# Sheila Colclasure

## Testimony to the Senate Judiciary Committee
## Subcommittee on Competition Policy, Antitrust, and Consumer Rights

## Big Data, Big Questions: Implications for Competition and Consumers
## September 21, 2021

---

### Executive Summary of Testimony

Sheila Colclasure is the Global Chief Digital Responsibility and Public Policy Officer for Kinesso, an IPG company. Sheila and IPG support national competition and data privacy laws that enable fair and open use of data, require accountability of companies that collect, process, share and use data, and ensure robust protection for individuals and their data.

### Witness Background

As Global Chief Digital Responsibility and Public Policy Officer, Sheila leads the global data policy and digital responsibility strategies for Kinesso, ensuring that data and digital technology are used ethically and accountably across the enterprise and with its parent company, IPG, and their clients. This means ensuring data and technology are used in ways that serve people. She helps ensure practices operating at the leading edge of digital technology are consistent with principles of responsible, respectful, proportionate and fair data use. Sheila is responsible for public policy engagement with regulators, policy groups, clients and other key stakeholders globally, advocating for ethical advertising and marketing practices in ways that earn trust. She is an advisor on the development and deployment of Kinesso's data-driven and digital solutions and services. She is a trusted thought partner, advisor, and reputational champion for IPG companies.

Ms. Colclasure is a recognized global thought leader on applied data ethics, accountable data governance and human-centered digital responsibility. Sheila has extensive knowledge of laws and societal expectations governing the collection and use of information, with particular depth in the rapidly evolving data-driven advertising and marketing ecosystem. She is continuously sought out by policy makers, regulators and government agencies for her views on data integrity and how to address the complexity of operationalizing and harmonizing next-generation data governance for the global digital data-driven ecosystem. Sheila is a Presidential Leadership Scholar and was recognized by CSO as one of the "12 amazing women in security" (2017).

She is a frequent speaker and media interviewee and has advanced data leadership and policy with the marketplace, regulators and lawmakers in many fora, including the Department of Health and Human Services' Datapalooza, the Attorney General Alliance, Dublin Tech Summit, Global Data Transparency Lab, Information Accountability Foundation Digital University for Regulator Series, and Ibero-American Data Protection Network. Sheila has presented key talks at global events for the Consumer Electronics' Show, Forrester, adExchanger, International Association

of Privacy Professionals, Healthcare Information and Management Systems Society, Digital Advertising Alliance, American Bar Association and the Marketing Sciences Institute.

Sheila serves on the advisory board of the Information Accountability Foundation (IAF) and is corporate liaison to several industry standards-setting groups.

## Testimony of Witness

### 1. Introduction of IPG

Kinesso, Acxiom and Matterkind, and our parent company, IPG, provide marketing services for many of the largest brands in the world. We believe that marketing done ethically, fairly and subject to accountability connects people to brand value, creates community, democratizes knowledge and access, and is a vital economic engine. This guardianship requires that marketing be done in a transparent, accountable, and trustworthy manner.

Taking a proactive approach to the ethical use of data is at the core of how we deliver products and services to our clients. We start with the application of the design principles of security, privacy, and ethical data use in the planning, engineering and deployment of our marketing products and services. This is our North Star, and our approach includes processes that facilitate security, compliance with data protection and privacy requirements, accountability, and the trusted use of data. We continuously seek ways to advance thought and practice leadership within the marketing and advertising industry.

### 2. The U.S. Economy Depends on Data for Innovation and Growth

a. Consumer Data and Technology Fosters Innovation, Transformation, and Growth

First and foremost, consumer data and technology are fundamental to the global economy. The United States is home to many of the most innovative data-driven and technology-enabled companies in the world. The U.S. is also home to large online ecommerce and social media platforms that combine the benefits of consumer data and technology, thereby changing the competitive landscape for publishers, advertisers and independent data providers. As data has become ever more central to the modern economy, multiple states in the US have adopted, or are considering, privacy laws that will significantly impact today's data-driven, competitive dynamics in ways that are both intended and unanticipated.

Rather than restricting consumer data usage in a manner that stifles innovation and picks economic winners and losers, we support national competition and data privacy laws that (i) enable fair and open use of data, (ii) require accountability of companies that collect, process, share and use data, and (iii) ensure robust protection for individuals and their data. It is vitally important for America to have national competition and data privacy laws that are well-balanced, future-fit, good for people, good for our economy, and good for America's globally competitive position. We cannot burden shift accountability to people, stifle innovation, or write laws that prevent fair, responsible, and accountable uses of data in critical ways that benefit American consumers and businesses alike.

For at least the past two decades, data driven companies in the U.S. have generated tremendous innovation, benefits for people, and benefits for our economy. Technological advances have improved Americans' lives, enabled consumers to perform more of their daily activities online,

and created more access for people to products, goods, services, and knowledge. The connected marketplace and economy became even more vital to American people during the COVID-19 crisis. This shift from brick and mortar to connected commerce was enabled by data, and as a part of this acceleration, generated increasing amounts of data. Given the breadth and depth of the connected ecosystem, it is fair to say that the health of the data ecosystem, and fair competition within that ecosystem, are critical to maintaining the economic leadership position of the United States.

Just a few examples of the dynamic innovation and competition in the digital ecosystem include:

- Connected Advertising: Innovation requires companies to try new things. Independent data providers and technology companies pioneered Internet advertising as we know it today. They invented real time online ad space auctions and developed the technology, standards, and protocols on which those auctions run today, powering much of the consumer-driven internet. This is now estimated by Statista to be a $378 billion market and projected to reach $646 billion by 2024, shaped and led by U.S.-headquartered companies. This advertising market is also the engine that enables the distribution of much of the valuable content online, which has put more information in the hands of more people than ever before. Connected advertising and independent data enables small businesses to compete in the connected marketplace and enables new market entrants to find audiences for their products and services.

- E-Commerce and Digital Payments: Fraud-detection and identity-verification tools, which enable online commerce, rely on robust and accurate data to protect businesses and consumers. These tools enable consumers to safely conduct transactions and make payments whenever, wherever, and however they want, with confidence that their identity and wealth will not be commandeered by online fraudsters. At the same time, companies that sell their goods online and companies that manage online payments must be able to detect fraud and confirm the identity of the consumers with whom they are doing business. The combination of technology and the free flow of consumer data across the internet are critical tools both for online commerce and payments and for companies providing those goods and services.

- Personalized Marketing: U.S. companies developed the all-in-one solutions that enable speakers and organizations to communicate directly with consumers via email, text, and other digital channels. The defaults on how information about people is used must be set at “benefits on” rather than “benefits off,” while also enabling consumers robust rights to transparency, choice, and other important controls over their data. Laws and regulations should support, rather than stifle or block the fair, open and accountable flow of information, payments and commerce, across the internet.

The combination of technology and consumer data allowed publishers to benefit from their own content, advertisers to benefit from tailored ad placement and campaign measurement, and consumers to benefit from the new products and services whose emergence and growth was accelerated through more personally relevant advertising and messaging. As the market evolved though, online ecommerce and social media platforms have become increasingly dominant in the technology aspects, audience aspects, and control of the online advertising marketplace that enables the connected marketplace. The size, volume and control of consumer data generated within their platforms may create natural limits on the ability of third parties to curate audiences, serve their own customers, and compete in and benefit from that marketplace.

b. Independent Data Providers Play a Key Role

Independent data providers play a key role in maintaining the competitive, vibrant, and innovative technology and data ecosystem the U.S. now enjoys. They collect consumer data from a variety of sources and make it available to other companies, subject to contractual protections, for responsible uses. This facilitates commerce and innovation that drives value for citizens and companies alike.

A good example of the power of combining consumer data and technology is customer relationship management (CRM) systems, which are virtually ubiquitous in corporate America. These systems allow companies to know who their customers are and manage customer needs and preferences on an individualized basis. Similar systems have been developed in other arenas (such as HR and marketing) to identify and communicate with individuals (who may be employees or prospects), manage their preferences and satisfy their requirements. Without accurate, robust and curated consumer data though, these technologies are unable to identify relevant individual citizens, develop appropriate communications for a particular citizen, and measure the effectiveness of those communications, while at the same time implementing the citizen's privacy, communications and data preferences.

**3. Privacy Laws Should Be Drafted to Enhance the Flow of Responsibly Sourced Data Which Fosters Innovation and Competition.**

Regulatory approaches to privacy thus far have not considered the potential impacts of data use restrictions on competition. Instead, U.S. and EU privacy laws have taken a "pure privacy" approach, with the apparently singular goal of further restricting use of consumer data. Responsible data collection and use is critical for citizens. Such principles must be implemented in a manner that promotes innovation and competition. This is best explored by considering (a) why data is important for competitive markets, (b) the (perhaps unintended) anti-competitive consequences of laws that focus myopically on data use restrictions, and (c) U.S. merger policy that impacts data-driven markets.

a. Data Sharing is Key for Competition because Data is "Non-Rivalrous"

Data sharing is particularly important at the intersection between privacy and competition. Data is what economists call a "non-rivalrous good." Company A and Company B can use the same data set at the same time. It is fundamentally different than a physical asset, such as a pair of shoes – if one person is wearing the shoes, no one else can wear them.

The ability to share data, rather than limiting its use to only one entity, thus simultaneously supports both innovation and competition. Independent data providers, for instance, can provide accurate, lawfully gathered and maintained consumer data to multiple companies, for responsible, fair, and legitimate uses. Multiple companies, for instance, can draw on a consumer data set to reduce fraud, and use that same data to advertise useful products and services, resulting in better service to people, and better economic and communications results. Those companies then compete against one another, but only to the extent they each have sufficient access to consumer data with which to do so.

When dominant players are able to maintain exclusive control over vast amounts of consumer data, it tends to enhance their market power and create barriers to entry. Exclusive control over data can provide an incumbent with critical economies of scale and scope, allowing them to raise product quality and attract consumers at lower cost than competitors. In contrast, lack of access

to that data constitutes a barrier to entry, expansion and innovation by smaller competitors. As the influential Stigler Committee on Digital Platforms observed in 2019, exclusive control over data tends to make the strong stronger and the weak weaker.[1]

Rules that unreasonably restrict the use or sharing of consumer data can exacerbate these concerns by transforming data into a rivalrous good. The General Data Protection Regulation adopted by the EU in 2018 (commonly known as the GDPR) gives preferential treatment to "first parties" – a company that collects consumer data directly from a consumer. The GDPR sets strict limits on beneficial consumer data uses by "third parties," such as companies that rely on consumer data they receive from independent data providers. The GDPR rules give the first parties control of consumer data. These are often larger and entrenched competitors who are given a major competitive advantage over third parties who may be smaller or nascent competitors. Under this regulatory approach, a company's position in the data ecosystem can perhaps outweigh its ability to innovate and provide better products and service.

b. The GDPR Experience Shows the Potential Negative Effects of Privacy Laws on Competition

The evidence is now in. The GDPR has harmed competition in the name of privacy protection. While it has increased protections for personal data in the EU, it has simultaneously undermined competition, and this has entrenched the dominant players in many online markets.

According to multiple observers, the GDPR helped the largest platforms become more dominant, while making it more difficult for smaller companies and new market entrants to survive. The Wall Street Journal[2], Politico,[3] and the New York Times[4] have all reported that the GDPR primarily benefitted Google and Facebook, while hurting smaller competitors in the online advertising industry. A survey conducted by Ghostery and Cliqz, two providers of cookie-related services, found widespread belief that "Google is the biggest beneficiary of the GDPR," while third parties, such as smaller and mid-sized online advertising companies, were the biggest losers.[5]

Academic experts Michal Gal and Oshrit Aviv have written the most comprehensive study of the effects of GDPR on competition. They wrote in 2020:

---

[1] STIGLER COMM. ON DIGITAL PLATFORMS, FINAL REPORT at 40 (2019), available at https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler%20center.pdf ("Barriers to equivalent data resources, a side effect of not having the history, scale, or scope of the incumbent, can inhibit entry, expansion, and innovation. The same effects that drive the quality of digital services higher as more users join—a positive feedback loop—makes the strong stronger and the weak weaker.").

[2] Nick Kostov & Sam Schechner, *GDPR Has Been a Boon for Google and Facebook*, WALL ST. J. (June 17, 2019), available at https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219.

[3] Mark Scott et al., *Six Months in, Europe's Privacy Revolution favors Google, Facebook*, POLITICO.COM (Nov. 23, 2018), available at https://www.politico.eu/article/gdpr-facebook-google-privacy- data-6-months-in-europes-privacy-revolution-favors-google-facebook/.

[4] *How Facebook and Google Could Benefit from the G.D.P.R.*, NEW YORK TIMES (Apr. 23, 2018), available at https://www.nytimes.com/2018/04/23/technology/privacy-regulation-facebook-google.html.

[5] Björn Greif, *Study: Google is the Biggest Beneficiary of the* GDPR, CLIQZ.COM (Oct. 10, 2018), available at https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.

> The GDPR creates two main harmful effects on competition and innovation: it limits competition in markets, creating more concentrated market structures and entrenching the market power of those who are already strong; and it limits sharing between different collectors, thereby preventing the realization of some synergies which may lead to better data-based knowledge.[6]

After studying the effects of GDPR, Professors Gal and Aviv report that these limits on competition help explain "troubling empirical evidence regarding investment in EU data-driven markets following the adoption of the GDPR," finding that the new law has had unintended effects on competition, efficiency, and innovation.

The findings of Professors Gal and Aviv are consistent with the analysis that consumer data is a non-rivalrous good. Their position is that the GDPR limits data sharing between data collectors, blocking the useful sharing of data. They further assert that the GDPR limits competition in data markets, because the law entrenches the first parties in their position of market dominance.

In short, if privacy laws focus myopically on restricting data collection and sharing, while ignoring the potential effects on competition, they are likely to harm the very citizens they set out to protect by entrenching dominant players and undermining competition and innovation. Congress should consider privacy laws that permit beneficial forms of data sharing while (a) increasing transparency, (b) regulating sensitive or harmful uses of consumer data, and (c) imposing accountability on companies that collect, hold, and transfer data.

c. Mergers Can have Anticompetitive Effects in Data-Driven Markets

Mergers have been a key part of the strategy for many of the largest companies in the U.S., including the largest digital platforms, to achieve their current market position. For years, it appeared that regulators did not perceive that these acquisitions posed a threat to competition or innovation.

For example, in 2007, Google received antitrust clearance to purchase DoubleClick, then the market leader in display ads on the internet. Later, Facebook was permitted to purchase Instagram, before the latter could become a competitor at scale in the social media space.

There are, however, signs of change. Late last year, for example, the Federal Trade Commission (FTC) brought suit against Facebook, alleging that it maintained its monopoly in personal social networking through a years-long course of anticompetitive conduct, including its acquisitions of WhatsApp and Instagram.[7] And just last week, the FTC took two steps that suggest a renewed commitment to aggressively scrutinizing acquisitions in data-driven markets. First, the FTC released a report in which it analyzed a decade's worth of acquisitions by large digital platforms that were too small or otherwise exempt from reporting requirements under the Hart-Scott-Rodino Act.[8] FTC Chair Lina Khan explained that in light of the report's findings, the FTC will closely

[6] Michael Gal & Oshrit Aviv, *The Competitive Effects of the GDPR*, 16 J. OF COMPETITION L. & ECON. 349 (May 18, 2020), available at https://academic.oup.com/jcle/article-abstract/16/3/349/5837809?redirectedFrom=fulltext.

[7] A timeline of the FTC's action against Facebook, including links to the FTC's complaints, can be found at https://www.ftc.gov/enforcement/cases-proceedings/191-0134/facebook-inc-ftc-v.

[8] *See* Fed. Trade Comm'n, *Non-HSR Reported Acquisitions by Select Technology Platforms, 2010-2019: An FTC Study* (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/reports/non-hsr-

examine reporting requirements to close reporting loopholes that she said may have allowed certain deals to "fly under the radar."[9] Second, the FTC voted to withdraw the Vertical Merger Guidelines just over a year after they were published. In doing so, the majority of the Commission promised to offer a new framework for vertical merger analysis that better takes into account the features specific to digital markets, including the potential for transactions to enable firms to exclude rivals by "degrading interoperability, reneging on access policies, or gaming algorithms."[10]

And, as this Committee knows, there are also a variety of legislative proposals before Congress that would make significant revisions to U.S. merger laws, including some that revise the standards for merger reviews or even bar some transactions altogether.[11]

Countries such as Germany have already amended their competition laws to provide more flexibility to address data-related issues. In Germany, Facebook was not subject to merger review when it purchased WhatsApp. Even though Facebook paid $19 billion to acquire WhatsApp, the merger controls did not apply because of the low amount of revenue WhatsApp generated at that time. Since then, Germany has implemented changes to permit regulatory scrutiny of acquisitions at lower revenue thresholds.

Given the importance of data to the economy and to consumers, we welcome efforts by enforcers and Congress to carefully consider appropriate steps to ensure that competition in data markets is unfettered and vibrant and that future acquisitions do not improperly stifle new entry and innovation.

### 4. How Privacy Legislation Can Foster Innovation and Competition

We encourage the Committee to consider privacy and competition not as separate bodies of law, but instead to be interrelated. Privacy laws materially impact markets, so they should be drafted to foster innovation and competition, not simply to increase data control and potential resulting concentration.[12] Antitrust laws impact citizen privacy, so they should be drafted to protect citizens

---

reported-acquisitions-select-technology-platforms-2010-2019-ftc-study/p201201technologyplatformstudy2021.pdf.

[9] *See* Fed. Trade Comm'n, *Remarks of Chair Lina M. Khan Regarding Non-HSR Reported Acquisitions by Select Technology Platforms*, Comm'n File No. P201201 (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1596332/remarks_of_chair_lina_m_khan_regarding_non-hsr_reported_acquisitions_by_select_technology_platforms.pdf.

[10] *See* Fed. Trade Comm'n, *Statement of Chair Lina N. Khan, Comm'r Rohit Chopra, and Comm'r Rebecca Kelly Slaughter on the Withdrawal of the Vertical Merger Guidelines*, Comm'n File No. P810034 at 7 (Sept. 15, 2021), available at https://www.ftc.gov/system/files/documents/public_statements/1596396/statement_of_chair_lina_m_khan_commissioner_rohit_chopra_and_commissioner_rebecca_kelly_slaughter_on.pdf.

[11] *See, e.g.,* the Competition and Antitrust Law Enforcement Reform Act of 2021, S. 224, 117th Cong. (2021), available at https://www.congress.gov/bill/117th-congress/senate-bill/225/text; and the Trust-Busting for the Twenty-First Century Act, S. 1074, 117th Cong. (2021), available at https://www.congress.gov/bill/117th-congress/senate-bill/1074. For a bill introduced in the House, *see* the Platform Competition and Opportunity Act, H.R. 3826, 117th Cong. (2021), available at https://www.congress.gov/bill/117th-congress/house-bill/3826/ (would prohibit dominant platforms from acquiring competitive threats or engaging in acquisitions that would "increase or enhance" the platform's market position).

[12] Of significant note, the United Kingdom announced earlier this month that it was beginning a consultation process that would build on principles within the GDPR in order to "support vibrant competition and innovation to drive economic growth" and "maintain high data protection standards without creating

and require responsible and accountable uses of their data. America should focus on constructing future-prepared laws that support a fair, competitive, healthy, trustworthy, connected economy.

a. Accountability-Based Frameworks Support Innovation and Growth

Our economy depends in key part on companies' ability to readily access and share consumer data. We thus encourage the Committee to consider legislative approaches that do not severely restrict companies from collecting, using, or sharing consumer data. The economy is too complex, and consumer data practices are too multilayered, for statutes to pinpoint who should hold consumer data and who should not. That approach potentially determines which companies can compete, unfairly entrenching companies with more consumer data with a superior competitive position.

Instead, we encourage the Committee to consider a more balanced approach that focuses on imposing accountability on companies that use citizens' data. Accountability-based frameworks regulate sensitive or potentially harmful uses of consumer data, while permitting the pro-competitive data collection and sharing the U.S. economy needs for innovation and growth. For example:

- Accountability can require holders of citizens' data to build internal governance programs for protecting data, such as (a) implementing internal privacy policies and controls, (b) designating data privacy officer(s), and (c) documenting Privacy Impact Assessments before engaging in activities that present heightened risks to citizens. Governance requirements can be scaled so that larger data holders are expected to have more robust governance in place.
- These frameworks can also require companies to contractually bind service providers and third parties that receive consumer data to specified protective obligations.
- Emerging practices that carry risk for citizens – such as algorithm development – can be subject to additional assessment and reporting requirements.
- Companies that hold consumer data and are not immediately visible to consumers, such as independent data providers, can register with a regulator to enable consumers to know who they are.

Accountability-based frameworks can also be supplemented with transparency rules and individual control rights that consumers can exercise. These can include rights to access their consumer data, delete that data, or opt-out of specified types of data sharing.

b. Now is the Time to Act

In closing, the right view of the intersection of data and competition should lead to the right outcome for a national privacy law. Congress has a critical window to act on privacy legislation. In January 2023, California's Privacy Rights Act (CPRA) as well as the new Virginia privacy law will go into effect, followed by the new Colorado Privacy Act in July 2023.[13] We expect more state

unnecessary barriers to responsible data use." *See* United Kingdom Department for Digital, Culture, Media, and Sport, *Data: A New Direction* (Sept. 10, 2021), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1016395/Data_Reform_Consultation_Document__Accessible_.pdf.

[13] For the California Consumer Privacy Act and/or California Privacy Rights Act, *see* Cal. Civ. Code § 1798.100 *et seq*. For the Colorado Privacy Act, *see* Colo. Rev. Stat. § 6-1-1301 *et seq*. For the Virginia Consumer Data Protection Act, *see* Va. Code § 59.1-571 *et seq*.

privacy laws to pass next year. These statutes will significantly limit how consumer data can be collected and shared, and will have practical effects across our national economy. In particular, CPRA will make consumer data sharing more difficult for online advertising. Consumers will have a right to opt-out of all "sharing" of their consumer data for common types of online advertising. Further, CPRA suggests that companies that provide online advertising services may not be able to use customer data to improve their advertising services for all their customers.

These rules are likely to have GDPR-like anticompetitive effects. Companies that have large quantities of citizen data may be by largely unaffected by CPRA, since they do not have to "share" consumer data with anyone but themselves. But for smaller competitors, which are critical to a robust marketplace and the development of future innovative solutions, access to essential consumer data may be cut off. This would require advertisers, publishers and others to work with fewer, more dominant players in order to communicate and interact with consumers, likely in a more expensive manner – which leaves small businesses fewer options on how to reach out to consumers. That is not an outcome that is pro-consumer.

## 5. Conclusion

Consumer data and technology are critical to the national and international economy. We support the adoption of a well-balanced federal privacy law and competition laws and policies that provide critical protections for individuals and their data, and enable the responsible flow of consumer data among all accountable companies, in order to preserve and enhance the connected marketplace.