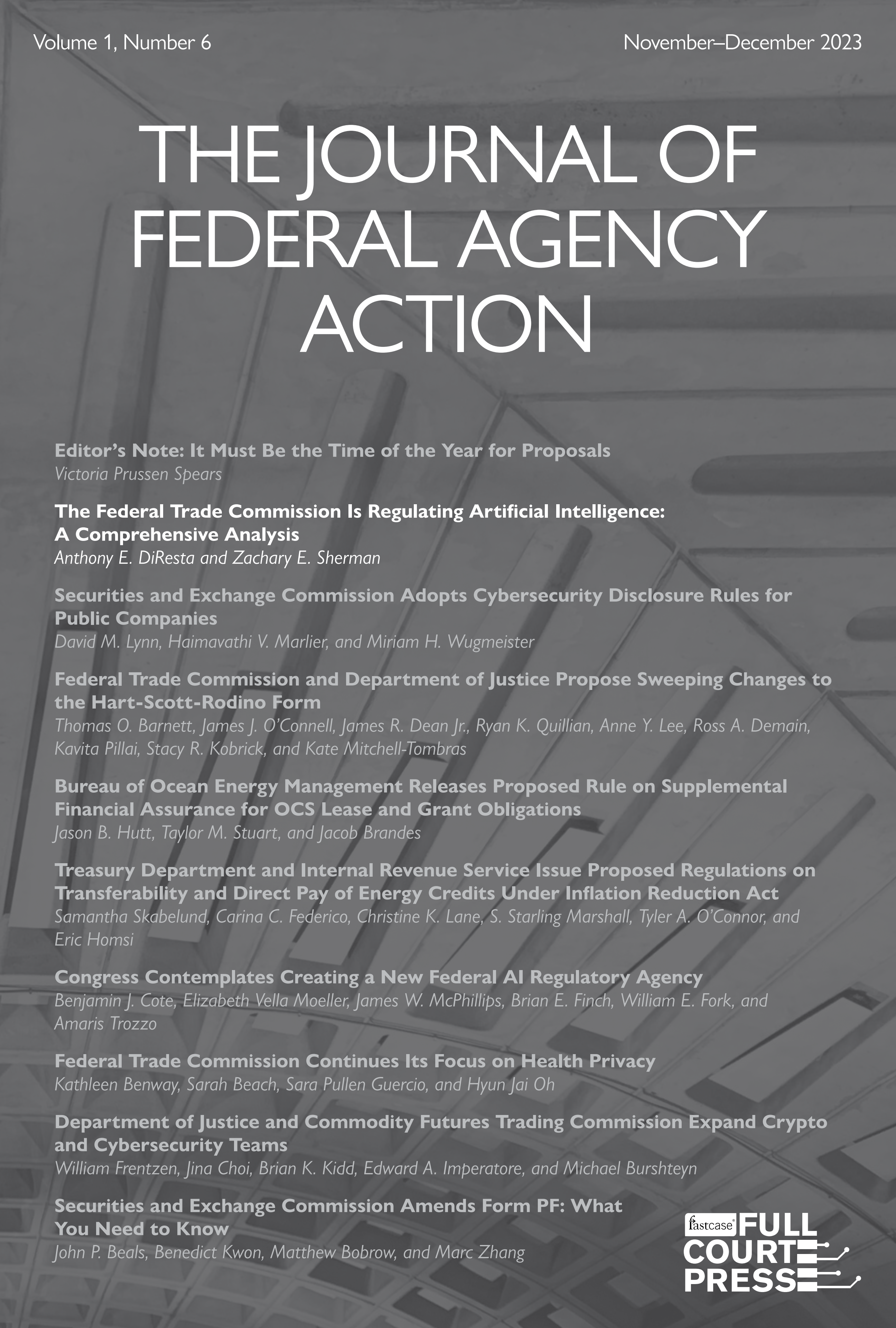

Volume 1, Number 6 November–December 2023

THE JOURNAL OF FEDERAL AGENCY ACTION

fastcase FULL COURT PRESS

The Journal of Federal Agency Action

Volume 1, No. 6 | November–December 2023

THE JOURNAL OF FEDERAL AGENCY ACTION (ISSN 2834-8796 (print) / ISSN 2834-8818 (online)) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2023 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

This journal's cover includes a photo of Washington D.C.'s Metro Center underground station. The Metro's distinctive coffered and vaulted ceilings were designed by Harry Weese in 1969. They are one of the United States' most iconic examples of the brutalist design style often associated with federal administrative buildings. The photographer is by XH_S on Unsplash, used with permission.

Cite this publication as:

The Journal of Federal Agency Action (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF FEDERAL AGENCY ACTION, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and anyone interested in federal agency actions.

This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2834-8796 (print)
ISSN 2834-8818 (online)

The Federal Trade Commission Is Regulating Artificial Intelligence: A Comprehensive Analysis

Anthony E. DiResta and Zachary E. Sherman*

In this article, the authors discuss how the Federal Trade Commission has recognized the need for, and has implemented, regulation and oversight of artificial intelligence (AI) technology as companies increasingly develop or apply AI solutions to their platforms.

Artificial intelligence (AI) is rewriting norms and changing the way we interact with the world. It is likely AI will have an outsized impact on every facet of life; this could be the start of the next technological revolution. This article discusses how the Federal Trade Commission (FTC) has recognized the need for regulation and oversight of this nascent technology as companies increasingly develop or apply AI solutions to their platforms.

The relevant sources of information used in this article include:

- FTC reports to Congress,
- FTC business blogs and business guidance,
- FTC press releases and joint statements,
- FTC enforcement actions,
- Case law,
- Law review and journal articles,
- Statements by FTC commissioners and testimony to Congress, and
- Interview with FTC attorney Michael Atleson.

FTC Authority

"The FTC's mission is protecting the public from deceptive or unfair business practices and from unfair methods of competition through law enforcement, advocacy, research, and education."[1] The

The Journal of Federal Agency Action / November–December 2023, Vol. 1, No. 6, pp. 425–441.

ISSN 2834-8796 (print) /ISSN ISSN 2834-8818 (online).

FTC derives much of its authority from the FTC Act. The majority of FTC enforcement actions stem from deceptive business practices or unfair business practices. The FTC also has a role regulating and enforcing antitrust concerns.

Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." Deceptive omissions of material facts and misrepresentations are also "deceptive acts or practices" prohibited by Section 5(a). "Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n)."[2]

Section 5(a) also prohibits "unfair methods of competition." Unfair methods of competition include any conduct that would violate the Sherman Antitrust Act or the Clayton Act.[3] While AI and its related technologies may be new, the tools the FTC possess to regulate them are not.

Definition of AI

Defining the term "AI" is an arduous task. The *Encyclopaedia Britannica* defines AI as: "the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings."[4] Congress has defined AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."[5] AI has been viewed as an infrastructure, a scientific discipline, a computational concept, or as the application of discrete algorithms.

The FTC has emphasized that pigeonholing AI, by a definition, into one of these specific buckets, is not useful in accomplishing its regulatory mission. The FTC admits that its discussion of AI, at times, may or may not fit into one of the more specific definitions of the term. In 2022, the FTC submitted a report to Congress, focused on AI. In that report, the FTC stated that it "assume[s] that Congress is less concerned with whether a given tool fits within a definition of AI.... In other words, what matters more is output and impact."[6] As such, the FTC mentions some products or tools it considers within the AI regulatory framework that are not necessarily AI by a stricter definition. By design, the FTC broadens the scope of products it regulates under the AI umbrella. The FTC uses terms such as "automated detection tool" or "automated decision system," noting that these systems "may or may not involve actual or claimed use of AI."[7]

AI Through the Lens of FTC Legal Authority

Deception and Misleading Claims

A claim is deceptive if it lacks scientific support—or if the claim applies only in certain conditions or to certain users. The FTC wants the business world on notice that "for FTC enforcement purposes—false[,] [] unsubstantiated [,or deceptive] claims about a product's efficacy are our bread and butter."[8]

Companies have begun promising that AI products are better than non-AI products. The FTC has noticed. Michael Atleson, an FTC attorney involved in AI issues, has discussed how AI fits within the FTC's existing deception and misleading claims framework. Whenever a business makes a qualitative claim, the FTC will require "adequate proof" of the truthfulness of the claim.[9] In Atleson's business blog, *Keep Your AI Claims in Check*, he emphasizes that for superiority or "better than" claims, the FTC will want specific evidence showing that the AI product is qualitatively superior to the non-AI product.[10]

The FTC has seen companies attempting to shift liability by claiming that the technology they are promoting is a "black box" that the company is incapable of understanding "or didn't know how to test."[11] The FTC employs a reasonably foreseeable standard: If the risk of deception associated with the offered products are reasonably foreseeable, the FTC will pursue liability.[12] If a company is going to offer the product, it cannot claim ignorance of the product's capabilities as a defense to a deception charge—irrespective of the complexity (true or alleged) of the product.

A clearly deceptive practice is claiming a product uses AI when in fact it does not. The FTC can analyze the offered product "to see if what's inside matches up with your claims."[13] Here, the FTC's burden is low. It is not proving a company had a duty to know its claim was false within a reasonable foreseeability. The FTC just has to prove that the claim itself is patently false or misleading.[14] In the same vein, the FTC warns companies to "be careful not to mislead consumers about the nature of [an] interaction" with AI.[15] The example that the FTC guidance provides is an AI interaction with consumers via chatbots.[16] To avoid misleading the consumer, the FTC states a company should make it clear that the customer is not interacting with a human representative.[17]

Even when a product or tool is accidentally or unwittingly deceptive, the FTC Act's prohibition on deceptive conduct may still apply.[18] If the tool is effectively designed to deceive, even if that is not the tool's intended or sole purpose, the FTC may have a strong basis to bring an enforcement action.[19]

In Atleson's business blog *Chatbots, Deepfakes, and Voice Clones: AI Deception for Sale* he cautions companies to "[c]onsider at the design stage and thereafter the reasonably foreseeable . . . ways it could be misused for fraud or cause other harm. Then ask . . . whether such risks are high enough that you shouldn't offer the product at all."[20] The FTC has brought actions against businesses that sold or distributed potentially harmful technology when the business had not taken reasonable measures to prevent injury to consumers.[21] As such, "deterrence measures should be durable, built-in features and not bug corrections or optional features that third parties can undermine via modification or removal."[22] Regarding advertisers on social media platforms: misleading followers through deepfakes, chatbots, fake dating profiles, and more "could result—and in fact have resulted—in FTC enforcement actions."[23]

Unfair Business Practices

"An act or practice is 'unfair' if it 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'"[24] Congress has asked the FTC, through this statutory lens, to closely watch AI applications for misuse and abuse. Specifically, in 2021, Congress asked the FTC to investigate "whether and how" AI could be utilized to "address a wide variety of specified 'online harms.'"[25] In June 2022, the FTC submitted a report to Congress titled "Combating Online Harms Through Innovation." In that report, the FTC underscores that AI and algorithmic models are the product of inputs. Just like their human inventors and operators, "unrepresentative datasets, faulty classifications, failure to identify new phenomena, missing context, and flawed design, can lead to biased, discriminatory, or unfair outcomes."[26]

Bias and Discrimination

The FTC is increasingly worried about inaccuracy, bias, and discrimination in AI tools. The FTC, Consumer Financial Protection Bureau (CFPB), U.S. Department of Justice, and U.S. Equal Employment Opportunity Commission (EEOC) released a joint statement on "Enforcement Efforts Against Discrimination and Bias in Automated Systems." Citing the FTC report to Congress discussed above, the statement warned that AI may contribute to unlawful discrimination via:

- *Data and Data Sets*. Automated system outcomes can be skewed by unrepresentative or imbalanced data sets, data sets that incorporate historical bias, or data sets that contain other types of errors. Automated systems also can correlate data with protected classes, which can lead to discriminatory outcomes.
- *Model Opacity and Access*. Many automated systems are "black boxes" whose internal workings are not clear to most people and, in some cases, even the developer of the tool. This lack of transparency often makes it all the more difficult for developers, businesses, and individuals to know whether an automated system is fair.
- *Design and Use*. Developers do not always understand or account for the contexts in which private or public entities will use their automated systems. Developers may design a system on the basis of flawed assumptions about its users, relevant context, or the underlying practices or procedures it may replace.[27]

While the FTC has gone to great pains on various iterations of press releases, reports, and business guidance documents to warn *how* AI and its inputs may result in outcomes such as unfair business practices, bias, or discrimination, decoding how the FTC will regulate these outcomes remains simple.

If an AI or algorithm "causes or is likely to cause substantial injury to consumers,"[28] the FTC has a strong basis on which to bring an enforcement action. The FTC warns that, under the Federal

Credit Reporting Act, “a vendor that assembles consumer information to automate decision-making about eligibility for credit, employment, insurance, housing, or similar benefits and transactions, may be a ‘consumer reporting agency.’”[29]

Even remote interaction with an AI tool may require a company to provide a consumer with an adverse notice action.[30] An example of such a remote interaction would be denying an individual a product (such as a mortgage) based on a background check, when the background check was created in whole, or in part, by AI. Any denial, and subsequent adverse notice action, must explain why the consumer was denied the service or product. Therefore, the FTC has advised that when you are using AI, “you must be able to explain [it, so] . . . consider how you would explain your decision to your customer if asked.”[31]

Lack of Transparency

Transparency takes two forms: internal and external.

Internal

An internal lack of transparency may occur due to the unique technical complexity of AI tools and products. It is not uncommon for companies to claim that the AI or algorithm that they employ is a “black box.” When faced with an FTC enforcement charge, attempting to state that a company or its employees were unable to understand the AI, or how it reached a given output, are not viable defenses. If the system is not immediately transparent, the company must invest in training, so employees understand how the AI operates.

External

In an interview, FTC attorney Michael Atleson stated that the FTC has not publicly waded into specific standards that a company must follow to be sufficiently, externally transparent. Atleson emphasized that “transparency is not the be all end all, it is just a first step.” However, the FTC has released three best practices to follow:

1. Test your algorithm—before you use it, and periodically after—to make sure it doesn’t discriminate,[32]

2. "Embrace transparency … conduct[] and publish[] the results of independent audits … [and] open[] your data or source code to outside inspection,"[33] and
3. Tell the truth about how your company uses data.[34]

Integrity of Data Sets

Cybersecurity matters to a company's bottom line, to its trust and reputation with consumers, and to its legal liability. The integrity, or safety, of the data that a company stores and uses will be closely scrutinized by the FTC. The FTC has said that safety measures should be "durable, built-in features" designed to prevent injury to consumers.[35]

A company carries an obligation to make sure its use or marketing of an AI product or service does not cause cognizable harm. Atleson emphasized that, in this context, judgments of data integrity are done on a case-by-case basis. There is no guide or specific set of practices to follow. The question the FTC will ask is: Was the harm or outcome "reasonably foreseeable" and could the company "have done anything about that foreseeability"? Atleson stated that the FTC is developing its jurisprudence in this area in the same manner that it developed its "reasonable data security" jurisprudence.[36] Atleson made a reference to how common law has already been built up in this regard and that the FTC has provided significant guidance.[37] It is not that a company experienced a breach that makes it liable; liability comes from a failure to follow "reasonable practices."

Duty to Monitor AI Products and Misuse of AI

The FTC has emphasized that it is looking for "real accountability" when it comes to algorithmic harms. To the FTC, "real accountability" means that "companies—the same ones that benefit from the advantages and efficiencies of algorithms—must bear the responsibility of (1) conducting regular audits and impact assessments and (2) facilitating appropriate redress for erroneous or unfair algorithmic decisions."[38] This is a crucial point for the agency[39] and seems bound for increased attention.[40]

Misuse of AI can be on the border of illegality or it can be relatively accidental. Misuse can happen by the producer of the AI or by a downstream firm. Companies are generally at a larger risk of accidental, or unknowing, misuse when they hire third-party vendors to provide the AI technology. Atleson was asked whether a company that had hired a third-party AI vendor had a duty to conduct due diligence and subsequently monitor and oversee the AI. Atleson stated, companies "can't hide behind or point fingers at a vendor, they are still on the hook." The best way to defend yourself, he said, was "to show that you did due diligence in determining which vendor you were going to use, to show you were monitoring the usage [of the AI] yourself or getting reports [about the AI] you could rely upon." Atleson clarified that the FTC has not enumerated any "specific standards," but said his suggestions "stand as a few possible best practices."

In May 2023, the FTC released a policy statement regarding the misuses of biometric information and potential harms to consumers. Samuel Levine, director of the FTC's Bureau of Consumer Protection, stated that the policy statement "makes clear that companies must comply with the law regardless of the technology they are using."[41] The FTC noted that it "would consider several factors in determining whether a business's use of biometric information or biometric information technology could be unfair in violation of the FTC Act."[42] These factors, which are generally applicable to AI technology in general, follow:

1. Failing to assess foreseeable harms to consumers before collecting biometric information;
2. Failing to promptly address known or foreseeable risks and identify and implement tools for reducing or elimination those risks;
3. Engaging in surreptitious and unexpected collection or use of biometric information;
4. Failing to evaluate the practices and capabilities of third parties, including affiliates, vendors, and end users, who will be given access to consumers' biometric information or will be charged with operating biometric information technologies;
5. Failing to provide appropriate training for employees and contractors whose job duties involve interacting with biometric information or technologies that use such information; and
6. Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or uses, in connection with biometric information to ensure that the

> technologies are functioning as anticipated and that the technologies are not likely to harm consumers.[43]

Use of Disclaimers

A false statement or communication about a product or service is a direct violation of 15 U.S.C. Sec. 45(n). It is an unfair business practice. Disclaimers serve the same purpose. If there is reasonable ambiguity regarding what a product or service may or may not do, it is likely necessary that an adequate disclaimer accompany it.

The efficacy of disclaimers, in the AI space, has not yet been tested by FTC enforcement action. Atleson has stated that the FTC is aware that disclosure regimes and notice and choice regimes may not be effective, and noted that Chairwoman Lina Kahn has been clear in her hope for more substantive legislation. Atleson clarified this meant regulation that would strictly prohibit companies from doing certain, statutorily enumerated, harmful acts.

To err on the side of caution, companies should provide disclaimers that are as accurate and effective as possible. That is likely why OpenAI, conspicuously, on the front page of its tool ChatGPT, has stated "limitations."[44] These limitations state that ChatGPT may (1) "occasionally generate false information," (2) "occasionally produce harmful instructions or biased content," and (3) has "limited knowledge of world events after 2021."[45] It is unknown whether the FTC or courts would consider these disclaimers effective, but they may definitely serve as the floor of plausible acceptability.

Marketplace Concerns

The FTC has witnessed a multitude of technological revolutions since its inception in 1914. One relatively recent advancement is at the top of FTC Chairwoman Khan's mind: the Web 2.0 era of the mid-2000s. Khan hopes that the FTC has "learned its lesson" from the historic rise of technology companies and platforms. "What we initially conceived of as free services were monetized through extensive surveillance of the people and businesses that used them. . . . What began as a revolutionary set of technologies ended up concentrating enormous private power over key services . . . at extraordinary cost to our privacy and security."[46] Khan worries that "[t]he expanding adoption of A.I. risks further locking in the market dominance of large incumbent technology firms," allowing them to "exclude or discriminate against downstream rivals" that can "facilitate collusive behavior."[47]

Khan has noted that "the A.I. tools that firms use to set prices for everything from laundry detergent to bowling lane reservations can facilitate collusive behavior that unfairly inflates prices—as well as forms of precisely targeted price discrimination."[48] While firms may have not yet found a way to employ AI in a monopolistic manner, as the technology advances and becomes more ingrained in businesses' operations, the FTC will keep a wary eye on this potential. While outside the scope of this memorandum, the FTC has increased its antitrust vigilance of big technology companies.[49]

Enforcement Actions and Algorithmic Deletion

"There is *no AI exemption to the laws on the books*, and the FTC will *vigorously enforce* the law to combat unfair or deceptive practices or unfair methods of competition."[50] "Although [AI] is novel, [it is] not exempt from existing rules, and the F.T.C. will vigorously enforce the laws we are charged with administering."[51] Both sentences are quotations from Chairwoman Khan. Both emphasize that the FTC will vigorously enforce AI with the existing tools in its toolkit. Not only is the FTC confident in its ability to regulate new and novel uses of AI with its existing regulatory instruments, as noted, it is confident that it has learned lessons from its failure to vigorously enforce the Web 2.0 era.

Algorithmic Deletion[52]

Economic profit linked to the use of data obtained fraudulently or misleadingly is skyrocketing. AI is trained and improved by feeding vast amounts of data into the operating system. This is the "machine learning" part of AI. The FTC is tinkering with new tools. The FTC hopes companies violating consumer privacy to cheaply train their AI may think twice because the punishment is becoming more severe.

"Algorithmic [deletion], also known as algorithmic destruction or model destruction, is the ordered deletion of computer data models or algorithms that were developed with improperly obtained data."[53] Essentially, algorithmic deletion requires a company to destroy an entire AI or algorithmic product or tool that the company has developed, if the company developed the product or tool with improperly obtained data.

Between 2019 and 2022, the FTC reached three settlements with remedies that included algorithmic deletion. This new enforcement tool burst onto the scene in the much-publicized Cambridge Analytica scandal of 2019. FTC Commissioner Rebecca Slaughter (who was acting chair at that time) said that the destruction of Cambridge Analytica's "algorithm it built with deceptively harvested data . . . la[id] the groundwork for similarly employing creative solutions or appropriate solutions rather than cookie-cutter solutions to questions in novel digital markets."[54]

A couple of years later, the FTC ordered Everalbum Inc. to delete an algorithm it had trained on the photos of the faces of its users.[55] Everalbum had a feature that grouped users' photos by faces of the people who appeared in the photos.[56] This was a default for most users and there was no opt out.[57] "When Everalbum first launched its facial recognition feature it 'used publicly available face recognition technology.' However, Everalbum soon began developing its own algorithm by using, in part, 'millions of facial images that it extracted from Ever users' photos.'"[58]

Most recently, the FTC issued an algorithmic deletion demand to WW International. The FTC's complaint alleged that the company's mobile application (which offered "weight-management and tracking services designed for use by children, [teenagers, and families]") violated the Children's Online Privacy Protection Act (which requires "direct notice to parents of information collection practices") by failing to notify the parents of the children.[59] WW used the data to train its algorithm; specifically, to improve the algorithms recommendations about health, fitness, and weight loss.[60] WW was ordered to delete any algorithm that, "in whole or in part," was trained on any personal information collected from children under the age of 13.[61]

The use of algorithmic deletion is an incredibly important change in FTC jurisprudence with as-of-yet unknown ramifications for the technology industry. Former FTC Commissioner Rohit Chopra stated that no longer allowing "data protection law violators to retain algorithms and technologies that derive much of their value from ill-gotten data [is an] important course correction."[62]

The use of this new remedy vastly changes the incentive structure for technology firms following the Silicon Valley mantra:

"move fast and break things." Firms may not want to move so quickly or ignore some of the finer points of data privacy and FTC Act law if the FCT's remedy results in the deletion of prized AI and algorithms. However, the FTC is not necessarily looking to "move fast and break things" either. While there may not be any hesitation to use algorithmic deletion as a requested remedy in litigation, the FTC may first ask a company to walk back its algorithm. If relief can realistically be limited to getting rid of the problematic data, depending on other surrounding circumstances, the FTC may not move to enforce algorithmic deletion. However, as a company's conduct becomes more egregious, it becomes more likely that the FTC requests more draconian penalties.

Whatever future FTC policy in this area may be, the FTC's authority to order algorithmic disgorgement remains unchallenged. The possible sources for this authority "under the FTC Act are (1) the power to issue cease and desist orders under Section 5(b), (2) the ability to order both temporary and permanent injunctions and restraining orders under Section 13(b) and (3) the FTC's rule-making authority under Section 18."[63]

Conclusion

An Old Framework Adapted to Today's Technology

The FTC was founded in 1914. Since then, it has witnessed multiple technological revolutions. However, the same regulatory and legal principles apply to modern, advanced technological products. The FTC is going to regulate AI the same way that it has always regulated everything else. One need look no further than at the FTC's current focus on social media advertising and the methods that these platforms and actors use to promote products and services.

Regulating a misleading claim published in a newspaper in 1914 entails the same analysis as regulating a misleading claim about the capabilities of a company's AI. The facts necessary to come to a conclusion in each circumstance are obviously very different, but the legal doctrine applying those facts to the law has changed little.

Deception, unfair business practices, antitrust concerns, and consumer harms are the FTC's bread and butter. The FTC does not care how you engaged in one of these illicit practices, only that you did. AI is novel and new, but the FTC is ready and prepared to enforce its mandate.

Best Practices

Before internally employing, or bringing to market, an AI or algorithm, ask:[64]

- How representative is the data set?
- Does the model account for bias?
- How accurate are the data-based predictions?
- Does reliance on this data raise ethical or fairness concerns?

Remember:

- Human intervention in AI is still a necessity:
  - Companies are responsible for inputs and outputs.
  - Hiring a diverse team of computer engineers to build and design the AI may reduce inadvertent bias or discrimination.[65]
  - Continuously monitor the AI's outputs to make sure it is not producing any discriminatory effects.[66]
- Attempt transparency:
  - Without broadcasting proprietary information, assess whether there is an opportunity to make the code available to the public or audit teams to double check its work.
  - Make sure that an AI tool is explainable and contestable: understand how the AI works and have a procedure in place to explain it to consumers or regulators.[67]
- Build AI with durable deterrence measures that are difficult to undermine, modify, or remove.

The following are practices to avoid:

- Do not misrepresent what an AI product can do.
- Do not advertise a product as AI if it is not an AI product.
- Do not use AI for illegal commercial surveillance.
  - No matter how strong the market incentive may be, if caught, the FTC's penalty may end up being much more financially untenable.

- Do not use AI to legitimatize biased or discriminatory behavior.
- Do not lie to consumers about how their consumer data is used.
- Do not use AI to collude with other firms to set prices.
- Do not provide an AI or algorithm to firms, or illicit groups, known to peddle deepfake video, voice clones, or are engaged in other nefarious activities.
  - The FTC is focused on finding the upstream producers of the AI products allowing malefactors to engage in "online harms."

Notes

[*] The authors, attorneys with Holland & Knight LLP, may be contacted at anthony.diresta@hklaw.com and zachary.sherman@hklaw.com.

[1] FTC, Federal Trade Commission Mission, https://www.ftc.gov/about-ftc/mission.

[2] Complaint at 11, United States v. Amazon.com, Inc. (W.D. Wash. 2023) (No. 2:23-cv-00811).

[3] FTC, A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority (May 2021) [hereinafter A Brief Overview of the FTC], https://www.ftc.gov/about-ftc/mission/enforcement-authority.

[4] B.J. Copeland, Artificial Intelligence, Encyclopaedia Britannica (June 6, 2023), https://www.britannica.com/technology/artificial-intelligence.

[5] National Defense Authorization Act for Fiscal Year 2021, Div. E, § 5002(3), https://www.govinfo.gov/app/details/BILLS-116hr6395ih.

[6] FTC, FTC Report to Congress: Combatting Online Harms Through Innovation 2 (2022) [hereinafter Combatting Online Harms]; *see also* Kristian Lum & Rumman Chowdhury, What Is an "Algorithm"? It Depends on Who You Ask, MIT Tech. Rev. (Feb. 26, 2021) ("What matters is the potential for harm, regardless of whether we're discussing an algebraic formula or a deep neural network."), https://www.technologyreview.com/2021/02/26/1020007/what-is-an-algorithm/.

[7] Combatting Online Harms, *supra* note 6, at 2.

[8] Michael Atleson, Keep Your AI Claims in Check, FTC (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check.

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] Andrew Smith, Using Artificial Intelligence and Algorithms, FTC (Apr. 8, 2020) [hereinafter Smith, Using AI], https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

[16] *Id.*

[17] *Id.*

[18] Michael Atleson, Chatbots, Deepfakes, and Voice Dlones: AI Deception for Sale, FTC (Mar. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale.

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.* Fake reviews are also the subject of FTC guidance for businesses and consumers. *See* Endorsement, Influencers, and Reviews, https://www.ftc.gov/business-guidance/advertising-marketing/endorsements-influencers-reviews, and How to Evaluate Online Reviews, https://consumer.ftc.gov/articles/how-evaluate-online-reviews.

[24] 15 U.S.C. Sec. 45(n); A Brief Overview of the FTC, *supra* note 3 (cleaned up).

[25] Combatting Online Harms, *supra* note 6, at 1.

[26] *Id.* at 43.

[27] FTC, Enforcement Efforts Against Discrimination and Bias in Automated Systems (April 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

[28] 15 U.S.C. Sec. 45(n).

[29] Smith, Using AI, *supra* note 15.

[30] *Id.*

[31] *Id.*

[32] Elisa Jillson, Aiming for Truth, Fairness, and Equity in Your Company's Use of AI, FTC (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

[33] *Id.*

[34] *Id.*

[35] Atleson, *supra* note 18.

[36] For context, Mr. Atleson was discussing "reasonable data security" in the context of the FTC's "big data" jurisprudence, which has been developing since the mid-2000s.

[37] *See* FTC, Start with Security, A Guide for Business, Lessons Learned from FTC Cases (June 30, 2015); FTC, Stick with Security: A Business Blog Series (Oct. 2017), https://www.ftc.gov/business-guidance/privacy-security/stick-with-security-business-blog-series.

38. Combatting Online Harms, *supra* note 6, at 50-51, quoting Rebecca Kelly Slaughter, Algorithms and Economic Justice, Yale J. L. & Tech. (Aug. 2021), https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf.

39. *See* Combatting Online Harms, *supra* note 6, at 9 n.24; "Commission staff is currently analyzing data collected from several large social media and video streaming companies about their collection and use of personal information as well as their advertising and user engagement practices. *See* 6(b) Orders to File Special Reports to Social Media and Video Streaming Service Provider, https://www.ftc.gov/reports/6b-orders-file-special-reports-social-media-video-streaming-service-providers. In a 2020 public statement, https://www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-social-media-video-streaming-service-providers/joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf, about this project, Commissioners Rebecca Kelly Slaughter and Christine S. Wilson remarked that '[i]t is alarming that we still know so little about companies that know so much about us' and that '[t]oo much about the industry remains dangerously opaque.'"

40. The FTC, very briefly, discusses the need to retain deleted data for a specific purpose: as evidence in terrorism or war crime cases. The FTC also notes that the need for this data does not involve how, when, and why a platform may delete data (or whether the platform was correct) but that there may need to be segmentation of the deleted data with limited access privileges for this reason. See Combatting Online Harms at 53.

41. Press Release, FTC, FTC Warns About Misuses of Biometric Information and Harm to Consumers (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.

42. *See* FTC, Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act (May 18, 2023).

43. *Id.*

44. ChatGPT login page, https://chat.openai.com/auth/login.

45. *Id.*

46. Lina Khan, We Must Regulate A.I. Here's How, New York Times (May 3, 2023) [hereinafter Khan, We Must Regulate AI], https://www.nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html.

47. *Id.*

48. *Id.*

49. *See* Press Release, FTC, FTC Staff Presents Report on Nearly a Decade of Unreported Acquisitions by the Biggest Technology Companies (Sept. 15, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-staff-presents-report-nearly-decade-unreported-acquisitions-biggest-technology-companies.

[50] Press Release, FTC, FTC Chair Khan and Officials from DOJ, CFPB and EEOC Release Joint Statement on AI (Apr. 25, 2023) (emphasis added), https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-chair-khan-officials-doj-cfpb-eeoc-release-joint-statement-ai.

[51] Khan, We Must Regulate A.I., *supra* note 46.

[52] It's worth noting that, as of this writing, the only use of algorithmic deletion has been through settlement consent orders agreed upon by the FTC and respective respondents.

[53] Joshua A. Goland, Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as the FTC's Newest Enforcement Tool for Bad Data, Richmond J. L. & Tech (2023), 2 [hereinafter Goland, Algorithmic Disgorgement].

[54] *Id.* at 18-19 (cleaned up).

[55] Complaint at 1, In re Everalbum, Inc., Comm'n File No. 1923172 (FTC May 6, 2021), https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint_final.pdf.

[56] *Id.* at 3.

[57] *Id.*

[58] Goland, Algorithmic Disgorgement, *supra* note 53, at 20 (quoting Complaint at 3, In re Everalbum, Inc.).

[59] Stipulated Order, United States v. Kurbo Inc., No. 22-CV-00946 (N.D. Cal. Mar. 3, 2022), at 7, https://www.ftc.gov/system/files/ftc_gov/pdf/wwkurbostipulatedorder.pdf.

[60] *Id.*

[61] *Id.*

[62] Statement of Commissioner Rohit Chopra Regarding the Matter of Everalbum and Paravision, Comm'n File No. 1923172 (Jan. 8, 2021), https://www.ftc.gov/system/files/documents/public_statements/1585858/updated_final_chopra_statement_on_everalbum_for_circulation.pdf.

[63] Goland, Algorithmic Disgorgement, *supra* note 53, at 27-28.

[64] Smith, Using AI, *supra* note 15.

[65] Combatting Online Harms, *supra* note 6, at 6.

[66] *Id.* at 7.

[67] *Id.*