mexico border.[15] As I recently wrote with my former Brookings Institution colleague Nicol Turner Lee, law enforcement officials can use private-sector surveillance technologies in ways that magnify existing civil rights concerns, and the lack of legal clarity around voluntary data access escalates this potential for disproportionate abuse or targeting based on race, ethnicity, country of origin, or religion.[16]

Next Steps

There is some uncertainty surrounding the application of *Carpenter* to voluntary disclosure by data brokers. Some legal experts suggest that *Carpenter* could be interpreted to prevent the voluntary sale of geolocation and other highly sensitive information, outside the narrow circumstances of the case.[17] Other academics either take a more nuanced view or side with DHS and DIA's

[12] *See, e.g.,* "Racial profiling and Islamophobia," Brown University's Watson Institute for International and Public Affairs, accessed July 6, 2022, https://watson.brown.edu/costsofwar/costs/social/rights/profiling; Carlos Torres, Azadeh Shahshahani, and Tye Tavaras, "Indiscriminate power: Racial profiling and surveillance since 9/11," Penn Law: Legal Scholarship Repository, 2015, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1183&context=jlasc; Rashawn Ray, "How can we enhance police accountability in the United States?" The Brookings Institution, August 25, 2020, https://www.brookings.edu/policy2020/votervital/how-can-we-enhance-police-accountability-in-the-united-states/; Tom Risen, "Racial profiling reported in NSA, FBI surveillance," U.S. News & World Report, July 9, 2014, https://www.usnews.com/news/articles/2014/07/09/racial-profiling-reported-in-nsa-fbi-surveillance; Nomaan Merchant, "As national discussion on race continues, within spy agencies a call to diversify," PBS, May 19, 2022, https://www.pbs.org/newshour/politics/as-national-discussion-on-race-continues-within-spy-agencies-a-call-to-diversify; Nicole Perlroth, "Accused of Spying for China, Until She Wasn't," The New York Times, May 9, 2015, https://www.nytimes.com/2015/05/10/business/accused-of-spying-for-china-until-she-wasnt.html; Alvaro M. Bedoya, "What the FBI's Surveillance of Martin Luther King Tells Us About the Modern Spy Era," Slate Magazine, January 18, 2016, https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html; Adam Goldman and Matt Apuzzo, "With Cameras, Informants, NYPD Eyed Mosques," The Associated Press, February 23, 2012, https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques.

[13] Joseph Cox, "How the U.S. military buys location data from ordinary apps," Vice, November 16, 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Joseph Cox, "More Muslim apps worked with X-Mode, which sold data to military contractors," Vice, January 28, 2021, https://www.vice.com/en/article/epdkze/muslim-apps-location-data-military-xmode.

[14] "Warren, Maloney, Wyden, DeSaulnier probe data broker's collection of data on Black Lives Matter demonstrators," August 4, 2020, https://www.warren.senate.gov/oversight/letters/warren-maloney-wyden-desaulnier-probe-data-brokers-collection-of-data-on-black-lives-matter-demonstrators.

[15] Rani Molla, "Law enforcement is now buying cellphone location data from marketers," Vox, February 7, 2020, https://www.vox.com/recode/2020/2/7/21127911/ice-border-cellphone-data-tracking-department-homeland-security-immigration.

[16] Nicol Turner Lee and Caitlin Chin, "Police surveillance facial recognition: Why data privacy is imperative for communities of color," The Brookings Institution, April 12, 2022, https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

[17] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, " Legal loopholes and data for dollars: How law enforcement and intelligence agencies are buying your data from brokers," Center for Democracy & Technology, 2021,

interpretations, suggesting that *Carpenter* does not prohibit willing sellers from consenting to share data with the government.[18] It is possible that the Supreme Court could clarify their interpretation in future decisions—but since that outcome could take years to occur, if it happens at all, there are several steps that Congress could take to provide stronger protections for individual privacy in the near term. When presenting these recommendations, I would like to reiterate that I work for CSIS, a nonpartisan public policy think tank, and my viewpoints should not be construed as advocacy or lobbying on behalf of any specific legislation.

1) Clarify rules for government access to data held by private companies.
In the short-term, Congress could reaffirm that voluntary disclosure by data brokers and digital platforms is subject to existing constitutional and statutory constraints—in other words, should a U.S. government official wish to obtain geolocation, communications, and other sensitive data from these businesses, they must first obtain a warrant, subpoena, or court order subject to either the Fourth Amendment or statutes like the Electronic Communications Privacy Act (ECPA) and Foreign Intelligence Surveillance Act (FISA). An example of a related approach is the *Fourth Amendment is Not For Sale Act*, which proposes to prevent U.S. law enforcement and intelligence agencies from purchasing "a covered customer or subscriber record or any illegitimately obtained information."[19]

In the long-term, however, the increasing sophistication of digital data collection will likely call for a more comprehensive reexamination of traditional constitutional and statutory frameworks as well. As one example, the proposed *Fourth Amendment is Not For Sale Act* would require foreign intelligence officials to follow FISA procedures to intercept electronic communications, preventing them from circumventing this process by purchasing such information. Although this is a pragmatic first step, FISA is not a perfect permanent solution for a variety of reasons: bulk surveillance can collect large amounts of incidental, sensitive communications from U.S. individuals; most affected individuals are never notified of data collection or retention; and there are insufficient safeguards to prevent racial profiling or privacy harms.[20] To holistically reform warrantless U.S. government access to private sector data, it then becomes necessary to continuously reevaluate ways to improve transparency, accountability, and oversight of the FISA process too—including by exploring the potential role of probable cause warrants for government officials to query communications relating to U.S. individuals that were originally intercepted under FISA.

---

https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf; Dori H. Rahbar, "Laundering data: How the government's purchase of commercial location data violates *Carpenter* and evades the Fourth Amendment," Columbia Law Review, 2022, https://www.columbialawreview.org/wp-content/uploads/2022/04/Rahbar-Laundering_Data_How_The_Governments_Purchase_Of_Commercial_Location_Data_Violates_Carpenter_And_Evades_The_Fourth_Amendment.pdf.

[18] Orin S. Kerr, "Buying data and the Fourth Amendment," Hoover Institution, 2021, https://www.hoover.org/sites/default/files/research/docs/kerr_webreadypdf.pdf.

[19] "Wyden, Paul and bipartisan members of Congress introduce the Fourth Amendment is Not For Sale Act," April 21, 2021, https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-.

[20] Ashley Gorski and Patrick Toomey, "The government is using its foreign intelligence spying powers for routine domestic investigations," ACLU, February 5, 2020, https://www.aclu.org/news/civil-liberties/the-government-is-using-its-foreign-intelligence-spying-powers-for-routine-domestic-investigations; Cindy Cohn, "Foreign Intelligence Surveillance Court rubber stamps mass surveillance under Section 702 – again," Electronic Frontier Foundation, May 6, 2021, https://www.eff.org/deeplinks/2021/05/foriegn-intelligence-surveillance-court-rubber-stamps-mass-surveillance-under.

In addition, any current or upcoming legislation will require focused hearings to explore their practical implications on a broad range of companies, especially since information brokers widely vary in their data collection mechanisms, types of information, and businesses models. For example, the Committee could consider the following questions related to the *Fourth Amendment is Not For Sale Act*:

- Does the proposed prohibition on government agencies from obtaining covered records "in exchange for anything of value" prevent monetary purchases only, or does it also extend to willful, non-monetary disclosures of information to law enforcement?
- Does the definition of "covered customer or subscriber record" also protect information that is either publicly-available or that pertains to individuals who are not customers or subscribers of a service—for instance, should a data aggregator collect and sell bulk license plate images, scraped public photos or surveillance camera footage, or social media posts that reference non-users?
- What does "illegitimately obtained information" entail in the context of terms of service agreements, especially as privacy policies of mobile apps and data brokers are often vague and contain language that contemplates commercial sharing with third parties, including government agencies?

2) Federal law enforcement and intelligence agencies must increase transparency around their data collection practices.

Outside of limited oversight actions and media reports, there is a general lack of transparency mechanisms for the public to determine the full extent of voluntary data sales to government agencies. Because many law enforcement and intelligence agencies have interpreted *Carpenter* to exempt willful sales of data from Fourth Amendment warrant requirements, these contracts often escape both judicial oversight and public disclosure. In 2020, an ICE representative stated that the agency does not "discuss specific law-enforcement tactics or techniques or discuss the existence or absence of specific law-enforcement-sensitive capabilities."[21]

By taking measured steps to improve the transparency of law enforcement access to private sector data, Congress could increase accountability over any privacy and civil rights harms. First, Congress could explore requirements for federal law enforcement and intelligence agencies to directly notify all identifiable individuals who they have surveilled through the private sector—even if that data access does not lead to further investigation or prosecution. To avoid potential interference with ongoing national security probes, Congress could consider a reasonable grace period for notification after the conclusion of an investigation, and grant exceptions for disclosure that might pose demonstrable risks. Second, federal agencies should annually publish transparency and equity statements related to all methods of data access from private companies. These reports could provide a generalized public overview of the frequency and circumstances in which private sector data is accessed on a voluntary or compelled basis, the names of data brokers and categories of initial companies the data was accessed from, high-level demographic information of affected individuals, and number of data access requests that lead to an arrest or prosecution.

[21] Byron Tau and Michelle Hackman, "Federal agencies use cellphone location data for immigration enforcement," The Wall Street Journal, February 7, 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

3) Federal commercial privacy legislation must include data broker provisions.
In recent years, gaps in U.S. federal privacy law have enabled private companies, especially those in digital sectors, to build highly profitable business models around collecting, processing, and sharing personal information. In addition to placing safeguards on government access, Congress must directly curb intrusive, extraneous data collection by private companies and data brokers in the first place. Legislation such as the *Consumer Online Privacy Rights Act* (COPRA), *SAFE DATA Act*, and *American Data Privacy and Protection Act* (ADPPA) aim to impose boundaries on data collection, processing, sharing, and retention for almost all private businesses. Such limitations could indirectly reduce the possibility for third parties, including government entities, to gain access to sensitive details in ways that could unreasonably harm personal privacy.

On an important note, commercial privacy rules should more closely consider specialized boundaries for data brokers. Data brokers often collect and sell de-identified, aggregated, and/or publicly-available information—but most current proposals, including COPRA, the SAFE DATA Act, and ADPPA, would exempt at least some of these data types from proposed privacy rules, even though they could still create privacy risks or potentially re-identify specific individuals when combined with other data points. For example, several researchers successfully re-identified 2014 taxi ride data points that the New York Taxi and Limousine Commission had released in pseudonymized form, demonstrating both the need for stronger anonymization standards and the murkiness of entirely exempting de-identified data from basic privacy protections.[22] In addition, even publicly-available information—such as photos or videos taken in public areas, social media posts online, or license plate location tracking—can pose privacy concerns when aggregated on a massive scale.

As "covered entities," data aggregators would be subject to new privacy rules under a comprehensive federal privacy bill, but legislation could also go further to improve regulatory transparency into data aggregation practices. One possible measure, as the *SAFE DATA Act* proposes, would be to require data brokers to register with the Federal Trade Commission (FTC). Another approach, as the draft Consumer Data Protection Act suggested in 2018, would be to implement a single "Do Not Track" website to allow individuals to collectively opt out of extraneous third-party data sharing without individually tracking down each data broker. For these and other recommendations to curb intrusive data collection in the private sector, I recommend turning to "Bridging the gaps: A path forward to federal privacy legislation," a report that Cameron F. Kerry, John B. Morris, Jr., Nicol Turner Lee, and I published at the Brookings Institution in 2020.[23]

Thank you again for exploring this critical issue and for the opportunity to provide written comments.

[22] Marie Douriez, Harish Doraiswamy, Juliana Freire, and Claudio T. Silva, "Anonymizing NYC taxi data: Does it matter?" IEEE, 2016, https://ieeexplore.ieee.org/document/7796899; Boris Lubarsky, "Re-identification of 'anonymized' data," Georgetown Law Technology Review, 2017, https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.
[23] Cameron F. Kerry, John B. Morris, Jr., Caitlin Chin, and Nicol Turner Lee, "Bridging the gaps: A path forward to federal privacy legislation," The Brookings Institution, June 3, 2020, https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/.