Technology is at an Inflection Point. The FTC is on the Front Lines.

Tech-Related Programmatic Advances at the FTC
(June 2021 - January 2025)

We are at a major technological inflection point. The rise of AI and algorithmic decision-making will shape the economy, and the consumer experience, for decades to come. In order to face these challenges most effectively, we need to understand the technology behind them.

The FTC established the Office of Technology to shore up tech expertise within the agency. Our in-house tech experts work directly with attorneys in the Consumer Protection and Competition Bureaus to look around the corner and anticipate the challenges and opportunities posed by technology.

- Cracked down on illegal tech practices through enforcement actions.
- Designed upstream remedies that get at root causes of harms.
- Adopted baseline data minimization principles to limit what firms can collect, retain, and share.
- Took action against companies' use of sensitive geolocation, health, and browsing data.
- Litigated cases to promote competition in the tech sector.
- Took action against dark pattern design practices.
- Required strong protections for kids and teens in online environments and services.
- Strengthened the FTC's digital capacity to keep pace with evolving technology and market realities.
- Held companies accountable for misleading claims, ensuring they live up to their promises.
- Advanced the agency's tech stack expertise through hardware & infrastructure knowledge.
- Emphasized holding both firms and individuals accountable for illegal practices.
- Elevated voices of consumers, businesses, experts, researchers, and advocates to understand the impact of complex harms on society.
- Ensured fair competition for a thriving, innovative tech landscape.
- Reinforced that the existing laws on the books apply to new technologies.
- Strengthened security practices and addressing risks systematically.
- Limited commercial surveillance by uncovering hidden middlemen layers of the economy.
- Advanced research and facilitated discussion of critical tech topics.
- Proactively identified ways AI can be used to supercharge scams.

The FTC has cracked down on illegal tech practices through enforcement actions and designed upstream remedies that get at the root cause of harm.

- **Established bans of products, or the marketing, offering, selling, or advertising of a product.**
  - Banned Rite Aid from using facial recognition technologies that the Commission alleged had wrongly accused innocent people—including children and mostly people of color—of shoplifting.
  - Banned NGL Labs from offering or promoting anonymous messaging apps to users under the age of 18 that the Commission alleged were unfairly marketed to kids and teens and sent fake messages to drive up usage.
  - Banned SpyFone and its CEO from the surveillance business over allegations that the stalkerware app company secretly harvested and shared data on people's physical movements, phone use, and online activities through a hidden devices hack.
  - Banned General Motors (GM) and OnStar from disclosing consumers' sensitive geolocation and driver behavior data to consumer reporting agencies for five years, over allegations they collected, used, and sold drivers' precise geolocation data and driving behavior information from millions of vehicles—data that can be used to set insurance rates—without adequately notifying consumers and obtaining their affirmative consent.

- **Adopted various baseline data minimization principles to limit what firms can use, collect, retain and share.**
  - Restricted companies from unlawful use, sale, licensing or collection of data.[1]
  - Restricted companies from certain data collection.[2]
  - Restricted the disclosure or sale of data for certain purposes.[3]
  - Required companies to create strong data retention schedules or minimize the data they collect in the first place.[4]
  - Required deletion of the data that the company improperly obtained, for example by using unfair or deceptive practices, or improperly retained.[5]
  - Required deletion of models or algorithms trained on improperly obtained or retained data, such as when the user did not agree to allow data to be used this way.[6]

[1] Avast, Cerebral, BetterHelp, GoodRx, Premom, InMarket, X–Mode Social

[2] Mobilewalla, Cerebral, Drizly, InMarket, Epic Games

[3] InMarket, Avast, GoodRx, BetterHelp, Premom, X-Mode Social

[4] CafePress, Drizly, Chegg, Cerebral, Premom, BetterHelp, Kurbo/WeightWatchers, 1Health.io/Vitagene, Blackbaud, Global Tel*Link

[5] SpyFone, Equifax, Drizly, FloHealth, 1Health.io / Vitagene, BetterHelp, Premom, NGL Labs, InMarket, Avast, Blackbaud, Global Tel*Link, Cerebral, X-Mode Social, RiteAid, Ring, Amazon Alexa

[6] Avast, Amazon Alexa, Kurbo/WeightWatchers, Ring, Edmodo

    - Finalized updates to the COPPA Rule to make clear that indefinite retention is unlawful, and firms should retain personal information only for as long as necessary to fulfill the original purpose.

    - Issued an Education Technology Policy Statement making clear that EdTech providers cannot condition access to educational tools on collecting more information than is reasonably necessary.

- **Took action against companies' use of sensitive geolocation, health, and browsing data.**

    - **Brought actions against multiple mass data collectors**, highlighting that browsing and location data are sensitive—full stop.[7]

    - **Secured orders banning the sharing of sensitive health data for advertising purposes.**[8]

- **Litigated cases to promote competition in the tech sector.**

    - Sued Amazon for allegedly illegally maintaining monopoly power, including through the use of algorithms to prevent third-party sellers from offering discounted prices on competing sites.

    - Continued the case against Meta (initiated under prior Chair Simons) for allegedly maintaining a personal social networking monopoly with its acquisitions of WhatsApp and Instagram.

    - Challenged Nvidia's attempted acquisition of Arm, the biggest semiconductor merger ever proposed, alleging it would lock up key inputs and make it harder for startups to develop innovative new technologies, like self-driving cars.

    - Sued John Deere for allegedly using its market power to prevent farmers and independent repair providers from performing the full range of repair services as a result of Deere's software policies.

- **Took action against dark pattern design practices.**

    - Restricted companies from obtaining consent through a user interface that has the effect of subverting or impairing user autonomy, decision-making, or choice.[9]

    - Took action against Vonage, alleging that the company used dark patterns to create obstacles to those who try to cancel their service and unfairly charging consumers without consent.

    - Brought a major action against Amazon alleging that the company deployed dark patterns to enroll consumers into its Prime program while making it difficult to cancel their subscriptions.

[7] Avast, X-Mode, InMarket, Kochava

[8] GoodRx, Premom, Monument, Cerebral, BetterHelp, FloHealth

[9] GoodRx, Premom, Monument, Cerebral, BetterHelp

    - Promulgated the Click to Cancel Rule requiring that companies must make subscriptions as easy to cancel as they are to enroll in.
    - Took action against Cognosphere, maker of the Genshin Impact video game, banning it from making misrepresentations about Loot Boxes and requiring the option to purchase them directly with real money.

- **Required strong protections for kids and teens in online environments and services.**
    - Required Epic Games to adopt stronger default privacy settings for children and teens on Fortnite.
    - Banned NGL Labs and its founders from offering anonymous messaging apps to kids under 18, and held NGL accountable for its alleged false claims that its AI content moderation program filtered out cyberbullying.
    - Alleged that TikTok was violating children's privacy laws, leading to a Justice Department lawsuit filed on behalf of the Commission.
    - Referred to the Department of Justice a complaint against Snap, Inc., pertaining to the company's deployment of an artificial intelligence powered chatbot, My AI, in its Snapchat application and the allegedly resulting risks and harms to young users of the application.

- **Emphasized holding both firms and individuals accountable for illegal practices.**
    - Banned SpyFone—a stalkerware app that allegedly collected data on people's movements, phone use, and online activities—and its CEO from entering the surveillance business again, in addition to requiring the company to delete illegally harvested information.
    - Held the CEO of alcohol delivery firm Drizly personally liable for alleged cybersecurity failures.
    - Took action against ITMedia and multiple executives for allegedly manipulating consumers into turning over sensitive financial information and then selling that data to marketers.

Strengthened the FTC's digital capacity to keep pace with evolving technology & market realities.

- Launched the agency's first Office of Technology (OT) to bring AI and technological expertise in-house, including software and privacy engineers, user experience researchers, data scientists, investigative journalists, and other experts, led by Chief Technologist Stephanie T. Nguyen.

- Strengthened foundations and pathways for public interest technologists in government by codifying insights learned in building the Office of Technology through a staff report on *Building Tech Capacity in Law Enforcement Agencies*.

- Hosted the FTC's first *Technology Forum* with 21 international competition agencies to share best practices and knowledge of tech-related topics, exchange tactics on how to keep pace with the increasing digitization of the economy, and strategize on how to continue to build technical capacity.

- Published a joint statement of principles with 24 member countries of the International Competition Network committed to continuing to strengthen its technical capacity.

- Collaborated with several U.S. federal and state agencies to release agency-specific action statements on strengthening tech capacity—including concrete actions like actively hiring technologists.[10]

- Clarified Ethics guidance FAQs in order to better ensure that talented candidates can better assess the opportunities in working for federal government enforcement agencies.

Held companies accountable for misleading claims, ensuring they live up to their promises.

- Launched a law enforcement sweep called Operation AI Comply to address, among other things, deceptive claims and practices relating to AI.[11]

- Explained in a staff blog that most services that provide "Data Clean Rooms" are not necessarily privacy-preserving—and just like other technologies that claim to protect privacy, can be used to obfuscate privacy harms.

- Reinforced in a staff blog that hashing doesn't make your data anonymous, and can still be used to identify users, and their misuse can lead to harm. The staff blog also warned that companies should not act or claim as if hashing personal information renders it anonymized.

- Published a staff blog that made clear that not all Privacy Enhancing Technologies (PETs) are fully private, and companies making representations to consumers about their use of PETs must ensure that any privacy claims or representations are accurate.

Advanced the agency's tech stack expertise through hardware & infrastructure knowledge.

- Launched a Cloud Computing Request for Information ("RFI"), published the analysis after a presentation at an Open Commission Meeting, and hosted a public panel of experts examining four specific areas (competition, single points of failure, security, and AI).

- Facilitated public dialogue through the FTC Tech Summit on AI amid a dynamic innovation landscape, focused on generative AI across the layers of technology, from hardware and computer infrastructure to consumer applications and devices.

Elevated voices of consumers, businesses, experts, researchers, and advocates to understand the impact of complex harms on society.

- Published a staff report that compiled the voices of everyday Americans who experience the effects of innovation in real-time in three easy-to-parse "quote books" for policymakers, summarizing statements from the wide range of participants in the FTC Tech Summit on AI on

[10] CFPB, FCC, EEOC, NLRB, CPPA, and Census.

[11] Automaters AI, Rytr, DoNotPay, Ascend Ecom, Empire Holdings, FBA Machine/Passive Scaling, IntelliVision, Evolv.

the different layers of the AI tech stack: Chips & Cloud Computing, Data & Models, and Consumer-Facing Applications.

- Staff brought clarity to policy- and decision-makers on how different lines of work for creative professionals are being reshaped by generative AI, through a roundtable with a dozen creative professionals and a companion Staff Report & Quote Book, which identified themes and associated statements from the discussion.
    - Assisted in submitting a staff public comment to the U.S. Copyright Office on behalf of the FTC, further elevating the voices of those creative professionals.

- Published a staff blog analyzing and summarizing thousands of reports related to AI from everyday consumers who are worried about their data being indiscriminately used to train AI; about the bias, inaccuracies, and their inability to appeal bad decisions made by AI; and about the misuse of AI for fraud and scams that they are already experiencing.

Ensured fair competition for a thriving, innovative tech landscape.

- Staff reinforced that Interoperability, Privacy, & Security are not inherently at odds, and any claims to that effect will be scrutinized to ensure they are not pretext for anticompetitive practices.

- Staff flagged that there are many ways in which Generative AI Raises Competition Concerns, from bundling and tying of products by market leaders, to exclusive dealing and discriminatory behaviors—especially from companies that hold control over key inputs to Generative AI systems—to mergers and acquisitions to consolidate market power and stifle innovation.

- Deepened our understanding of the competition considerations and impact surrounding investments and partnerships related to Generative AI through the AI Investments & Partnerships 6(b) Study, culminating in a Staff Report, which highlights, among other things, key terms of the AI partnerships and areas to watch moving forward.

- Joined the Justice Department in submitting a Statement of Interest in a hotel room algorithmic price-fixing case, explaining that hotel companies cannot use algorithms to evade antitrust laws.

- Staff discussed the benefits and pitfalls of Open-Weights Foundation Models—from both a competition and consumer protection perspective—expanding on Chair Khan's Remarks at the January Tech Summit on AI that highlighted the need to scrutinize any existing or emerging bottlenecks across the AI stack to promote healthy competition; focusing on how business models drive incentives; aligning liability with capability and control; and, crafting effective remedies that establish bright-line rules on the development, use and management of AI inputs.

Limited commercial surveillance by uncovering hidden middlemen layers of the economy.

- Initiated a Surveillance Pricing 6(b) study and issued orders to intermediary companies regarding their use of surveillance pricing technology that use personal data, including finances and browser history, to set individualized prices for the same goods or services.

  - Staff wrote a blog post explaining the FTC's Inquiry into Surveillance Pricing Practices, covering both how this practice has evolved over time and how recent technological developments, such as machine learning, can help transform targeted pricing into surveillance pricing.

  - Published staff's Surveillance Pricing Research Summaries, highlighting initial findings of the Surveillance Pricing 6(b) study, a working prototype designed to showcase ideas and emerging findings, facilitate early engagement and collaboration within the research community, present general learnings in service of increased transparency to the public, and address the time-sensitivity of a quickly moving technological landscape.

  - Released a Surveillance Pricing Request for Information, inviting public comments on surveillance pricing to better understand the opaque market for products and services that collect and use personal data to allow firms to set individualized/differing prices for the same goods or services.

  - Published staff's Surveillance Pricing Issue Spotlight, an overview of publicly available information from both industry and academia, focusing on the documented growth of surveillance pricing as well as its scope and impacts on consumers.

  - Staff created a Surveillance Pricing resources landing page to aggregate resources on the FTC's research, inquiries, and statements about surveillance pricing practices.

- Published a staff blog on Unpacking Real Time Bidding through enforcement action against Mobilewalla, a data broker that the Commission alleged engaged in problematic data practices including sensitive location information. The blog discussed the concerns—such as how RTB incentivizes invasive data sharing—and technical difficulties associated with protecting the vast amounts of data that is transacted through ad exchanges.

- Staff reinforced the agency's focus on connected cars, tying findings from recent actions taken against data aggregators and mass data collectors and concerns surrounding Cars & Consumer Data, thus bringing more clarity to the industry on potentially unlawful collection and use practices.

- Published a staff blog about three enforcement actions against mass data collectors,[12] highlighting that the original purpose of data collection matters, location and browsing data are sensitive, and that companies need to live up to their promises and obligations surrounding privacy.

- Published a staff blog explaining how Pixel Tracking, the key technology at issue in the GoodRx and BetterHelp cases, works and its hidden impact, including that it creates an invisible data collection apparatus to collect large amounts of potentially sensitive data from consumers without their awareness.

Reinforced that the existing laws on books apply to new technologies.

[12] Avast, X-Mode, and InMarket

- Published a staff blog making clear that even when technology and markets change, the authorities granted by the FTC Act remain steadfast; and that not upholding, or quietly changing, commitments made to consumers may be found to be unfair or deceptive practices.

- Chair released a joint statement on AI with DOJ, EEOC, and CFPB describing potential AI-driven harms such as illegal discrimination, and outlined a commitment to enforce the agencies' respective laws and regulations to promote responsible innovation in automated systems.

Strengthened security practices & addressing risks systematically.

- Staff presented at the December 2022 Open Commission meeting on the FTC's efforts to refine its approach to data security by building on the solid foundations of safety engineering and a set of controls that address risks systemically—highlighting the Commission's efforts to keep pace with technological developments, learn from past experiences, and strengthen remedies to address root causes, even as technologies evolve.

- Staff communicated to the broader market some reasonable steps that can be taken to avoid outages and prevent widespread system failures—treating code, configuration files, and data changes with the same care as introducing changes via batched rollouts, while also preempting arguments that would pit reliability against interoperability.

- Staff created clarity on minimum security principles and expectations through a series of blogposts summarizing previous order requirements and best practices to systematically address the risk of security vulnerabilities.

  - In its first iteration, Security Principles: Addressing underlying causes of risk in complex systems, staff focused on basic requirements that can provide significant security improvements over the current status quo. Those included offering multi-factor authentication (MFA) for consumers and requiring it for employees, to reduce the odds that an account will be taken over; requiring that connections within a company's systems must be both encrypted and authenticated, in line with the principle of "zero trust"; and requiring companies to develop a data retention schedule, publish it, and then stick to it, as the most secure data is the data that's not stored at all.

  - In its second iteration, Security Principles: Addressing Vulnerabilities Systematically, staff focused on the most prevalent types of vulnerabilities and known approaches to address them. We focused on Cross Site Scripting (XSS), SQL injection, and buffer overflows and use-after-free vulnerabilities.

  - In its most recent iteration, Lenses of security: Preventing and mitigating digital security risks through data management, software development, and product design for humans, we covered reasonable steps that can be taken throughout the software lifecycle, reinforcing previously stated steps—multi-factor authentication, encryption, and data retention—as well as other steps like using memory-safe programming languages, limiting third-party data sharing, and not using dark patterns.

- Staff drafted remedies that get at the root cause of the issues at hand while still strengthening security practices, such as mandating multi-factor authentication modes that would prevent companies from repurposing data collected to enhance security for secondary purposes, as highlighted in On FTC's Twitter Case: Enhancing Security Without Compromising Privacy

- Staff highlighted the importance of security breach detection and response to a reasonable security program, impacting not only the company's ability to better respond and prevent against future breaches, but also consumers' ability to mitigate harm from the breach. This makes the lack, or poor implementation, of these security functions a potential law violation.

- Published a staff blog that warned companies to remediate Log4j security vulnerability, providing actionable steps for companies to take and highlighting that companies have a duty to take reasonable steps to mitigate known software vulnerabilities.

Advanced research and facilitated discussion of critical tech topics.

- Staff guided the direction of external research efforts towards thorny topics that, if better understood, can help law enforcement protect consumers and promote healthy competition, by releasing a series of research topics of interest to agency staff.

    - Starting from a focus on pixel tracking, in Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking staff proposed five areas where continued research may be beneficial, including industry conditions and competitive dynamics; consumer harms; business rationales; data processing, use, and monetization; and data retention and management.

    - Through P = NP? Not exactly, but here are some research questions from the Office of Technology, staff published a blog to highlight emerging areas that could benefit from further research and insights. Topics include AI-enabled fraud and scams; AI and competition; algorithmic pricing; surveillance and data privacy; data security; open models; platform design; and digital capacity.

    - Published staff research blog: Solving the Traveling Salesman Problem? Not quite, but here are more research questions from the Office of Technology, with topics including AI & competition; AI procurement; commercial surveillance and data privacy; tech investors; hardware and manufacturing; and building digital capacity.

- Staff hosted the 8th PrivacyCon, bringing together a diverse group of stakeholders including academics, researchers, industry representatives, consumer advocates, and government regulators to critically engage with the latest research and trends related to consumer privacy and data security.

- The Commission issued a report to Congress warning about using artificial intelligence (AI) to combat online problems, outlining significant concerns that AI tools can be inaccurate, biased, and discriminatory by design and incentivize relying on increasingly invasive forms of commercial surveillance, but acknowledging that given that major tech platforms and others are already using AI tools to address online harms, lawmakers should consider focusing on developing legal frameworks that would ensure that AI tools do not cause additional harm.

Proactively identified ways that AI can be used to supercharge scams, staying vigilant in its bread–and–butter work to fight scams.

- Included language in the "Fake Reviews and Testimonials" rule that makes clear AI-generated reviews are covered by the final rule, and which should deter the use of AI for that illicit purpose.

- Charged Rytr with violating the FTC Act by allegedly providing subscribers with the means to generate false and deceptive written content for consumer reviews with its AI "writing assistant" service.

- Encouraged the development of multidisciplinary approaches to address AI-enabled voice cloning by launching an exploratory challenge to identify ways to protect consumers from the harms from this new technology, such as fraud and the broader misuse of biometric data and creative content.

- Sought public comment on a supplemental notice of proposed rulemaking that would prohibit the impersonation of individuals—motivated by the surging complaints around impersonation fraud, as well as public outcry about the harms caused to consumers and to impersonated individuals.

- Amended the Telemarketing Sales Rule in ways that will help ensure the FTC can take action against deceptive marketers who use AI robocalls.

***