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

Office of the Chair

Remarks of Chair Lina M. Khan
FTC Tech Summit

January 25, 2024

Hi, everyone. Thanks so much for joining the FTC's first Technology Summit on artificial intelligence.

I'm thrilled to welcome our panelists, who bring deep expertise to this conversation. And I'd like to give a special thanks to the FTC's Office of Technology and our fantastic Chief Technologist, Stephanie Nguyen, for spearheading today's summit. In the year since its launch, the Office of Technology has hit the ground running, deepening our agency's expertise as we navigate this fast-moving moment of technological opportunity and risk.

Over the last 18 months, the rapid deployment of artificial intelligence tools has captured the world's attention, spurring some combination of awe, wonder, apprehension, and fear. We hear how these automated technologies could open the door to breakthroughs across fields ranging from science to education, making life better for millions of people. But we also already see how these tools can turbocharge fraud, automate discrimination, and entrench surveillance, putting people in harm's way.

More fundamentally, we face basic questions of power and governance. Will this be a moment of opening up markets to fair and free competition, unleashing the full potential of emerging technologies? Or will a handful of dominant firms concentrate control over these key tools, locking us into a future of their choosing?

Which of these potential trajectories AI will take is not an inevitability. The outcome will be a direct result of policy choices we make now. The last time we faced similar questions prompted by new technologies was back in the mid-2000s, at the onset of the Web 2.0 era.

But what began as a revolutionary set of technologies ended up concentrating enormous private power over what have become near-essential services. Through aggressive strategies to acquire or lock out companies that threatened their position, a handful of firms solidified their dominance, while locking in business models that we now realize came at the expense of our privacy and security. Lawsuits around the country have surfaced the heavy costs, from the decimation of independent journalism to serious harm to kids' mental health.

Across history, we've routinely seen large firms—going back to U.S. Steel in the early 1900s, to Alcoa in the 1930s, to IBM and AT&T in the 1970s, to Boeing in the 1990s, and to dominant technology platforms today—argue that their market power is good for America.[1]

And yet, when you concentrate production, you concentrate risk. Unfortunately today we are living through the heavy costs of undue concentration. United Airlines CEO Scott Kirby recently drew a straight line between the 1997 mega-merger between Boeing and McDonnell Douglas and the transformation of Boeing from a highly profitable world-class engineering enterprise to an ossified money-losing corporation with dangerous quality issues.[2] After the merger, organized labor lost out, as the combined entity took on a union that had been essential to maintaining Boeing's innovative culture and commitment to quality.[3] Shareholders have lost out too, not having seen a dividend in four years.[4]

Boeing's journey is no different than that of many large corporations that policymakers have historically shielded from competition, and whose market power masked the decline and degradation of internal capacity. The difference between Boeing and many of those companies is there's simply no masking airplanes falling apart in the sky.

Today, policymakers across government recognize the importance of learning from these missteps as we navigate the challenges and opportunities posed by AI.

At the FTC, the rapid development and deployment of AI is informing our efforts across the agency, as we work to promote fair competition and protect Americans from unfair or deceptive tactics. There is no AI exemption from the laws on the books, and we're looking

---

[1] Government officials have often agreed. In the 1990s, officials even reportedly threatened the Europeans with sanctions if they wouldn't allow the merger of Boeing and McDonnell Douglas. As one White House advisor put it, aerospace was the "only sector where we have a de facto national champion and you can be an out-and-out advocate for it."

[2] David Koenig, Chester Dawson & Mary Schlangenstein, *United Airlines CEO Scott Kirby Takes Aim At Boeing Over More 737 Max Missteps*, DALLAS MORNING NEWS (Jan. 23, 2024), https://www.dallasnews.com/business/airlines/2024/01/23/united-airlines-ceo-scott-kirby-takes-aim-at-boeing-over-more-737-max-missteps/, ("'My own assessment is that this goes all the way back to the McDonnell Douglas merger and it started a changing culture,' [Kirby] said.").

[3] For instance, following a prolonged strike at its unionized plants in Washington state, Boeing announced in 2009 that it would assemble its new 787 Dreamliner aircraft in a new non-union plant in South Carolina. *See* Kathy Lohr, *Union Workers Cry Foul Over New S.C. Boeing Plant*, NPR (June 9, 2011), https://www.npr.org/2011/06/09/137081954/union-workers-cry-foul-over-new-s-c-boeing-plant. During the COVID-19 pandemic, Boeing would close its Dreamliner production line in Washington, concentrating all 787 production in South Carolina. *See* Nicholas Reimann, *Boeing Moving All 787 Production Away From Seattle Area, Possibly Costing 1,000 Jobs*, FORBES (Oct. 1, 2020), https://www.forbes.com/sites/nicholasreimann/2020/10/01/boeing-moving-all-787-production-away-from-seattle-area-possibly-costing-1000-jobs/. *See also* Natasha Frost, *The 1997 merger that paved the way for the Boeing 737 Max crisis*, QUARTZ (Jan. 3, 2020), https://qz.com/1776080/how-the-mcdonnell-douglas-boeing-merger-led-to-the-737-max-crisis.

[4] Claire Bushey, *Boeing Investors Could Wait 'Years' For Dividend To Return*, FIN. TIMES (Apr. 27, 2020), https://www.ft.com/content/842082c4-543b-4c0e-b826-2437a409db1f.

closely at the ways companies may be using their power to thwart fair competition or trick the public.[5]

As part of this effort, the Commission today is launching a market inquiry into the investments and partnerships being formed between AI developers and cloud service providers.[6] Through using the agency's 6(b) authority, we are scrutinizing whether these ties enable dominant firms to exert undue influence or gain privileged access in ways that could undermine fair competition across layers of the AI stack.

As we continue this work, a few key principles are top of mind.

First, we are focused on scrutinizing any existing or emerging bottlenecks across the AI stack. History shows that firms that capture control over key inputs or distribution channels can use their power to exploit those bottlenecks, extort customers, and maintain their monopolies. The role of antitrust is to guard against bottlenecks achieved through illegal tactics and ensure dominant firms aren't unlawfully abusing their monopoly power to block innovation and competition.

The agency is taking a close look across the AI stack to understand the extent of competition across the various layers and sub-layers. We are examining whether dominant firms with control over key inputs—like cloud infrastructure and access to GPUs—may be able to impose coercive terms, charge extractive fees, or deepen their existing moats. We're keen to sharpen our thinking on the various opportunities and potential obstacles for competition across AI markets and are eager to be learning from players within this ecosystem.

Second, we are squarely focused on how business models drive incentives. Just as we've seen behavioral advertising fuel the endless collection of user data, model training is emerging as another feature that could further incentivize surveillance. The FTC's work has made clear that these business incentives cannot justify violations of the law. The drive to refine your algorithm cannot come at the expense of people's privacy[7] or security,[8] and privileged access to customers'

---

[5] FTC Technology Blog, Tick, Tick, Tick. Office of Technology's Summit on AI (Jan. 18, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/tick-tick-tick-office-technologys-summit-ai.

[6] Press Release, Fed. Trade Comm'n, FTC Launches Inquiry into Generative AI Investments and Partnerships (Jan. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-launches-inquiry-generative-ai-investments-partnerships.

[7] Press Release, Fed. Trade Comm'n, FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

[8] Press Release, Fed. Trade Comm'n, FTC Order Will Require Blackbaud to Delete Unnecessary Data, Boost Safeguards to Settle Charges its Lax Security Practices Led to Data Breach (Feb. 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-require-blackbaud-delete-unnecessary-data-boost-safeguards-settle-charges-its-lax; Press Release, Fed. Trade Comm'n, FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users; *see also* FTC Technology Blog, Security Principles: Addressing Underlying Causes Of Risk In Complex Systems (Feb. 1, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems.

data cannot be used to undermine competition.[9] We similarly recognize the ways that consumer protection and competition enforcement are deeply connected—with firms engaging in privacy violations to build market power and the aggregation of market power, in turn, enabling firms to violate consumer protection laws. And our remedies will continue requiring that firms delete models trained on unlawfully acquired data in additional to the data itself.[10]

Third, we are squarely focused on aligning liability with capability and control. This requires looking upstream and across layers of the AI stack to pinpoint which actor is driving or enabling the lawbreaking. Our enforcement experience in other domains will directly inform how we approach this work. For example, our recent robocall enforcement sweep not only targeted telemarketers and the companies that hire them, but also looked upstream to the lead generators and Voice over Internet Protocol (VoIP) providers that enable illegal telemarketing.[11] And in our recent work to combat scams, we are holding upstream payment actors accountable for knowingly facilitating fraud.[12]

And fourth, we're focused on crafting effective remedies that establish bright-line rules on the development, use, and management of AI inputs. The FTC is making clear that some data is simply off the table for training models. For example, our recent order against Rite Aid bans

---

[9] FTC Technology Blog, Generative AI Raises Competition Concerns (June 29, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns.

[10] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data; Press Release, Fed. Trade Comm'n, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (Jan. 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data; Press Release, Fed. Trade Comm'n, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

[10] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data; Press Release, Fed. Trade Comm'n, FTC Order Will Ban InMarket from Selling Precise Consumer Location Data (Jan. 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data; Press Release, Fed. Trade Comm'n, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

[11] Press Release, Fed. Trade Comm'n, FTC and Federal and State Partners to Announce Nationwide Robocall and Telemarketing Enforcement Sweep in Chicago on July 18 (July 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-federal-state-partners-announce-nationwide-robocall-telemarketing-enforcement-sweep-chicago-july.

[12] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Files Amended Complaint Charging that Walmart Facilitated Scams Through Its Money Transfer Services That Fleeced Customers Out of Hundreds of Millions (June 30, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-files-amended-complaint-charging-walmart-facilitated-scams-through-its-money-transfer-services; Press Release, Fed. Trade Comm'n, FTC Acts to Block Payment Processor's Credit Card Laundering for Tech Support Scammers (Apr. 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-acts-block-payment-processors-credit-card-laundering-tech-support-scammers; Press Release, Fed. Trade Comm'n, FTC, Florida Attorney General Sue Chargebacks911 for Thwarting Consumers Who Were Trying to Reverse Disputed Credit Card Charges (Apr. 12, 2023).

the company from using facial recognition tools after its reckless application of the technology led to innocent people being accused of shoplifting.[13] And our recent cases against data brokers include bans on using or monetizing people's highly sensitive location data.[14]

As we continue to establish rules of the road for AI, it's essential that we set clear boundaries on the content that can and cannot be used for scraping and model-training. The Commission recently held a public workshop with creative professionals to better understand the types of guardrails that would help protect against creators' work being appropriated and devalued by generative AI models, including in ways that may undermine fair competition. Our subsequent report on generative AI and the creative economy lays out our core concerns and how our authorities may apply in this space.[15]

Across all of our work, we are making clear that there is no AI exemption from the laws on the books.[16] Firms can't use claims of innovation as a cover for lawbreaking. And we've already made that clear in a number of AI-specific contexts. Model-as-a-service companies that deceive users about how their data is collected may be violating the law.[17] Companies claiming that interoperability must come at the expense of privacy and security may be violating the law.[18] And companies that deceptively change their terms of service to their own advantage may be violating the law.[19]

Learning from our experience in the mid-2000s, where delayed government action locked in exploitative business models and monopoly power, we're using the full scope of our authorities to make sure this hard-learned lesson doesn't repeat itself.

Much is uncertain about what the precise future of this technology will look like. But it's clear these technologies could potentially transform industries across the economy, just as the rise of the internet did nearly forty years ago. Just like back then, this technology has already seen a huge influx of capital, with promise to grow our economy and catalyze major advances. And the good news is we have the experience and expertise to meet the moment.

I'm grateful for the experts who are sharing their time with us today. With that, I'll turn it over to our Deputy Chief Technologist, Alex Gaynor, who will be leading our first panel.

---

[13] Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards, *supra* note 9.
[14] *See, e.g.*, FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data, *supra* note 9; FTC Order Will Ban InMarket from Selling Precise Consumer Location Data, *supra* note 9.
[15] *See supra* note 5.
[16] Tick, Tick, Tick. Office of Technology's Summit on AI, FTC Technology Blog (Jan. 18, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/tick-tick-tick-office-technologys-summit-ai.
[17] AI Companies: Uphold Your Privacy and Confidentiality Commitments, FTC Technology Blog (Jan. 9, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/ai-companies-uphold-your-privacy-confidentiality-commitments.
[18] Interoperability, Privacy, & Security, FTC Technology Blog (Dec. 21, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/12/interoperability-privacy-security.
[19] AI Companies: Uphold Your Privacy and Confidentiality Commitments, FTC Technology Blog (Jan. 9, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/ai-companies-uphold-your-privacy-confidentiality-commitments.

***

https://abc.xyz/investor/board-and-governance/code-of-conduct/#top

Board & Governance

Code of Conduct

Preface
Employees of Alphabet and its subsidiaries and controlled affiliates ("Alphabet") should do the right thing – follow the law, act honorably, and treat co-workers with courtesy, support, and respect.

We expect all of our employees and Board members to know and follow this Code of Conduct. Failure to do so can result in disciplinary action, including termination of employment. Any waivers of this Code for directors or executive officers must be approved by our Board.

Never retaliate against anyone who reports or participates in an investigation of a possible violation of the Code.

If you are employed by a subsidiary or controlled affiliate of Alphabet, please comply with your employer's code of conduct. If your employer doesn't have its own code of conduct, if you have a question or concern about this Code or believe that someone may be violating it, or if you want to remain anonymous, you can make a report of a suspected violation or concern through our Helpline. And if you believe a violation of law has occurred, you can always raise that through the Ethics & Business Integrity helpline or with a government agency.

While the Code is specifically written for Alphabet employees and Board members, we expect Alphabet contractors, consultants, and other members of the extended workforce who may be temporarily assigned to perform work or services for Alphabet to follow the Code in connection with their work for us. Failure of a member of the Alphabet extended workforce to follow the Code can result in termination of their relationship with Alphabet.

I. Avoid Conflicts of Interest
When you are in a business situation in which competing loyalties could cause you to pursue a personal benefit for you, your friends, or your family at the expense of Alphabet or our users, you may be faced with a conflict of interest. All of us should avoid conflicts of interest and circumstances that reasonably present the appearance of a conflict.

When considering a course of action, ask yourself whether the action you're considering could create an incentive for you, or appear to others to create an incentive for you, to benefit yourself, your friends or family, or an associated business at the expense of Alphabet. If the answer is "yes", the action you're considering is likely to create a conflict of interest situation, and you should avoid it.

II. Ensure Financial Integrity and Responsibility

Ensure that money is appropriately spent, our financial records are complete and accurate, and our internal controls are honored.

If your job involves the financial recording of our transactions, make sure that you're familiar with all relevant policies, including those relating to revenue recognition.

Never interfere with the auditing of financial records. Similarly, never falsify any company record or account.

If you suspect or observe any irregularities relating to financial integrity or fiscal responsibility, no matter how small, immediately report them.

III. Obey the Law

Comply with all applicable legal requirements and understand the major laws and regulations that apply to your work. A few specific laws are easy to violate unintentionally and so are worth pointing out here. If you have any questions about these laws or other laws governing our work, please consult the Helpline or our legal counsel.

1. Trade Controls

Various trade laws control where we can send or receive our products and services. These laws are complex and apply to:

- importing and exporting goods to or from the United States and other countries
- exporting services or providing services to non-U.S. persons
- exporting technical data, especially data originating in the U.S.

If you are involved in sending or making available products, services, software, equipment, or technical data from one country to another, work with your manager to ensure that the transaction stays within the bounds of applicable laws.

2. Competition Laws

Be sure you follow all laws designed to promote free and fair competition and protect consumers. These laws generally prohibit 1) arrangements with competitors that restrain trade, 2) abuse of market power to unfairly disadvantage competitors, and 3) misleading or harming consumers. Some of these laws carry civil and criminal penalties for individuals and companies.

3. Insider Trading Laws

Do not use non-public information to buy or sell stock, or to pass it along to others so that they may do so. That could constitute the crime of insider trading.

Familiarize yourself with Alphabet's Insider Trading Policy. It describes policies that address the risks of insider trading, such as:

- a prohibition on hedging Alphabet stock

- periodic blackout windows when you may not trade Alphabet stock

4. Anti-Bribery Laws
Various laws that prohibit bribery in different settings. Our rule is simple – don't bribe anybody, at any time, for any reason.

Non-government relationships. Be careful when you give gifts and pay for meals, entertainment or other business courtesies on behalf of Alphabet. Avoid the possibility that the gift, entertainment or other business courtesy could be perceived as a bribe. Provide such business courtesies infrequently and, when you do, to keep their value moderate.

Dealings with government officials. Various laws prohibit seeking to influence official action by offering or giving anything of value to government officials, candidates for public office, employees of government-owned or controlled companies, public international organizations, or political parties. Avoid not only traditional gifts, but also things like meals, entertainment, travel, political or charitable contributions, and job offers for government officials' relatives. With pre-approval, it may be permissible to make infrequent and moderate expenditures for gifts and business entertainment for government officials that are directly tied to promoting our products or services (e.g., a modest meal at a day-long demonstration of our products).

IV. Promote a workplace that is supportive and respectful for all employees and members of the extended workforce
Alphabet has an unwavering commitment to prohibiting and effectively responding to harassment, discrimination, misconduct, abusive conduct, and retaliation. To that end, Alphabet adheres to these Guiding Principles:

A. Commitment: Alphabet sets a tone at the top of commitment to a respectful, safe, and inclusive working environment for all employees and members of the extended workforce.

B. Care: Alphabet creates an environment with an emphasis on respect for each individual at all levels of the organization, including specifically by offering assistance and showing empathy to employees and members of the extended workforce throughout and after the complaint process.

C. Transparency: Alphabet is open and transparent as an organization regarding the frequency with which complaints arise regarding harassment, discrimination, misconduct, abusive conduct, and retaliation, and the Company's approach to investigating and responding to those allegations.

D. Fairness & Consistency: Alphabet ensures that individuals are treated respectfully, fairly, and compassionately in all aspects of Alphabet interactions and applies policies, procedures, and outcomes consistently regardless of who is involved.

E. Accountability: Alphabet holds all individuals responsible for their actions, and ensures that where appropriate, those individuals hold others accountable too.

Each Bet has specific policies that implement Alphabet's commitment and these Guiding Principles. Be sure to read and comply with those policies. And if you're ever concerned that Alphabet, a Bet, or a fellow employee or member of the extended workforce is falling short, don't stay silent, you can make a report through your Bet's reporting channels and the Alphabet helpline.

V. Conclusion
We rely on one another's good judgment to uphold a high standard of integrity for ourselves and our company. Each of us should be guided by both the letter and the spirit of this Code.

See Google Code of Conduct here.

Report concerns

To notify Alphabet's Audit and Compliance Committee of any concerns regarding Alphabet's accounting, internal controls, auditing, conflict minerals matters or workplace concerns, you may mail your concern to:

Alphabet Inc.
Attn: Accounting Concerns or Workplace Concerns
1600 Amphitheatre Parkway
Mountain View, CA 94043

You may report your concerns anonymously; however the Audit and Compliance Committee encourages you to provide your name and contact information so that we may contact you directly if necessary.

https://www.google.com/chrome/choicescreen/

About the choice screen

On September 6, 2023, the European Commission announced that Google had been designated as a gatekeeper under the Digital Markets Act (DMA), a new piece of legislation designed to ensure fair and open digital markets. To comply with its DMA obligations, Google's changes to its choice screens include: (i) introduce a new browser choice screen during initial device setup in addition to a search choice screen on Android smartphones and tablets; and (ii) show a search choice screen in Chrome on non-Android platforms. An illustrative version of the search choice screen follows. Providers may vary by country.

https://a2a-protocol.org/latest/specification/

What is A2A Protocol?¶

Welcome to the **official documentation** for the **Agent2Agent (A2A) Protocol**, an open standard designed to enable seamless communication and collaboration between AI agents.

Originally developed by Google and now donated to the Linux Foundation, A2A provides the definitive common language for agent interoperability in a world where agents are built using diverse frameworks and by different vendors.

Why use the A2A Protocol¶

- **Interoperability**

Connect agents built on different platforms (LangGraph, CrewAI, Semantic Kernel, custom solutions) to create powerful, composite AI systems.

- **Complex Workflows**

Enable agents to delegate sub-tasks, exchange information, and coordinate actions to solve complex problems that a single agent cannot.

- **Secure & Opaque**

Agents interact without needing to share internal memory, tools, or proprietary logic, ensuring security and preserving intellectual property.

A2A and Model Context Protocol (MCP) are complementary standards for building robust agentic applications:

- **Model Context Protocol (MCP)**: Provides agent-to-tool communication. It's a complementary standard that standardizes how an agent connects to its tools, APIs, and resources to get information.
- **IBM ACP**: Incorporated into the A2A Protocol
- **Cisco agntcy**: A framework that provides components to the Internet of Agents with discovery, group communication, identity and observability and leverages A2A and MCP for agent communication and tool calling.
- **A2A**: Provides agent-to-agent communication. As a universal, decentralized standard, A2A acts as the public internet that allows ai agents—including those using MCP, or built with frameworks like agntcy—to interoperate, collaborate, and share their findings.

1. Introduction¶

The Agent2Agent (A2A) Protocol is an open standard designed to facilitate communication and interoperability between independent, potentially opaque AI agent systems. In an ecosystem where agents might be built using different frameworks, languages, or by different vendors, A2A provides a common language and interaction model.

This document provides the detailed technical specification for the A2A protocol. Its primary goal is to enable agents to:

- Discover each other's capabilities.
- Negotiate interaction modalities (text, files, structured data).
- Manage collaborative tasks.
- Securely exchange information to achieve user goals **without needing access to each other's internal state, memory, or tools.**

1.1. Key Goals of A2A¶

- **Interoperability:** Bridge the communication gap between disparate agentic systems.
- **Collaboration:** Enable agents to delegate tasks, exchange context, and work together on complex user requests.
- **Discovery:** Allow agents to dynamically find and understand the capabilities of other agents.
- **Flexibility:** Support various interaction modes including synchronous request/response, streaming for real-time updates, and asynchronous push notifications for long-running tasks.
- **Security:** Facilitate secure communication patterns suitable for enterprise environments, relying on standard web security practices.
- **Asynchronicity:** Natively support long-running tasks and interactions that may involve human-in-the-loop scenarios.

1.2. Guiding Principles¶

- **Simple:** Reuse existing, well-understood standards (HTTP, JSON-RPC 2.0, Server-Sent Events).
- **Enterprise Ready:** Address authentication, authorization, security, privacy, tracing, and monitoring by aligning with established enterprise practices.
- **Async First:** Designed for (potentially very) long-running tasks and human-in-the-loop interactions.
- **Modality Agnostic:** Support exchange of diverse content types including text, audio/video (via file references), structured data/forms, and potentially embedded UI components (e.g., iframes referenced in parts).
- **Opaque Execution:** Agents collaborate based on declared capabilities and exchanged information, without needing to share their internal thoughts, plans, or tool implementations.

Use Case Highlights¶

A2A unlocks powerful new ways for AI agents to collaborate and solve complex problems. Here are a few examples of what's possible:

- **Multi-Agent Workflows:** Chain specialized agents together to automate complex processes, like candidate sourcing for hiring or streamlining supply chain logistics.
- **Agent Marketplaces:** Create platforms where agents can discover and utilize the capabilities of other agents from different providers.
- **Cross-Platform Integration:** Connect agents built on different frameworks—like LangGraph, BeeAI, and more—to work together seamlessly.
- **Evaluating Multi-Agent Systems:** Use frameworks like Vertex AI to assess the performance and success of collaborative agent trajectories.

Community Spotlight¶

Featured Contributions¶

A2A is an open-source protocol, and we thrive on community contributions. A huge thank you to everyone who has helped build and improve A2A! Here are some recent highlights:

- Python Quickstart Tutorial (PR#202)
- LlamaIndex sample implementation (PR#179)
- Autogen sample server (PR#232)
- AG2 + MCP example (PR#230)
- PydanticAI example (PR#127)

The Word on the Street¶

The launch of A2A has sparked lively discussions and positive reactions across various social and video platforms.

- **Microsoft's Semantic Kernel:** Asha Sharma, Head of AI Platform Product at Microsoft, announced on LinkedIn that "Semantic Kernel now speaks A2A," enabling instant, secure interoperability.
- **Matt Pocock's Diagramming:** Well-known developer educator Matt Pocock shared diagrams on X explaining the A2A protocol, which were liked and reposted hundreds of times.
- **Craig McLuckie's "Hot Take":** Craig McLuckie shared his thoughts on LinkedIn, highlighting A2A's focus on interactions *between* agentic systems as a sensible approach.

- **Zachary Huang's Deep Dive:** In his YouTube video, Zachary explains how A2A complements MCP, with A2A handling communication between agents and MCP connecting agents to tools.

A2A Integrations¶

These agentic frameworks have built-in A2A integration, making it easy to get started:

- Agent Development Kit (ADK)
- AG2
- BeeAI Framework
- LangGraph
- Pydantic AI

The Future is Interoperable¶

The excitement surrounding Google's A2A protocol clearly indicates a strong belief in its potential to revolutionize multi-agent AI systems. By providing a standardized way for AI agents to communicate and collaborate, A2A is poised to unlock new levels of automation and innovation. As enterprises increasingly adopt AI agents, A2A represents a crucial step towards realizing the full power of interconnected AI ecosystems.

Join the growing community building the future of AI interoperability with A2A!