Senator Grassley
Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers
Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer, IPG Kinesso

1. **There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?**

Response to Senator Grassley:

In our modern American economy, any data privacy law is also competition law. Both privacy and competition concerns have data availability, use, and control at their core. For businesses of all sizes, but especially small business and new entrants, access to data is the dependent factor on whether the business can compete or not. Companies may have better technology, better ideas, and innovation at their core, yet without access to data, they cannot compete.

Recently introduced data privacy legislation, as drafted, would have a catastrophic impact on competition because it restricts who can collect, control, and use data. This effectively picks winners and losers, consolidating market power into the hands of a few massive, Big Tech, data holders. In many ways, Big Tech is like a basic consumer utility, like water and energy. Big Tech has grown data-dominant relatively unimpeded, offering functionality to people that has become ubiquitous with our daily lives, giving these companies tremendous market power to gain consumer consent for the collection of their data.

There has been much debate about consumer consent versus other data regulatory approaches such as fair, open, and accountable data flow and use. While consumer consent is important, and a laudable goal, it alone is an insufficient model in the complex digital ecosystem of data infinity and tech certainty. Data is essential to all market players, especially small business, new business, and our innovators. By writing laws that grant control of data to a few companies that get to the consumer first, we create economic winners and losers. Such laws would effectively grant data access to some and deny it for others. This approach frustrates free and fair competition among all of the players in the ecosystem.

We are beyond the point where it is possible to pass a data privacy law that does not also – whether explicitly or by omission – affect competition. The reality is that today's connected marketplace is dominated by companies who were able to thrive and grow, thanks in part to ready access to consumer data. A comprehensive federal privacy law that in practical effect limits consumer data to just a few dominant players risks concentrating even more power in the hands of a few, giving more exclusive control of

data about people to a few. In our data-intense economy, this precludes robust competition, vibrant innovation, and the possibility of the small company becoming connected, finding its audience, and serving its audience competitively. We emphasize the essential nature of data availability, open data flow, and fair uses of data to innovation, competition, and a vibrant ecosystem of connected market participants. We contend that a federal data privacy law and a competition law should be complementary and provide for responsible and accountable data sharing so that everyone can compete on a level playing field.

We urge the Committee to consider the effect that mergers have had on control of the consumer data value chain, and thus on competition. Traditional antitrust analysis has focused on the effect of mergers in a specific consumer-facing market, but the enhancement of dominant data positions plays a large role in the acquisition strategy of the dominant online platforms. We hope this Committee will recognize the essential nature of data to our entire connected economy and the ecosystem of companies that enable our connected marketplace.

In order to protect people, promote the fair use of their data, and support a robust, trustworthy and competitive connected marketplace, a federal privacy law should be drafted in a way that protects and enables competition. It should promote fundamental privacy rights for consumers and enable responsible and accountable use and sharing of consumer data by commercial enterprises. This allows the market to continue to provide a wide array of benefits to people including things like safer online payments, ready access to business and consumer credit, access to free content and platforms, and cost efficient and effective advertising for all, especially small businesses, and new market entrants.

We at IPG have built accountability and responsible data practices into everything we do. We believe that corporate America is ready to responsibly collect and share consumer data and be accountable for its actions in doing so. We encourage the Committee to protect the fair and open use of data as fundamental to competition. We urge the Committee to help develop a federal privacy law that is future-fit for the realities of the Digital Age, protects consumers, and enables a connected marketplace in which all participants can compete fairly, so long as they engage in safe and accountable data use and sharing.

Senator Ossoff
Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers
Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer, IPG Kinesso

1. **Please list any instance where any IPG company provides or has ever provided products or services to any federal agency, or to any federal prime contractor or federal subcontractor for purposes of supporting a federal program, including the nature and value of the products or services provided. As part of this response, please describe the nature of Acxiom's 2019 contract with the United States Special Operations Command, including how Acxiom supports "Project Red Mouse." If necessary, submit a classified annex to the Committee on the Judiciary to ensure this information responsive to this question is complete**.

At the outset, it is important to note that the Interpublic Group of Companies, Inc. (IPG) is a holding company compromised of roughly 90 different companies, the vast majority of which are creative advertising agencies. For purposes of these responses, I have limited my response to the two principal data and technology companies within IPG: Acxiom and Kinesso. Moreover, given the limited availability of some historical records, the resources that would be required to undertake a comprehensive search, and my desire to respond with confidence based on records that we do have, I have limited our investigation and responses to facts going back to 2017. Kinesso was launched in 2019 and so my responses specifically applicable to Kinesso go back to that date. With that understanding, I offer the following responses to the QFRs.

Response to QFR 1: Kinesso has not provided products or services to any federal agency or to any federal prime contractor or federal subcontractor for purposes of supporting a federal program. Acxiom has performed occasional work with federal agencies, such as analytic programs with the Department of Veterans Affairs, Office of Enterprise Integration (OEI). OEI's primary goal is to utilize data and analytics to develop insights that enable VA programs to better connect with veterans and strengthen the VA's delivery of services and benefits to veterans, their families, survivors, and caregivers. The accuracy and reliability of that data is critical to the success of the mission. Acxiom serves as a subcontractor to the prime contractor and provides Data Products and Information Services as part of that relationship. (Data Products and Information Services are defined in response to QFR 7 below.)
Acxiom provides consulting services to the United States Department of State Visa and Passport Analysis Branch (VPAB) in Diplomatic Security, pursuant to GSA Schedule 70. Our relationship began with a strategic consulting assessment focused upon information assets and resources related to VPAB's Investigative Management System (IMS). IMS is the central repository and user portal for all State Department investigative cases, predominantly visa and passport fraud. Acxiom's primary goal is to assist the State Department in making IMS a more accurate and complete investigation solution for its

agents and analysts. Acxiom provides consulting services only and does not provide any Data Products or Information Services as part of that relationship.

Finally, Acxiom is not at liberty to confirm or deny the existence of any classified agreement or to discuss any other work the company may do on a classified basis for agencies of the United States Government. We recommend the Committee contact U.S. Special Operations Command or other appropriate resources within the United States Government if additional information is needed on any classified initiative.

2. **Please list any instance where any IPG company provides or has ever provided products or services to any state or local law enforcement agency**.

Response to QFR 2: Based on our investigation, neither Kinesso nor Acxiom has bid for, or provided any products or services to state or local law enforcement agencies since 2017.

3. **Please list all bids for federal contracts submitted by any IPG company, even if such bids were unsuccessful. Specify the federal agency, the title and purpose of the bid, the products or services that were to be provided, and where applicable the estimated or suggested value of the contract(s).**

Response to QFR 3: As there does not appear to be a public database or reliable comprehensive resource that tracks bidding on federal contracts, research for this question proved difficult. In addition to the work we perform for the Veterans Administration mentioned in Response to QFR 1 as a sub-contractor to Sierra7 (prior to that, the prime contractor was HMS Technologies, Inc.), we identified four additional bids to federal agencies:

Year	Agency	Purpose	Products/Services	Value	Bid Status
2018	DMDC	Identity Verification	Data and Data Processing	$275,000	Lost
2018	Login.gov	Identity Verification	Data and Data Processing	$25,000	Lost
2020	HHS	Digital Activation of Vaccine Campaign	Data and Data Processing	$625,000	Lost
2020	Defense Health Agency	Information Management	Consulting	$1.1 million	Lost

4. **Please list all bids for contracts with state or local law enforcement agencies submitted by any IPG company, even if such bids were**

unsuccessful. Specify the agency, the title and purpose of the bid, the products or services that were to be provided, and where applicable the estimated or suggested value of the contract(s).

Response to QFR 4: As indicated in response to QFR 2, we did not find any instances where Acxiom or Kinesso bid on state or local law enforcement work since 2017.

5. **Please describe any instance where any IPG company provides any product or service to any foreign governmental entity, foreign state-owned enterprise, or foreign political entity (e.g., foreign political parties, political candidates, or political campaigns).**

Response to QFR 5: Kinesso in the US has not provided a product or service to any foreign government entity, foreign state-owned enterprise, or foreign political entity since 2019. Acxiom has performed small data enhancement projects (i.e., two projects for under $100,000 total), for a Caribbean tourism authority. A sister company, Acxiom Ltd. (UK), has provided information services to the UK Information Commissioner's Office (UK Data Protection Authority). We cannot rule out situations where Acxiom or Kinesso may have provided products or services to an entity that is wholly or partially owned by a foreign government (e.g., a national airline), however, no such entity was readily apparent while we performed our research.

6. **Please describe any instance where any IPG company provides or has provided any product or service to any foreign or U.S. business for purposes of supporting that business' contract work on behalf of any foreign governmental entity**.

Response to QFR 6: It is important to note that data ethics is integral to everything we do. For more than two decades, we have focused on the sources of our data, how it is used, and whether both of those complied with law and were consistent with our ethical data framework. We have extensive systems and policies and procedures in place to make sure that this is the case. While it is possible that one of our clients used our products and services for purposes for purposes of supporting its work on behalf of a foreign governmental entity, our investigation failed to identify any instance where we knew about this type of service when it was contracted for, and we have not identified any instance since 2017 where this occurred.

7. **Please describe any relationship through which any IPG company receives personally identifiable data or any data pertaining to U.S. persons from federal, state, or local governments or government agencies. As part of this response, please describe whether data received includes information about the online presence of individuals, such as social media accounts.**

Response to QFR 7: Kinesso does not directly license personally identifiable data or data pertaining to US persons from federal, state, or local governments or government agencies. Acxiom serves as the primary data sourcing entity for Kinesso.

Acxiom has two primary lines of business. The first line of business is referred to as "information services," which includes sophisticated database administration services to improve the useability of data that Acxiom's clients provide. The second line of Acxiom's business is data products, where Acxiom provides data to its clients for their (and in the case of an Acxiom data reseller, their end users'), internal use. Acxiom licenses public records such as voter records, hunting/fishing licenses, and real estate transactions, for its data products. All of this information is publicly available, and if its use is restricted in any way by a statute or by the licensor, we conform our use and distribution of that data with those restrictions and our own guidelines.

8. **Please describe in detail the sources from which Acxiom or other IPG companies obtain unique device identifiers, including IMEI, IMSI, MAC addresses, or IDFA/Ad-IDs.**

    a. **If you receive or obtain unique identifiers from commercial partners, please describe the means by which those partners obtained the identifiers.**

Response to QFR 8: Acxiom and Kinesso collect Mobile Ad IDs (MAIDs) via a licensed file from SDK providers. We do not receive lat/long or IP addresses in combination with those MAIDs. We do not incorporate the MAIDs into any other product, but we do provide them to third parties as a data product. Consistent with our overall ethical data framework, we require that the source of this information represent and warrant their compliance with laws and applicable industry practices when they provide us the data and we have a program in place to confirm that their sources have not changed and these fundamental representations remain in place on an annual basis.

9. **Please describe efforts by any IPG company to link unique device identifiers with the IP addresses of residential or commercial internet connections.**

Response to QFR 9: Acxiom and Kinesso have not traditionally offered this type of product, nor do we currently have any commercial offerings where we link device identifiers to IP addresses. Given client interest and demand, we are exploring this potential opportunity from a commercial and regulatory perspective. If we decide to move forward and offer a commercial product that links unique device identifiers with IP commercial or residential addresses, it will be legal under all applicable laws and will also comply with our ethical data framework, which verifies the source and the intended use of the data on a client- by-client basis.

10. **Please describe any products or services any IPG company offers to clients to enable them to see connections between personally identifiable data, such as SSN, home address, email address, or telephone number, and sensitive data, such as web browsing activity, web search history, or purchase history.**

Response to QFR 10: Acxiom offers its "Real Identity" product, which performs a valuable function for Acxiom's clients. Real Identity allows Acxiom's clients to synchronize identity data (e.g., name, home and email address, and telephone number) used across the client's enterprise. By synthesizing and analyzing billions of customer transactions and interactions, both digitally and offline, Real Identity allows Acxiom's clients to build and maintain first-party identity graphs to recognize individuals and build deeper customer relationships across their full enterprise.

Importantly, this service is only used to build first party data graphs for our clients, the data flowing through this service is not added to any Acxiom third-party data graph. So, whether it is the client using the product on its own behalf or Acxiom providing those services as the client's processor, the client's own data or ethically sourced, third-party data licensed by our client is used to make these connections in accordance with the client's own privacy policy and the client's notice to consumers of the potential for re-identification.

Lastly, it is also important to state that Acxiom and Kinesso do not offer products or services to clients that enable them to see connections between personally identifiable data and sensitive data, such as SSN, web browsing activity, or web search history, that is not already in their possession. Acxiom does license consumer purchase behavior data that is associated to personally identifiable information. However, that data is categorical (e.g., clothing, hardware); not at an item/SKU level of granularity, nor is it associated to the specific location that the purchase was made.

11. **Please describe any contractual limitations Acxiom places on entities' use or disclosure of data about individuals.**

    a. **Does Acxiom monitor its clients for contract adherence? If so, how?**
    b. **Has Acxiom or any other IPG company discovered or become aware of a contracting partner's contractual breach relating to personally identifiable information? If so, please describe any resulting actions taken by IPG or an IPG company.**

Response to QFR 11: Acxiom's client contracts require clients to comply with all applicable laws and restrict the use of data and services for client to internal business purposes. Acxiom includes similar flow-down obligations through restrictions in its contracts with resellers and data brokers (so that their customers are subject to the same restrictions). This is central to how we conduct our business and how we have conducted it over the last three decades. It is part of our internal ethical data framework.

In addition to contractual restrictions, Acxiom has a due diligence team that confirms who our client are and what they do (to the extent, their business can be determined). That team also reviews compliance with our client contracts, including data use provisions in the contracts. It is impossible to confirm compliance with every client contract, so reviews are done on a systematic basis to sample compliance across our

user base. We also follow up on any credible information we receive regarding potential non-compliance with our agreements.

Acxiom has business interactions with many clients that can be described as “high touch” and “long-term” information services. In these situations, Acxiom has a close working relationship with the particular client over a long period of time. These types of relationships afford greater visibility into the manner in which the client uses our products and services, allowing greater confidence regarding their compliance with contractual restrictions in those situations.

12. **Other than its website, what steps does Acxiom take to alert consumers to their ability to opt out of the company’s use of their data?**

    a. **Do you treat opt-out requests from California residents differently than opt-out requests from residents of other state?**
    b. **If so, please describe any differences in how Acxiom would treat data about a person from California after receiving an opt-out request, compared to how it would treat data about a person from another state who submitted an opt-out request.**

Response to QFR 12: Acxiom provides CCPA rights to all individuals in the United States. Acxiom does not treat California residents differently from an opt out (or any other data rights perspective), than any other resident of the United States.

Acxiom works hard to provide as much educational information to consumers as possible. We have extensive information available on our website, but in addition, we promote consumer awareness in media interactions and in consumer oriented educational activities (e.g., conferences, seminars, and consumer group sponsorships).

Senator Tillis
Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers
Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer, IPG Kinesso

1. **The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. How would you define "data" and "big data", as used in your written testimony?**
    a. **How would you define consumer and user data, specifically what would be included and excluded from these definitions?**
    b. **Would this include user uploaded videos, images, and text?**
    c. **Would such content be considered part of the "user" data, even if it includes content that originates from other sources?**
    d. **Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?**

Response to Senator Tillis**:**

The fact that humans use data in so many different ways is part of what makes legislating with respect to data issues so difficult. Policymakers generally want to preserve and foster beneficial data uses while limiting harmful ones. The unique purpose for which data is being regulated should help define the term – and different inclusions or exclusions may be needed within the scope of a single bill.

You specifically asked how I would define the term "data" "as used in my written testimony." I was asked to testify about how my company competes in data-driven marketing as compared to others, specifically first-party platforms. The main data that matters for the purposes of that competition is not user-generated content, such as you describe above. Such data may be of interest to others, but not to us. However, user-generated digital history – product search information, for example – is useful for marketing, and therefore access to it is relevant to competition issues. Again, Congress should consider the purpose it intends to effectuate in determining the scope of defined terms.

Data may be protected by intellectual property rights in and of itself, or it may be processed by use of algorithms or processes that themselves constitute IP, in which case the resulting product may contain protectable IP. However, IP protections are not incompatible with any of privacy, competition and the enforcement of antitrust laws.

2. **Your testimony advocates for an expansive view of competition law that would account for the flexibility to account for data-related issues, and advocates for the Committee to consider privacy and competition to be interrelated.**

a. **Would the same consideration be extended to other "big data" issues, such as intellectual property rights, cybersecurity, national security, data protection, and other issues?**

b. **How should antitrust law be tailored to appropriately account for privacy rights, or other legitimate concerns such as intellectual property rights?**

Response to Senator Tillis:

I did advocate for the Committee to consider privacy and competition to be interrelated, and in the context of the hearing, which related to S. 2992, I stand by that recommendation. I did not, and did not intend, to advocate for an expansive view of antitrust law, and therefore underscore my suggestion that the Committee "consider privacy and competition not as separate bodies of law, but instead to be interrelated." A better statement would be that in the context of this legislation, antitrust and privacy become interrelated. If Congress is going to regulate competition, it should consider the privacy implications of doing so, and vice versa. Congress should consider the other interests you mention, as well.

The ability to access data that consumers are making available about themselves is key to competition in today's markets. Legislation that would regulate competition in digital markets must recognize this, and so must legislation that would protect privacy by regulating use of consumer data.

3. **Ms. Slaiman advocates for "a digital regulator to comprehensively [regulate] the policy questions surrounding digital platforms."**

   a. **Do you agree that this is necessary?**

   b. **Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?**

   c. **Is it important to you that the regulator should be politically accountable?**

Response to Senator Tillis:

We support enactment of a national privacy law, with enforcement by the FTC and state attorneys general. We also support resourcing the FTC appropriately to conduct this expanded mission. We do not have a position on whether it is necessary to have a regulator specific to digital platforms.

For privacy regulation, the best situated agency is the FTC, because it has developed experience and expertise. We do not oppose creation of a Bureau of Privacy in the FTC. Privacy regulation primarily impacts the commercial sector, and as a commercial regulator, the FTC is well-positioned.

I would also add that, as demonstrated by the August 11, 2022, FTC Advanced Notice of Proposed Rulemaking, federal legislation is necessary to prevent FTC overreach and to ensure that the FTC develop rules pursuant to congressional authorization and consistent with congressional intent.

Senator Blackburn
Questions for the Record – Big Data, Big Questions: Implications for Competition and Consumers
Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer, IPG Kinesso

It's imperative for the U.S. to get a national consumer privacy law in place – the EU and China have already done so. Given consumer concerns about how their data is being used online, what should that regime look like? What are the obstacles the United States faces in getting to that point?

Response to Senator Blackburn:

While many proponents of a national privacy law point to the EU General Data Protection Regulation as a model for the United States, Congress can, and should, do better. Studies since the GDPR went into effect in 2018 make clear that the GDPR has had a severe negative effect on the European economic market, including suppressing competition and consolidating market power into the large gate-keeper technology platforms. See, e.g., "GDPR Cost Businesses 8% of Their Profits, According to A New Estimate," https://techmonitor.ai/policy/privacy-and-data-protection/gdpr-cost-businesses-8-of-their-profits-according-to-a-new-estimate. It is also clear that the GDPR has not been able to adjust to the rapid change of innovation. In part for these reasons, both the European Union and the UK are already considering a major overhaul of their GDPR legislation. "UK Pauses Data Reform Bill to Rethink How to Replace GDPR," https://techcrunch.com/2022/10/03/uk-data-reform-bill-replace-gdpr/. In fact, GDPR has had such anticompetitive effects that the EU has introduced five additional pieces of legislation to attempt to better govern the big gatekeepers and the realities of data and algorithms in the Digital Age. "A Europe Fit for the Digital Age," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en. The EU's difficulties with GDPR demonstrate that it should not serve as model for the U.S. Contrary to GDPR, U.S. privacy legislation should protect data-driven business practices, while providing meaningful redress to Americans who suffer actual harm through violation of their privacy rights.

The U.S. should restore its leadership role on the global stage with a forward-thinking, future-fit approach. Congress should consider a bill that focuses on harm prevention and accountability. The law should prohibit certain uses of data that are per se unfair, such as fraud, unlawful discrimination, stalking, and harassment, and expressly permit the collection, sharing, and use of data for beneficial uses including advertising and marketing purposes. The policy principles championed by the Privacy for America coalition are incredibly instructive and should be fully adopted in any national privacy law. https://www.privacyforamerica.com. Additionally, the Information Accountability Foundation has developed model legislation, The FAIR and OPEN USE Act, that would be better for America and better for Americans. https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-

content/uploads/2021/05/FAIR-and-OPEN-USE-Act-May-26-2021-1.pdf?time=1622546970.

The U.S. should also consider the model of Singapore, which has enacted a national privacy law that leads to accountability without unnecessarily hampering the flow of information or favoring certain market participants in the information economy over others. https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act. The law, which was drafted in consultation with The Information Accountability Foundation and the Center for Information Policy Leadership addresses the practicalities of the digital future, and ensures robust, competitive and trustworthy economy. Essentially, the law says, "let data flow for beneficial uses, but be accountable to detect and prevent harms."

In addition to adopting a harms-based approach, a federal privacy law must resolve two issues that are relatively unique to the U.S. system: state law preemption and the scope of any private right of action.

If federal privacy legislation is to ensure future a competitive digital economy, it must include a provision that broadly preempts recent and future state forays into the use of personal information for marketing and advertising. Given the importance of advertising to the U.S economy and the fact that advertising also directly subsidizes valuable services and free speech activities on the Internet, a comprehensive national privacy law should expressly indicate Congress' intent to occupy the field. Without a strong preemption provision, the national law simply becomes yet another law that companies must navigate, creating uncertainty, operational inconsistencies, and administrative costs that are passed right back to consumers in the form of increased costs of goods and services and less access to knowledge, news, and the connected marketplace. The inevitable differences in these state level laws creates administrative and financial burdens that divert important resources that can be otherwise devoted to innovation and will substantially restrict companies' ability to grow.

More specifically, a well-drafted preemption provision would expressly preempt states and state subdivisions from adopting, maintaining, or enforcing a state law or regulation that relates to the subject matter of the national privacy law or any regulation promulgated by the national privacy law. Similarly, to remove any potential ambiguity, the national privacy law should explicitly reference and preempt the California Consumer Privacy Act, as amended by the California Privacy Rights Act, Cal. Civ. Code §1798.100 et seq., the Virginia Consumer Data Protection Act, Va. Code Ann. §59.1-580 et seq., the Colorado Privacy Act, Co. Rev. Stat. 6-1-1301 et seq., the Utah Privacy Act, Utah Code Ann. §13-61-101 et seq., and the Connecticut act concerning personal data privacy and online monitoring, 2022 Ct. SB 6, as well as any regulations implementing those statutes.

The second major obstacle to a national privacy law is whether to include a private right of action, especially if that right includes statutory damages. As we saw with other state and federal statutes that include a private right of action with a statutory damage

component, (e.g., the Fair Credit Reporting Act, the Telephone Consumer Protection Act, and the Michigan Video Rental Privacy Act), lawyers brought a number of class action cases seeking astronomical statutory damages even though the consumers objectively did not suffer actual harm. See, e.g., TransUnion v. Ramirez, 141 S.Ct. 2190 (2021).

Many companies are willing to accept a limited ability to sue to recover actual damages, provided the resulting privacy law includes a corresponding strong preemption provision. Without a correspondingly strong preemption provision, companies have continued exposure to causes of action under state law that likely include significant administrative penalties under those laws (e.g., the California Privacy Rights Act), as well as class action lawsuits for statutory damages under state laws. Such a situation is untenable and would undo any efforts by Congress to institute and enable digital innovation, while protecting privacy and competition.