Office of Commissioner
Melissa Holyoak

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

PRIVACY ENFORCEMENT PRIORITIES FOR THE DIGITAL ECONOMY

MELISSA HOLYOAK*
COMMISSIONER, U.S. FEDERAL TRADE COMMISSION

APRIL 22, 2025

KEYNOTE AT IAPP GLOBAL PRIVACY SUMMIT 2025
WASHINGTON, D.C.

* The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.

I want to start by thanking IAPP and its staff for inviting me to speak at this year's Global Privacy Summit. It is a tremendous honor to be with you all tonight. Before I begin, I need to give a disclaimer about my remarks: the views that I share tonight are my own; they do not necessarily reflect the views of the Federal Trade Commission ("FTC") or any other Commissioner.

I. Introduction

As we all know, the digital economy has become a cornerstone of economic growth, job creation, and innovation worldwide.[1] By 2028, the global digital economy is projected to grow to approximately $16.5 trillion and account for 17% of the global GDP.[2] In the U.S. alone, the digital economy was recently estimated to add more than $2.6 trillion in value and employ millions of American workers across nearly all economic sectors.[3] Leadership in digital technologies, including artificial intelligence, is critical to securing our economic and national security.[4] The growth of the digital economy has been fueled by the rapid development of artificial intelligence and other digital tools. These new technologies—which are powered by vast quantities of data—are driving innovation and transforming entire industries.

Businesses are now leveraging these technologies to improve their decision-making and efficiency, develop new products, and personalize users' experiences.[5] But the pace of these technological advancements presents challenges—or, in my view, opportunities—for all of us as policymakers, regulators, enforcers, and compliance professionals to protect consumers while still allowing this innovation to flourish.[6] Congress has empowered the FTC to protect consumers' privacy interests in a number of different statutes including, for example, the Children's Online Privacy Protection Act,[7] the Fair Credit Reporting Act,[8] and the Gramm-Leach-Bliley Act.[9] We should focus on robustly enforcing these laws. And we should apply—but must avoid stretching—

---

[1] *See* U.S. International Trade Administration, *Global Digital Economy Reporting*, https://www.trade.gov/digital-economy-reporting (last visited Apr. 21, 2025) (noting that "in 2022, the U.S. digital economy added nearly $2.6 trillion in value to the overall U.S. economy").

[2] *See* Michael O'Grady, David Hoffman, Ian Jacobs, *et al.*, *Global Digital Economy Forecast, 2023 To 2028*, Forrester Forecast Report (July 17, 2024), https://www.forrester.com/report/global-digital-economy-forecast-2023-to-2028/RES181192?ref_search=0_1740355200579.

[3] *U.S. Digital Economy: New and Revised Estimates, 2017–2022*, Survey of Current Business, Journal of the U.S. Bureau of Economic Analysis (Dec. 6, 2023), https://apps.bea.gov/scb/issues/2023/12-december/pdf/1223-digital-economy.pdf; Adam Thierer, *The Policy Origins of the Digital Revolution & the Continuing Case for the Freedom to Innovate*, R Street Institute (Aug. 15, 2024), https://www.rstreet.org/commentary/the-policy-origins-of-the-digital-revolution-the-continuing-case-for-the-freedom-to-innovate/ (citing the U.S. Bureau of Economic Analysis report, and noting that "the U.S. digital economy accounted for over $4 trillion of gross output, $2.6 trillion of value added (translating to 10 percent of U.S. GDP), $1.3 trillion of compensation, and 8.9 million jobs").

[4] *See* Dr. Rebecca Grant, *Race for the Future: Securing America's Innovation Edge Against Authoritarian Threats*, Lexington Institute, at 3 (Mar. 2025), https://lexingtoninstitute.org/wp-content/uploads/2025/03/Race-to-the-Future-March-2025.pdf; *See also* U.S. House Committee on Energy and Commerce, *Request for Information to Explore Data Privacy and Security Framework* (Feb. 21, 2025), https://d1dth6e84htgma.cloudfront.net/02_21_2025_PWG_Request_for_Info_2_e1753e1356.pdf (inviting stakeholders to provide written responses to questions regarding these technologies).

[5] Secure Privacy, *Understanding the Value of Data: Exploring Why Data is the New Gold* (Oct. 19, 2023), https://secureprivacy.ai/blog/significance-of-data-in-digital-era.

[6] U.S. House Committee on Energy and Commerce, *supra* note 4.

[7] 15 U.S.C. §§ 6501-6506.

[8] 15 U.S.C. §§ 1681-1681x.

[9] 15 U.S.C. §§ 6801-6809, §§ 6821-6827.

our legal authorities under Section 5 of the FTC Act.[10] For instance, our unfairness authority must be grounded in sound economic theories of harm and reliable empirical research. And, for the cost-benefit analysis test, the Commission must balance the risks and harms of data misuse against the benefits to consumers and competition.[11]

Striking this balance correctly is essential, not only to protect consumers' privacy interests, but also to promote competition and foster a predictable regulatory environment that encourages growth and innovation. Taking these principles into account, I'll highlight some of my specific priorities as a Commissioner. *First*, with artificial intelligence, the Commission should create a predictable regulatory and enforcement environment that promotes innovation and development of new technologies. This starts by seeking to better understand this nascent industry and how privacy enforcement and regulations may impact its development. *Second*, the Commission should leverage its existing authorities and tools to better protect children and teens from online harms that result when Big Tech and other companies prioritize profit over kids' privacy and safety. And *third*, we need stronger enforcement against companies that sell, transfer, or disclose Americans' sensitive personal data, like precise geolocation data, including to malicious foreign actors.

II. Establishing a Predictable AI Regulatory Environment

Let's start with artificial intelligence. As Vice President Vance remarked in February, "we face the extraordinary prospect of a new industrial revolution, one on par with the invention of the steam engine."[12] But, as he observed, "it will never come to pass if overregulation deters innovators from taking the risks necessary to advance the ball."[13] The Commission plays an important role in ensuring that AI development is done in a manner that promotes innovation, avoids entrenching dominant firms, and combats deceptive and fraudulent behaviors. We, of course, will aggressively root out AI-powered fraud and scams, and stop companies from making false or unsubstantiated representations that harm consumers.[14] Under the leadership of Chairman Ferguson, the Commission will promote AI growth and innovation, not hamper it with misguided enforcement actions or excessive regulation. [15]

But we must also study the issues surrounding the development of AI, the emerging risks to consumers, and evolving AI markets. I supported the issuance of the Commission's use of Section 6(b) of the FTC Act[16] to issue a report regarding AI partnerships and investments because

---

[10] 15 U.S.C. § 45.
[11] 15 U.S.C. § 45(n).
[12] Remarks by the Vice President at the Artificial Intelligence Action Summit in Paris, France (Feb.11, 2025), https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france.
[13] *Id.*
[14] *See, e.g.*, Concurring Statement of Comm'r Melissa Holyoak, Joined by Chair Lina M. Khan, *DoNotPay, Inc.*, FTC Matter No. 2323042 (Sept. 25, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Holyoak-Khan-Statement-re-DoNotPay-09-25-2024.pdf.
[15] *See* Dissenting Statement of Comm'r Melissa Holyoak, Joined by Comm'r Andrew N. Ferguson, *Rytr LLC*, FTC Matter No. 2323052 (Sept. 25, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/holyoak-rytr-statement.pdf; Dissenting Statement of Comm'r Andrew N. Ferguson, Joined by Comm'r Melissa Holyoak, *Rytr LLC*, FTC Matter No. 2323052 (Sept. 25, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/ferguson-rytr-statement.pdf.
[16] 15 U.S.C. § 46(b).

it advanced our knowledge of some of the commercial dynamics shaping AI's evolution.[17] While this information and research are valuable to the Commission, policymakers, and the public, I see several additional opportunities to further our understanding of AI.

For example, as part of that 6(b) report, the Commission staff identified key inputs for AI including the massive amounts of data required for training models and the major undertaking for gathering, cleaning, and preparing that data.[18] AI developers obtain training data from various sources including "scraping training data from the web, using data collected from users of other products to train their models, hiring short-term contractors to create the data, buying data from data brokers or third-party companies, or buying it from rightsholders directly."[19] We need to better understand how regulatory and enforcement efforts in privacy may impact a firm's ability to access and train data and, importantly, how they impact the firm's ability to compete. On one hand, requiring consent, at least for certain types of data or in certain contexts, may level the competitive playing field, by requiring the same level of privacy protection across the board. On the other hand, a privacy regime that requires affirmative consent from users for data collection or use *may favor* dominant players. Users are more familiar with these firms, and thus, may have more trust in how these firms will collect or use their data.

- So, would a consent-based regime give these dominant firms an advantage in the development of AI?
- How do regulatory or enforcement burdens in specific jurisdictions impact firms competing globally?
- Do they restrict access to, and use of, data that powers AI technologies?
- Are there alternatives to such regulations that are better suited to balancing privacy concerns with interests in fostering innovation and competition?
- How do data portability and interoperability requirements for platforms and online services affect competition in the AI space?

We should seek answers to these and other questions based on sound economic principles and robust empirical analysis. Economics has been a critical component of the Commission's privacy enforcement program for many years. Indeed, our economists have a long history of developing sound economic theories of harm. We must continue such study in the AI space; it may be critical now more than ever.

---

[17] *Concurring and Dissenting Statement of Comm'r Melissa Holyoak Joined by Comm'r Andrew N. Ferguson Regarding the FTC Staff Report on AI Partnerships & Investments 6(b) Study*, FTC Matter No. P246201 (Jan. 17, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/holyoak-statement-ai-6b.pdf.

[18] Fed. Trade Comm'n, *Partnerships Between Cloud Service Providers and AI Developers*, FTC Staff Report on AI Partnerships & Investments 6(b) Study, at 13 (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246201_aipartnerships6breport_redacted_0.pdf.

[19] *Id*. at 26.

To that end, the Commission and the Department of Justice recently issued Requests for Information to help identify anticompetitive regulations at the state and federal level.[20] Recently, at the state level alone, over 500 AI-related bills have been introduced.[21] I encourage thought leaders like yourselves to respond to these RFIs. Your responses will help us understand the different regulatory burdens for firms and whether those burdens create barriers to new entrants and competition.

III. Protecting Children and Teens from Online Harms

I now want to discuss protecting children and teens from online harms. Protecting kids online is one of my top priorities as a Commissioner. I know firsthand that children and teens are a particularly vulnerable population online. They face myriad risks online and across digital platforms, including cyberbullying, predatory behavior, inappropriate content, and scams, as well as risks to their own privacy. The Commission must use every tool that Congress has given it to help protect children and teens from online harms, and to better understand emerging technologies that could negatively affect kids' online privacy and safety.

I am proud of the Commission's recent work, and I have supported enforcement actions to protect children and teens from harm online. For example, last summer, we brought an action with the Los Angeles District Attorney's Office to shut down an online messaging app marketed as a "safe space for teens."[22] Instead, the app sent fake, provocative messages to prey on teens' insecurities and lure them into buying the company's subscription. More recently, we settled a case against the developers and distributors of Genshin Impact—a child-directed video game that collected children's personal information without parental consent and deceptively sold "loot boxes" to kids in violation of Section 5.[23] It is critical that the Commission continue this important enforcement work and that we use all available statutory tools to protect children and teens online.

Just today, the Federal Register published the Commission's COPPA Rule amendments voted out in January.[24] The amendments are a culmination of the bipartisan effort that started in

---

[20] Fed. Trade Comm'n, *FTC Launches Public Inquiry into Anti-Competitive Regulations* (Apr. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/04/ftc-launches-public-inquiry-anti-competitive-regulations; U.S. Dep't of Justice, *Justice Department Launches Anticompetitive Regulations Task Force* (Mar. 27, 2025), https://www.justice.gov/opa/pr/justice-department-launches-anticompetitive-regulations-task-force.

[21] Bus. Software Alliance, *2025 State AI Wave Building After 700 Bills in 2024* (Oct. 22, 2024), https://www.bsa.org/news-events/news/2025-state-ai-wave-building-after-700-bills-in-2024; *Artificial Intelligence (AI) Legislation*, https://www.multistate.ai/artificial-intelligence-ai-legislation (last visited April 21, 2025).

[22] Fed. Trade Comm'n, *FTC Order Will Ban NGL Labs and its Founders from Offering Anonymous Messaging Apps to Kids Under 18 and Halt Deceptive Claims Around AI Content Moderation* (July 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-order-will-ban-ngl-labs-its-founders-offering-anonymous-messaging-apps-kids-under-18-halt.

[23] Fed. Trade Comm'n, *Genshin Impact Game Developer Will be Banned from Selling Lootboxes to Teens Under 16 without Parental Consent, Pay a $20 Million Fine to Settle FTC Charges* (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/genshin-impact-game-developer-will-be-banned-selling-lootboxes-teens-under-16-without-parental.

[24] Children's Online Privacy Protection Rule, 90 Fed. Reg. 16918 (Apr. 22, 2025), https://www.federalregister.gov/documents/2025/04/22/2025-05904/childrens-online-privacy-protection-rule.

2019.[25] And, while I would have preferred a different approach to certain amendments, I voted in favor of the final Rule because it expands privacy protections for children. For example, in April 2026, operators will need to publish retention schedules; obtain separate parental consent for disclosures of children's personal information to third parties not integral to the service; and comply with the Rule's enhanced data security requirements.

The Commission has—and will continue to use—other valuable tools in its arsenal. This includes our ability to facilitate public discussion between, and learn from, diverse stakeholders. An example of this tool is the Commission's upcoming workshop on the "Attention Economy" in June.[26] The workshop will bring together parents, child safety experts, and others to discuss concrete ways to protect kids online and empower parental choice. As part of those efforts, we should study new technologies that may affect kids' online privacy and safety, such as AI chatbots. And we should understand better how parental controls and settings work on different digital platforms and apps. Parents know their kids best and understand better than any online service how much supervision their kids need. Parents deserve meaningful choices to protect their children – not mere fig leaves to insulate the operator from liability for design choices that expose kids to sexual predators, obscene content, violence, or other such harms.

Finally, we should explore how emerging age verification technologies and requirements can help protect children and teens. Many legislatures are actively considering this issue. In fact, my home state of Utah recently enacted a law that requires app store providers to verify users' ages and obtain parental consent for anyone under 18 to download apps or make in-app purchases.[27] Age verification requirements, like Utah's, can help establish baseline protections for children and teens when they are online. But these requirements are complicated and may raise other important concerns as courts have recognized when enjoining their implementation.

IV. Protecting Americans' Sensitive Personal Data from Malicious Foreign Actors

The last issue I'll discuss tonight is how we can protect Americans' sensitive personal data from being sold in bulk to foreign adversaries and malicious actors. It is no surprise that malicious actors and foreign adversaries want to obtain vast troves of personal data about consumers. And they obtain this data in a number of ways. For example, consumers may inadvertently share their data with unscrupulous third parties due to misleading or deceptive representations about an app's privacy or data sharing practices. In other cases, bad actors may exploit vulnerabilities in a company's security program to gain access to consumers' personal data. The Commission has deep experience fighting misleading data sharing practices and deficient information security practices,[28] and I expect enforcement to continue in these areas.

---

[25] Fed. Trade Comm'n, *FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data* (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data; Fed. Trade Comm'n, *FTC Seeks Comments on Children's Online Privacy Protection Act Rule* (July 25, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-seeks-comments-childrens-online-privacy-protection-act-rule.

[26] Fed. Trade Comm'n, *The Attention Economy: How Big Tech Firms Exploit Children and Hurt Families* (June 4, 2025), https://www.ftc.gov/news-events/events/2025/06/attention-economy-tech-firms-exploit-children.

[27] App Store Accountability Act, Utah S.B. 142 (2025), https://le.utah.gov/Session/2025/bills/enrolled/SB0142.pdf.

[28] *See generally* Fed. Trade Comm'n, *FTC Privacy and Security Cases*, https://www.ftc.gov/enforcement/cases-proceedings/terms/1420.

But there is another, and often overlooked, way that foreign adversaries can gain access to Americans' sensitive personal data. They buy it.[29] Foreign adversaries will purchase data, usually in bulk, from data brokers that aggregate, analyze, and sell data collected from unwitting individuals. Precise geolocation data is particularly sensitive, and can reveal our religious beliefs, political affiliations, and even medical conditions and treatment.[30] This information can be exploited and poses significant—and frankly, unacceptable—risks to our national and economic security.

So, what can the Commission do to prevent these purchases? One step is to leverage our existing statutory authorities, like the Protecting Americans' Data from Foreign Adversaries Act (PADFAA).[31] In short, that Act prohibits businesses from selling, licensing, transferring, disclosing, or providing access to Americans' sensitive personal data that they do not collect directly to entities controlled by foreign adversaries. Additionally, in the future there may be opportunities to partner with the Department of Justice, as it enforces its recently enacted rule that restricts the transfer of Americans' sensitive personal data to countries of concern.[32]

* * * * *

I want to conclude my remarks tonight by reiterating that the Commission is committed to protecting consumers' privacy and security interests while promoting competition and innovation. We'll do that by enforcing the laws we have, not by stretching our legal authorities. And we'll continue to take a "flexible, risk-based approach" to privacy enforcement that "'balance[s] business needs, consumer expectations, legal obligations, and potential privacy harms.'"[33]

---

[29] *See, e.g.*, Concurring Statement of Comm'r Melissa Holyoak, Joined in Part by Comm'r Alvaro M. Bedoya, *Gravy Analytics*, at 3, FTC Matter No. 2123035 (Dec. 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/commissioner-holyoak-concurring-statement-gravy.pdf.

[30] *Id.* at 2. *See also, e.g.*, Concurring Statement of Comm'r Melissa Holyoak, *Kochava Inc.*, at 2, FTC Matter No. X230009 (July 15, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2024-7-15-Commissioner-Holyoak-Statement-re-Kochava-final.pdf.

[31] Pub. Law No.118-50(I) (Apr. 24, 2024).

[32] Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 28 C.F.R § 202 (2025).

[33] Comment of Staff of Fed. Trade Comm'n, *Developing the Administration's Approach to Consumer Privacy*, Nat'l Telecomm. & Info. Admin. Docket No. 180821780-8780-01 (Nov. 9, 2018) (quoting Nat'l Telecomm. & Info. Admin., *Request for Comment on Developing the Administration's Approach to Consumer Privacy*, Docket No. 180821780-8780-0183, Fed. Reg. 48600, 48602 (Sept. 26, 2018)).