Richmond Journal of Law & Technology

Volume 29 | Issue 2 Article 1

3-3-2023

Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as the FTC's Newest Enforcement Tool for Bad Data

Joshua A. Goland
University of Virginia School of Law

Richmond Journal of Law & Technology Volume XXIX, Issue 2

ALGORITHMIC DISGORGEMENT: DESTRUCTION OF ARTIFICIAL INTELLIGENCE MODELS AS THE FTC'S NEWEST ENFORCEMENT TOOL FOR BAD DATA

Joshua A. Goland*

Cite as: Joshua A. Goland, *Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as The FTC's Newest Enforcement Tool for Bad Data*, 29 RICH. J.L. & TECH. 1 (2023).

* J.D. Candidate, University of Virginia School of Law (2023). I would like to thank Professor Kristen Eichensehr for her invaluable help in the research, writing, and revising of this Article and the editors of the Richmond Journal of Law & Technology for their careful edits and thoughtful feedback.

I. INTRODUCTION

[1] Algorithmic disgorgement, 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. It is a relatively new remedy that the Federal Trade Commission (FTC) has used several times since 2019 under its broad authority to "order relief reasonably tailored to the violation of the law."[1] Historically, FTC commissioners have "voted to allow data protection law violators to retain algorithms and technologies that derive much of their value from ill-gotten data,"[2] with the remedy for violating data collection laws being only the deletion of the data itself and possible monetary fines.[3] However, in what former FTC Commissioner Rohit Chopra called an "important course correction,"[4] the FTC has recently begun to require algorithmic disgorgement in its settlements—that is, the deletion of not just the improperly obtained data itself, but any models and algorithms built using such data.[5]

---

[1] Rebecca K. Slaughter et al., *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 YALE J.L. & TECH. (SPECIAL ISSUE) 1, 39 (2021).

[2] FTC, COMM'N FILE NO. 1923172, STATEMENT OF COMM'R ROHIT CHOPRA: IN THE MATTER OF EVERALBUM AND PARAVISION (2021), https://www.ftc.gov/system/files/documents/public_statements/1585858/updated_final_chopra_statement_on_everalbum_for_circulation.pdf [https://perma.cc/X2EX-GY2F].

[3] *Id.*

[4] *Id.*

[5] *See e.g.*, Decision and Order, *In re* Everalbum, Inc., Comm'n File No. 1923172 (FTC May 6, 2021), https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf [https://perma.cc/ZKM4-H7Y5]; Stipulated Order, United States v. Kurbo Inc., No. 22-CV-00946 (N.D. Cal. Mar. 3, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/wwkurbostipulatedorder.pdf [https://perma.cc/KKE9-6CAE].

[2] Machine learning models and algorithms underpin some of the most essential services that exist online today,[6] and the forced deletion of such models and algorithms could have widespread effects on companies across industries as well as their consumers.[7] Ashkan Soltani, the former Chief Technologist of the FTC and head of the California Privacy Protection Agency, said that ordering companies "to delete 'models and algorithms' that relied on deceptively collected information" was a "kind [of] major" development that could require the deletion of "core [machine learning] models."[8] This type of required deletion could be a "significant precedent" possibly affecting millions of users worldwide.[9] Modern computer algorithms are costly and time-consuming to develop, with the initial data

[6] *See e.g.*, Cade Metz*, AI Is Transforming Google Search. The Rest of the Web Is Next*, WIRED (Feb. 4, 2016, 7:00 AM), https://www.wired.com/2016/02/ai-is-changing-the-technology-behind-google-searches [https://perma.cc/X2B7-45TR]; Gideon Lewis-Kraus, *The Great A.I. Awakening*, N.Y. TIMES MAG. (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html [https://perma.cc/XS34-LWPC]; Blake Morgan, *How Amazon Has Reorganized Around Artificial Intelligence And Machine Learning*, FORBES (July 16, 2018, 2:37 PM), https://www.forbes.com/sites/blakemorgan/2018/07/16/how-amazon-has-re-organized-around-artificial-intelligence-and-machine-learning/ [https://perma.cc/D4Q5-ZUX5] ("AI also plays a huge role in Amazon's recommendation engine, which generates 35% of the company's revenue.").

[7] *See* Dave Gershgorn, *The FTC Forced a Misbehaving A.I. Company to Delete Its Algorithm*, MEDIUM: ONEZERO (Jan. 19, 2021), https://onezero.medium.com/the-ftc-forced-a-misbehaving-a-i-company-to-delete-its-algorithm-124d9f7e0307 [https://perma.cc/5PAD-6FBY].

[8] *See* Ashkan Soltani (@ask4n), TWITTER (Jan. 11, 2021, 6:24 PM), https://web.archive.org/web/20210112024342/https://twitter.com/ashk4n/status/1348818030319398913 [https://perma.cc/MMW5-6FM9].

[9] *Id.*

collection stage being one of the biggest obstacles to development.[10] The ordered deletion of an algorithm could cost a company years in development time and millions of dollars spent on research and data collection—potentially making algorithmic disgorgement one of the FTC's most powerful enforcement tools.[11]

[3] Part II of this Article provides a brief overview of machine learning models and algorithms and the basic function and use of Artificial Intelligence (AI). It then describes the purpose and technology behind machine learning algorithms and data collection mechanisms as well as the FTC's role in the regulation and enforcement of data collection. Part III describes recent enforcement actions brought by the FTC that utilized algorithmic disgorgement, analyzes the legality of the FTC's authority to order the destruction of computer data models or algorithms, discusses the likelihood and possibility of future use of the new remedy. Finally, Part IV deliberates on the legal, policy, and social implications of algorithmic disgorgement and proposes some possible alternatives to and restraints on the FTC's use of algorithmic destruction orders.

[10] *See* DIMENSIONAL RSCH., ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING PROJECTS ARE OBSTRUCTED BY DATA ISSUES (2019), https://cdn2.hubspot.net/hubfs/3971219/Survey%20Assets%201905/Dimensional%20Research%20Machine%20Learning%20PPT%20Report%20FINAL.pdf [https://perma.cc/E6PH-5FZW].

[11] *See* Avi Gesser, et al., *Model Destruction – The FTC's Powerful New AI and Privacy Enforcement Tool*, DEBEVOISE DATA BLOG (Mar. 22, 2022), https://www.debevoisedatablog.com/2022/03/22/model-destruction-the-ftcs-powerful-new-ai-enforcement-tool [https://perma.cc/GE39-FC6K].

II. BACKGROUND

A. What is AI?

[4] When hearing the words "Artificial Intelligence" or "AI," it is easy to conjure images of robots and star ships, but in today's reality, the term "AI" generally describes software that can "model[] massive amount of data."[12] This dichotomy can be resolved by categorizing AI into two separate concepts: strong AI (also called general intelligence) and weak AI. Strong AI is AI that can "understand."[13] There is no single agreed-upon definition of strong AI, but it must, "at the very least . . . entail the ability to transfer what [it] has learned to new tasks."[14] However, some stricter definitions also require a level of self-awareness.[15] Despite being the subject of both scientific and public thought since at least the 1950s, strong AI is, for now, still relegated to the realm of science fiction.[16] Accordingly, for the purposes of this Article, "AI" refers to weak AI—that is, AI focused on a

[12] Oren Etzioni, *AI's progress isn't the same as creating human intelligence in machines*, MIT TECH. REV. (June 28, 2022), https://www.technologyreview.com/2022/06/28/1054270/2022-innovators-ai-robots/ [https://perma.cc/D7SK-TWGW].

[13] *See* Jerry Swan, et al., *The Road to General Intelligence*, *in* 1049 STUDIES IN COMPUTATIONAL INTELLIGENCE 1, 116 (2022).

[14] *Id*.

[15] *See What is strong AI?*, IBM, https://www.ibm.com/cloud/learn/strong-ai [https://perma.cc/Z73F-4BVJ].

[16] *See id.*

single task,[17] whether it be answering questions (Siri),[18] playing chess (Stockfish),[19] or driving a car (Tesla Autopilot).[20]

[5] Machine learning is a subset of AI and the vast majority of AI that is available today is built on machine learning algorithms.[21] In the simplest terms, these are programs that, after being trained on large sets of data, can make decisions or predictions.[22] There are many types of machine learning algorithms,[23] as well as methods used to train them.[24] For the purposes of this Article, however, imagine a supervised machine learning algorithm model: a model that takes a labeled dataset, one with already classified data, and after being trained on such pre-defined data, can then take new data input and classify the new data based on the learned process.[25] Think of an anti-spam feature in an email account—after being manually told by millions of users and datasets given by the service provider that certain emails are spam, the anti-spam software can automatically filter out further

[17] *See id.*

[18] *Siri*, APPLE, https://www.apple.com/siri/ [https://perma.cc/N5EJ-SA9K].

[19] *Stockfish 15.1*, STOCKFISH, https://stockfishchess.org [https://perma.cc/B8WL-DCGZ].

[20] *Autopilot and Full Self-Driving Capability*, TESLA, https://www.tesla.com/support/autopilot [https://perma.cc/G2UZ-M354].

[21] *What is Machine Learning?*, IBM, https://www.ibm.com/cloud/learn/machine-learning[https://perma.cc/K69J-62MG].

[22] *Id.*

[23] *Id.*

[24] *Id*.

[25] *Id.*

spam emails without any additional input or instructions.[26] Other types of machine learning algorithms exist, including some that are able to make predictions without requiring the initial set of data to be labeled, but all similarly require an initial set of data and, once trained, are able to work with new data that they have never been exposed to before.[27]

[6] Due to the nature of how machine learning algorithms work, the more data they can be trained with, the more accurate they become, and a deployed algorithm will continue to "learn" as it receives new input. Therefore, it is important for machine learning algorithms to be trained with a wealth of data. To obtain data needed to train a machine learning algorithm, companies can create it, gather it from their existing users, scrape the internet[28], use existing, publicly available datasets, or buy datasets from data brokers. [29] The latter two options may result in multiple machine learning algorithms being trained on the same set of initial data.[30] These methods are costly and difficult and data collection is a significant obstacle

[26] *What is Machine Learning?*, *supra* note 21. Please note that this is a very simplified example of just one type of machine learning algorithm.

[27] *See id.*

[28] *Data collection and pre-processing techniques*, QUALCOMM DEV. NETWORK, https://developer.qualcomm.com/software/qualcomm-neural-processing-sdk/learning-resources/ai-ml-android-neural-processing/data-collection-pre-processing [https://perma.cc/V3L5-KHSQ]; Rachell Wolff, *What Is Training Data in Machine Learning?*, MONKEYLEARN (Nov. 2, 2020), https://monkeylearn.com/blog/training-data/ [https://perma.cc/AD9P-BBPN].

[29] Rachel Wilka et al., *How Machines Learn: Where Do Companies Get Data for Machine Learning and What Licenses Do They Need?*, 13 WASH. J.L. TECH. & ARTS 217, 231 (2018).

[30] *See id.*

to the in-house creation of AI.[31] As such, over 70% of companies wishing to deploy an AI algorithm end up outsourcing their data collection.[32]

B. Privacy Concerns Over Data Collection and the FTC's Role and Enforcement Mechanisms

[7] There is, as of now, no single, all-encompassing data privacy regulation framework in the U.S.[33] Among these laws are the Children's Online Privacy Protection Act (COPPA)[34] for data concerning children, the Health Insurance Portability and Accountability Act (HIPAA)[35] for medical records, and the Family Educational Rights and Privacy Act (FERPA)[36] for education records. Beyond these federal, data-specific regulations, as well as several more comprehensive privacy laws passed by some states,[37] there are generally few restrictions on the type of data companies are permitted to gather from their customers. "In most states, companies can use, share, or sell any data they collect about [their users] without notifying [the users]

[31] DIMENSIONAL RSCH., *supra* note 10.

[32] *Id.*

[33] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/X8XN-NE7U].

[34] 15 U.S.C. §§ 6501–6506.

[35] 42 U.S.C. § 1320d.

[36] 20 U.S.C. § 1232g.

[37] *State Laws Related to Digital Privacy*, NAT'L CONF. OF STATE LEGISLATURES (June 7, 2022), https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy [https://perma.cc/X5VC-7C4S] (comparing California, Colorado, Connecticut, Utah, and Virginia privacy laws).

that they're doing so."[38] Despite this seeming lack of regulation, because of several state privacy regulations, such as the California Online Privacy Protection Act (CalOPPA)[39] and the California Consumer Privacy Act (CCPA),[40] as well as international regulations like the General Data Protection Regulation (GDPR)[41] many companies engaged in data collection are effectively required to have a posted privacy policy statement describing what data they collect and how that data is used.[42] Further, even without an applicable regulation requiring a privacy policy, a lack of a privacy policy might in and of itself be considered an unfair practice by the FTC, leading to enforcement action.[43] These combined practices result in almost all websites, applications, and other technology services listing their

[38] Klosowski, *supra* note 33.

[39] Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575–22579 (Deering 2022).

[40] California Privacy Rights Act of 2020, CAL. CIV. CODE §§ 1798.100–.199 (Deering 2022).

[41] Regulation 2016/679 of April 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[42] *See* Klosowski, *supra* note 33*; see also GDPR Privacy Notice or Consent*, BOISE STATE UNIV., https://www.boisestate.edu/compliance/eu-gdpr/privacy-notice-or-consent/ [https://perma.cc/K83L-2RLQ] ("An explicit privacy notice is generally required for any lawful processing of personal data under the GDPR where the lawful basis for that processing is not the consent of the data subject.").

[43] Leslie A. Reis et al., *Session III: Privacy Regulation and Policy Perspectices*, 29 J. MARSHALL J. COMPUT. & INFO. L. 343, 355 (2012) ("'Well, why don't we just not have [a privacy policy],' or 'why don't we just not have a provision in our privacy policy or terms of service that relate to privacy?' And the answer was simple at the FTC, we would just call that unfair, which is probably the worst classification you could have at the Federal Trade Commission.").

privacy policies, with 88% of all websites (and 100% of the top 100 busiest websites) having posted at least one privacy disclosure by 2000.[44] Once posted, companies are bound to their own policies and violating them can lead to the FTC initiating an enforcement action.[45]

[8] Under Section 5(a) of the FTC Act, the FTC may bring an enforcement action against companies for "unfair or deceptive practices in or affecting commerce."[46] Although an act is considered to be unfair only if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable,"[47] a "small harm to a large class of people" is considered a substantial injury.[48] Under Section 5(b), the FTC may challenge "'unfair or deceptive act[s] or practice[s]' . . . by instituting an administrative adjudication."[49] When the FTC believes that the law has been broken, it will issue a complaint stating its charges and hold a

[44] FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKET PLACE ii (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [https://perma.cc/ZP8W-5XFT].

[45] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement [https://perma.cc/4EWV-S2BV].

[46] 15 U.S.C. § 45(a)(1); *see A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FTC, https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/RQT3-HVFL] (May 2021).

[47] 15 U.S.C.§ 45(n).

[48] FTC v. Pointbreak Media, LLC, 376 F. Supp. 3d 1257, 1285 (S.D. Fla. 2019).

[49] 15 U.S.C. § 45(b); *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, *supra* note 46.

hearing.[50] If the respondent challenges the charges, the complaint is brought before an administrative law judge (ALJ) who can either dismiss the case or recommend an entry of a cease and desist order.[51] Either party can appeal the ALJ's decision to the entire FTC, which will then issue its final decision.[52] The respondent may then appeal that decision to any United States Court of Appeals.[53] If the respondent chooses to settle the charges, they may do so without admitting liability, but must waive all rights to judicial review.[54] Finally, under Section 18 of the FTC Act, the FTC can promulgate new rules addressing unfair or deceptive practices which the Commission has reason to believe are "prevalent."[55] Violations of these rules may result in civil penalties, initiated by the FTC "filing a suit in federal district court."[56]

C. The FTC's Focus on Privacy Protection

[9] The FTC has "[s]ince the late 1990s . . . been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices," with "nearly all" of these cases ending in a settlement.[57]

[50] 15 U.S.C. § 45(b).

[51] *Id.*

[52] *Id.*

[53] *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, *supra* note 46.

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

Violations of privacy policies rarely resulted in monetary fines.[58] Instead, the "heart of a privacy-related . . . order" has been the "prohibition [of] future wrongful activities."[59] Companies were also "regularly," but not always, required to delete improperly obtained data.[60] When monetary damages were levied, they ranged from $1,000 to $35 million.[61] Companies "have also regularly agreed to [monetary] disgorgement and remuneration to consumers, as well as the freezing of assets."[62]

[10] While the FTC has previously used its authority to go after violations of privacy policies and unfair data collection practices, there has been a renewed focus on the enforcement of data and privacy abuses in recent years. In a Statement of Regulatory Priorities published in 2021,[63] the FTC emphasized that it is now "particularly focused" on "data abuses."[64] In a statement to Congress the same year, the FTC stated that it "seeks to continuously reevaluate whether it is doing all it can to provide relief for consumers and deter unfair or deceptive privacy and security practices."[65] In an address at the Global Privacy Summit, FTC Chair Lina Khan stated that the "Federal Trade Commission is refining its approach in light of . . .

[58] *Id.* at 612.

[59] *Id.* at 614.

[60] *Id.* at 616–17.

[61] *Id.* at 615.

[62] Solove & Hartzog, *supra* note 57, at 616.

[63] FTC, STATEMENT OF REGULATORY PRIORITIES 1–2 (2021).

[64] *Id.* at 1–2.

[65] FTC, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 4 (2021) [hereinafter 2021 FTC REPORT].

new market realities," particularly the "political economy of how Americans' data is tracked, gathered, and used."[66] As part of this new focus on data, the FTC has begun taking steps to issue new rules "concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive."[67] The FTC also aims to advance remedies, and "[i]n many cases . . . seek[s] injunctive relief that can include requirements to delete data and algorithms developed with user data . . . ."[68]

D. Monetary Damages, Section 13(b) and AMG Capital Management

[11] The FTC has limited authority to issue monetary damages for unfair and deceptive practices. Under Section 5 of the FTC Act, the FTC may generally issue only a cease and desist order for first-time offenses involving unfair or deceptive practices and may not obtain equitable relief unless an order, rule, or injunction has been violated.[69] Section 5(m)(1)(B) of the FTC Act, a cumbersome rule that has been rarely used since the 1980s[70], allows the FTC to seek civil penalties if it can show a party has

[66] Lina M. Khan, Chair, FTC, Remarks at IAPP Global Privacy Summit 2022 (Apr. 11, 2022), https://www.ftc.gov/news-events/news/speeches/remarks-chair-lina-m-khan-prepared-delivery-iapp-global-privacy-summit-2022 [https://perma.cc/GGC2-9MK7].

[67] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51, 273 (Aug. 22, 2022).

[68] 2021 FTC REPORT, *supra* note 65, at 1.

[69] 15 U.S.C. § 45(l).

[70] Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC Act's Penalty Offense Authority*, 170 U. PA. L. REV. 71, 98 (2021).

engaged in a practice that the FTC had previously ruled was unfair or deceptive and issued a cease or desist order on, and the offending party had actual knowledge that the practice was unfair or deceptive.[71] The difficulties of showing actual knowledge, the requirement of a *de novo* hearing on any issue of fact, and the respondent's ability not only to challenge the current ruling but the prior determination of unlawful conduct, have resulted in the exceedingly rare use of the Section 5(m)(1)(B) as enforcement mechanism.[72] Finally, Section 19 of the FTC Act allows the Commission to seek court-ordered monetary relief in cases where it is "necessary to redress injury to consumers or other persons."[73] To obtain relief under Section 19, the FTC must first determine whether an act was unfair or deceptive and issue a final cease and desist order.[74] The FTC must also show that "the act or practice to which the cease and desist order relates is one which a reasonable man would have known under the circumstances was dishonest or fraudulent."[75] Similarly to Section 5, Section 19 can be challenging to enforce and has also, therefore, been rarely relied upon by the FTC.

[12] Historically, when the FTC sought monetary damages for unfair or deceptive practices, it was almost always done under Section 13(b) of the FTC Act, which "authorizes the Commission to seek preliminary and permanent injunctions to remedy 'any provision of law enforced by the Federal Trade Commission.'"[76] However, in 2021 in *AMG Cap. Mgmt., LLC*

[71] *Id.* at 95–96.

[72] *Id.* at 96.

[73] 15 U.S.C. § 57b.

[74] *Id.*

[75] *Id.*

[76] FTC, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY, https://webharvest.gov/peth04/20041022140933/

v. Fed. Trade Comm'n, the Supreme Court ruled that the FTC may not obtain monetary relief under Section 13(b), finding that monetary relief does not fit Section 13's definition of "injunctive relief."[77] The *AMG* decision further stated that Congress had "expressly authoriz[ed] *conditioned* and *limited* monetary relief" under Sections 5 and 19 and that the FTC was using Section 13 to "obtain that same monetary relief and more without satisfying those conditions and limitations."[78]As the Court noted, nothing in the decision "prohibits the Commission from using its authority under [Section] 5 and [Section] 19 to obtain restitution on behalf of consumers."[79] The Court further advised the Commission that "[i]f the Commission believes that authority too cumbersome or otherwise inadequate, it is, of course, free to ask Congress to grant it further remedial authority."[80]

[13] The *AMG* ruling significantly hindered the FTC's ability to obtain monetary relief for unfair and deceptive practices, depriving it of the "strongest tool [it] had to help consumers."[81] Following the decision, the FTC appealed to Congress for new legislation to increase its enforcement power and began looking for new non-monetary enforcement

http://www3.ftc.gov/ogc/brfovrvw.htm [https://perma.cc/5D7T-NBTS] (Sept. 2002).

[77] AMG Cap. Mgmt., LLC v. FTC, 141 S. Ct. 1341, 1350 (2021).

[78] *Id.* at 1349.

[79] *Id.* at 1352.

[80] *Id.*

[81] Press Release, FTC, Statement by FTC Acting Chairwoman Rebecca Kelly Slaughter on the U.S. Supreme Court Ruling in AMG Capital Management LLC v. FTC (Apr. 21, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/04/statement-ftc-acting-chairwoman-rebecca-kelly-slaughter-us-supreme-court-ruling-amg-capital [https://perma.cc/V69M-CHTS].

mechanisms.[82] The FTC "initiat[ed] new rulemakings about unfair or deceptive practices" and brought "more administrative proceedings" in order to begin the process to obtain relief under Section 19.[83] It also "sent warning letters to companies to put those companies on notice that they may be subject to civil penalties for engaging in other behavior the FTC has previously declared unfair or deceptive" for purposes of Section 5(m)(1)(B).[84] In addition to using established methods, the Commission turned to alternative enforcement tools, such as algorithmic disgorgement.

III. ALGORITHMIC DISGORGEMENT

[14] Between 2019 and 2022, the FTC reached settlements that included algorithmic disgorgement orders with three different companies.[85] While the underlying fact patterns which led to the violations were unique to each case, the language of the algorithmic disgorgement order itself was similar in all three cases. Because the orders were all achieved through settlements,

[82] Press Release, FTC, FTC Asks Congress to Pass Legislation Reviving the Agency's Authority to Return Money to Consumers Harmed by Law Violations and Keep Illegal Conduct from Reoccurring (Apr. 27, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/04/ftc-asks-congress-pass-legislation-reviving-agencys-authority-return-money-consumers-harmed-law [https://perma.cc/3FPA-BBS9].

[83] So Jung Kim, *Post-FTC v. AMG: Consumer Redress Through Other Means*, U. CHI. L. REV. ONLINE (Sept. 20, 2022), https://lawreviewblog.uchicago.edu/2022/09/20/kim-ftc-amg [https://perma.cc/5CBN-8NV7].

[84] *Id.*

[85] Lauren Merk & Bailey Sanchez, *FTC Requires Algorithmic Disgorgement as a COPPA Remedy for First Time*, FPF (Mar. 14, 2022), https://fpf.org/blog/ftc-requires-algorithmic-disgorgement-as-a-coppa-remedy-for-first-time/ [https://perma.cc/253P-ZCB4].

the FTC was not required to show a legal basis for ordering algorithmic destruction.[86]

[15] As such, the algorithmic disgorgement orders were broad and contained little explanation regarding the mechanics or details around the deletion. The following sections provide an overview of the circumstances leading to the three existing algorithmic disgorgement orders enforced by the FTC and discuss the legality behind any possible future algorithmic disgorgement orders not agreed upon through settlements.

A. Existing Orders

[16] The FTC first used algorithmic disgorgement in November of 2019 in a settlement with Cambridge Analytica.[87] The settlement came out of a complaint by the FTC alleging that an application Cambridge Analytica created used "deceptive acts and practices to harvest personal information from Facebook users for political and commercial targeted advertising purposes."[88] In particular, the FTC alleged that Cambridge Analytica "obtained the app users' consent to collect their Facebook profile data through false and deceptive means," and "falsely represented that the [app]

[86] *See generally* Brief for Petitioner, United States v. Kurbo Inc., No. 22-CV-00946 (N.D. Cal. Mar. 3, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/wwkurbostipulatedorder.pdf [https://perma.cc/KKE9-6CAE] (referring of the order, one can discern there is an evident lack of information relevant to the decision which the agency reached in its adjudications).

[87] *See* Final Order, *In re* Cambridge Analytica, LLC, Comm'n File No. 1823107 (FTC Nov. 25, 2019), https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_orderpublic.pdf [https://perma.cc/FQC5-AELE].

[88] Complaint, *In re* Cambridge Analytica, LLC, Comm'n File No. 1823107 (FTC July 22, 2019), https://www.ftc.gov/system/files/documents/cases/182_3107_cambridge_analytica_administrative_complaint_7-24-19.pdf [https://perma.cc/27R2-EWH9].

did not collect any identifiable information from the Facebook users who authorized [their data collection]."[89] As part of the settlement, Cambridge Analytica was ordered to destroy "any information or work product, including any algorithms or equations, that originated, in whole or in part" from the improperly obtained data.[90]

[17] The Cambridge Analytica settlement did not raise any eyebrows by ordering the deletion of work product from the news media or the legal world.[91] An explanation for this lack of fanfare might be that no one anticipated that this settlement would be the start of a pattern. The novelty of the Cambridge Analytica scandal paired with the lack of any indication by the FTC that ordering the deletion of models and algorithms would start to become a more common occurrence, allowed the first use of algorithmic disgorgement to pass by relatively unnoticed by the world at large. It turned out, however, that it was not an accidental move by the FTC—in an interview in 2021, almost two years after the Cambridge Analytica settlement was reached, FTC Commissioner Rebecca Slaughter (who was FTC Acting Chair at the time of the order) spoke about the "little-known requirement that Cambridge Analytica destroy[] the algorithms it built with

[89] *Id.*

[90] Final Order, *supra* note 87.

[91] *See* Allison Prang, *FTC Approves Settlement Related to Cambridge Analytica*, WALL ST. J. (Dec. 18, 2019. 1:01 PM), https://www.wsj.com/articles/ftc-approves-settlement-related-to-cambridge-analytica-11576692106 [https://perma.cc/F7KT-PJHD] (describing the settlement agreement between the FTC and Cambridge Analytica); *see also* GIBSON DUNN, U.S. CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2020 8 (2020), https://www.gibsondunn.com/wp-content/uploads/2020/01/us-cybersecurity-and-data-privacy-outlook-and-review-2020.pdf [https://perma.cc/BL58-W6J7] (mentioning the settlement and order to delete work product, but neglecting to indicate that it was anything of note).

deceptively-harvested data."[92] Commissioner Slaughter said that the requirement was "an important part of the outcome" which "la[id] the groundwork for similarly employing creative solutions or appropriate solutions rather than cookie-cutter solutions to questions in novel digital markets."[93]

[18] In May of 2021, the FTC issued its second algorithmic disgorgement order in a settlement with Everalbum.[94] Everalbum operated a photo album application, Ever, which allowed users to upload photos and videos to Everalbum's cloud servers to free up users' local storage space.[95] The FTC's complaint alleged that Everalbum, a company that provided a "photo storage and organization" application, engaged in "unfair or deceptive acts or practices" by misrepresenting what collected data was used for and how data was deleted pursuant to user requests.[96]

---

[92] Kate Kaye, *'Don't Lie': FTC Commissioner Rebecca Slaughter on why today's data privacy approaches don't work (Audio Q&A)*, DIGIDAY (July 7, 2021), https://digiday.com/media/dont-lie-a-qa-with-ftc-commissioner-rebecca-slaughter-on-why-todays-data-privacy-approaches-dont-work/ [https://perma.cc/HZ23-B7E6].

[93] Kate Kaye, *Why the FTC is forcing tech firms to kill their algorithms along with ill-gotten data*, DIGIDAY (July 9, 2021), https://digiday.com/media/why-the-ftc-is-forcing-tech-firms-to-kill-their-algorithms-along-with-ill-gotten-data/ [https://perma.cc/593M-4HYY].

[94] Decision and Order, *In re* Everalbum, Inc., Comm'n File No. 1923172 (FTC May 6, 2021), https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf [https://perma.cc/JJ3Q-97TE].

[95] 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 [https://perma.cc/H9FJ-FKMK].

[96] *Id.* at 6–7.

[19] One of the features of the software used "face recognition to group users' photos by faces of the people who appear in the photos."[97] When this feature was launched, it was enabled by default for almost all users and did not provide the ability to opt out of the feature.[98] Eventually, Everalbum rolled out to users (in stages based on location) a popup that informed them about the facial recognition and allowed them to opt out.[99] Several months after this popup was introduced, Everalbum posted on the "Help" section of its website an article titled "What is Face Recognition," which informed users that "[w]hen face recognition is turned on, you are letting us know that it's ok for us to use the face embeddings of the people in your photos and videos . . . ."[100] When Everalbum first launched its facial recognition feature it "used publicly available face recognition technology."[101] However, Everalbum soon began developing its own algorithm by using, in part, "millions of facial images that it extracted from Ever users' photos."[102]

[20] Everalbum also told users in multiple instances that deactivating their account would "permanently delete all photos and videos stored on [their] account"[103] and Everalbum's privacy policy stated that upon account deletion it would "try to delete . . . information as soon as possible."[104] The

[97] *Id.* at 2.

[98] *Id.*

[99] *Id.*

[100] Complaint, *supra* note 95, at 3.

[101] *Id.*

[102] *Id.*

[103] *Id.* at 4.

[104] *Id.* at 6.

complaint alleged that "Everalbum did not, in fact, delete the photos or videos of any users who had deactivated their accounts and instead retained them" for several months after it released its facial recognition feature.[105]

[21] As part of its settlement with the FTC, Everalbum was ordered to delete or destroy "any models or algorithms developed in whole or in part using [data such as images and scans] [Everalbum] collected from Users of the "Ever" mobile application" as well as any of the underlying photos and facial embeddings it had collected.[106] Unlike the Cambridge Analytica disgorgement order, the Everalbum settlement generated a significant amount of buzz from news articles[107] to Practicing Law Institute courses designed to keep attorneys abreast of developments in the law.[108] Legal observers called the settlement a "significant precedent"[109] and

[105] Complaint, *supra* note 95, at 6.

[106] Decision and Order, *supra* note 94, at 2.

[107] Natasha Lomas, *FTC settlement with Ever orders data and AIs deleted after facial recognition pivot*, TECHCRUNCH (Jan. 12, 2021, 8:43 AM), https://techcrunch.com/2021/01/12/ftc-settlement-with-ever-orders-data-and-ais-deleted-after-facial-recognition-pivot/ [https://perma.cc/TC5X-52PH].

[108] *Digital Risk: Lessons from the FTC's Settlement with Everalbum*, PRACTICING L. INST. (May 17, 2021), https://plus.pli.edu/Browse/Title?rows=10&fq=%7e2B%7etitle_id%7e3A282B22%7e322320%7e2229%7e&fq=title_id%7e3A2822%7e322320%7e2229%7e [https://perma.cc/638B-AVZC].

[109] Zachary Sorenson, *Everalbum, Inc: In first facial recognition misuse settlement, FTC requires destruction of algorithms trained on deceptively obtained photos*, HARV. JOLT DIG. (Jan. 13, 2021), https://jolt.law.harvard.edu/digest/everalbum-inc-in-first-facial-recognition-misuse-settlement-ftc-requires-destruction-of-algorithms-trained-on-deceptively-obtained-photos [https://perma.cc/7QF3-QTMM].

"revolutionary,"[110] pointing out that it "may have implications for developers of AI, to the extent the FTC requires the deletion of an algorithm, itself, developed using data not appropriately acquired or used for such means."[111] Immediately after the settlement was made public, FTC Commissioner Rohit Chopra issued a statement hinting that the requirement of algorithmic disgorgement was the first of many, stating that no longer allowing "data protection law violators to retain algorithms and technologies that derive much of their value from ill-gotten data" was an "important course correction."[112] In a similar statement, Commissioner Rebecca Slaughter, then Acting Chair of the FTC, also noted that going forward, the FTC "should require violators to disgorge not only the ill-gotten data, but also the benefits—here, the algorithms—generated from the data."[113]

[22] The most recent use of algorithmic disgorgement came from a settlement with WW International (formerly known as Weight Watchers International Inc.).[114] The FTC complaint stemmed from a mobile application operated by WW called Kurbo, which offered "weight-

[110] Mireille Hildebrandt (@mireillemoret), TWITTER (Jan. 12, 2021, 2:08 AM), https://twitter.com/mireillemoret/status/1348889492200022017 [https://perma.cc/WP4A-QMH5].

[111] Linda A. Malek & Blaze Waleski, *Significance of FTC guidance on artificial intelligence in health care*, REUTERS (Nov. 24, 2021, 11:20 AM), https://www.reuters.com/legal/litigation/significance-ftc-guidance-artificial-intelligence-health-care-2021-11-24/ [https://perma.cc/QS5H-P62E].

[112] FTC, *supra* note 2.

[113] Rebecca Kelly Slaughter, Acting Chairwoman, FTC, Protecting Consumer Privacy in a Time of Crisis (Feb. 10, 2021), https://www.ftc.gov/system/files/documents/public_statements/1587283/fpf_opening_remarks_210_.pdf [https://perma.cc/CC5U-PEAZ].

[114] Stipulated Order, supra note 5, at 7.

management and tracking service designed for use by children ages eight and older, teenagers, and families."[115] Because the app was targeted to children and because WW had actual knowledge that children under 13 were using the app, it was subject to COPPA rules which require "direct notice to parents of information collection practices . . . verifiable parental consent . . . and the retaining [of] children's personal information for only as long as is reasonably necessary to fulfill the purpose for which it was collected."[116] The complaint alleged that the Kurbo app did not comply with these requirements by failing to notify parents of its data collection practices or properly obtain parental consent.[117] The app also failed to verify a user's age when they initially signed up and allowed users to alter this information after gaining access without disabling the user's account or requiring parental consent if the new age was set to under 13.[118]

[23] WW used the obtained data to "make recommendations about health, fitness and weight loss" using algorithms "based on an analysis of user data."[119] Similarly to the Everalbum settlement, WW was ordered to delete any of these algorithms which were "in whole or in part" obtained

[115] *See* Press Release, FTC, FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data (Mar. 4, 2023) (stating the FTC's stance on Weight Watcher's illegal activity), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive [https://perma.cc/ZJ27-VTS3].

[116] Stipulated Order, *supra* note 5, at 1–2.

[117] *Id.*

[118] Press Release, FTC, *supra* note 115.

[119] *Destroying Personal Digital Data*, *The Indicator From Planet Money*, NPR, at 03:16 (Mar. 24, 2022, 7:03 PM), https://www.npr.org/2022/03/24/1088655807/destroying-personal-digital-data [https://perma.cc/4XWH-K2RK].

from any personal information collected from children under the age of 13.[120]

[24] It is important to note that, as of now, the only use of algorithmic disgorgement has been through settlement consent orders, agreed to by the FTC and respondents. WW, Everalbum, and Cambridge Analytica all agreed to the destruction of their data and algorithms without challenging the FTC's order.[121] None of the companies have released statements discussing this portion of the settlement so it is hard to say for certain why these orders were not challenged. We can, however, speculate. Cambridge Analytica filed for bankruptcy shortly after the order and its executives were facing personal liability for their actions.[122] The worldwide negative press that Cambridge Analytica received,[123] as well as the political ramifications of its actions,[124] might have encouraged executives to resolve the matter as

[120] Stipulated Order, *supra* note 5, at 7.

[121] *Id.*; *see* Decision and Order, supra note 5, at 1, 4–5; Final Order, *supra* note 87, at 4.

[122] Press Release, FTC, *supra* note 115.

[123] *See* Joe Westby, *'The Great Hack': Cambridge Analytica is just the tip of the iceberg*, AMNESTY INT'L (July 24, 2019), https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/ [https://perma.cc/5DXR-6Q98]; Issie Lapowsky, *How Cambridge Analytica Sparked the Great Privacy Awakening*, WIRED (Mar. 17, 2019, 7:00 AM), https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/ [https://perma.cc/4LB2-PG6N]; Sinead Garvan, *Netflix Cambridge Analytica film: Social media is 'like a crime scene'*, BBC: NEWSBEAT (July 26, 2019), https://www.bbc.com/news/newsbeat-49085306/ [https://perma.cc/B95F-BL4G].

[124] *See* Lauren Feiner, *How Cambridge Analytica and the Trump campaign changed Big Tech forever*, CNBC (Dec. 26, 2019, 9:01 AM), https://www.cnbc.com/2019/12/24/how-facebook-and-big-tech-gained-dc-scrutiny-in-the-2010s.html [https://perma.cc/SV52-KTPL]; Issie Lapowsky, *House Probes Cambridge Analytica on Russia and WikiLeaks*, WIRED (Mar. 4, 2019, 3:04 PM), https://www.wired.com/story/congress-democrats-trump-inquiry-cambridge-analytica/ [https://perma.cc/9YNR-SEDV].

quickly and with as little media coverage as possible. A prolonged battle with the FTC over disgorgement would have contradicted these goals. Further, following the scandal, Cambridge Analytica lost "nearly all" of its clients, and with the inevitable bankruptcy looming, it might not have been worth fighting to save the data or the algorithms.[125]

[25] The photo storage app Ever shut down before the settlement and its parent company, Everalbum, rebranded to Paravision and began developing new AI systems for the corporate and military sectors.[126] In a statement, Paravision claimed that "the FTC Consent Order reflects a change that has already taken place" and that it had already switched to its "latest-generation face recognition model which does not use any Ever users' data."[127] The destruction of its Ever AI might not have been worth the effort to challenge the FTC order, whether for publicity purposes or because it had already been rendered obsolete by Paravision's newer models.

[26] Similar to Cambridge Analytica, WW's Kurbo app received widespread negative media coverage even before its rule-breaking data collection practice came to light.[128] Given this negative attention, which

[125] Brandy Zadrozny & Ben Collins, Inside the final days of Cambridge Analytica: Failed rebrands, fleeing clients and Nerf basketball, NBC NEWS (May 18, 2018, 9:19 AM), https://www.nbcnews.com/business/business-news/inside-final-days-cambridge-analytica-failed-rebrands-fleeing-clients-nerf-n875321 [https://perma.cc/XAP3-SUN9].

[126] Kim Lyons, *FTC settles with photo storage app that pivoted to facial recognition*, THE VERGE (Jan. 11, 2021, 2:59 PM), https://www.theverge.com/2021/1/11/22225171/ftc-facial-recognition-ever-settled-paravision-privacy-photos [https://perma.cc/P4RM-N7DL]; *Trusted Vision AI*, PARAVISION, https://www.paravision.ai/company/ [https://perma.cc/A34N-V9F3].

[127] Lomas, *supra* note 107.

[128] Alysee Dalessandro, *I Joined Weight Watchers at Age 12. Here's Why Their Kurbo App Concerns Me*, HEALTHLINE (Aug. 27, 2019), https://web.archive.org/web/

only increased after the FTC complaint,[129] WW likely would have wanted to settle the matter quickly to reduce the publicity of its violations. Finally, WW shut down Kurbo shortly after the complaint and insinuated the algorithms might have not been worth trying to save.[130]

[27] The FTC has stated its plans to step up its use of algorithmic disgorgement and it is predicted to become a "standard enforcement mechanism" for the agency.[131] This enforcement is unlikely to remain exclusively contained within consent orders, as the FTC signaled it intends to "require violators to disgorge [algorithms generated from] ill-gotten data" in the same manner that it "routinely obtain[s] disgorgement of ill-

20190828013832/https://www.healthline.com/health/kurbo-weight-watchers-dangerous-for-kids#1 [https://perma.cc/C76N-J3UB]; Sarah Perez, *WW launches Kurbo, a hotly debated 'healthy eating' app aimed at kids*, TECHCRUNCH (Aug. 14, 2019, 4:00 PM), https://techcrunch.com/2019/08/14/ww-launches-kurbo-a-hotly-debated-healthy-eating-app-aimed-at-kids [https://perma.cc/89KM-3G7G]; Ragen Chastain, *For Healthy Kids, Skip the Kurbo App*, U.S. NEWS (Sep. 7, 2019, 9:00 AM), https://health.usnews.com/health-news/blogs/eat-run/articles/for-healthy-kids-skip-the-kurbo-app []; Maija Kappler, *Weight Watchers Under Fire for Kurbo, Its Weight Loss App for Teens*, HUFFPOST (Aug. 16, 2019, 11:40 AM), https://www.huffpost.com/archive/ca/entry/kurbo-weight-watchers-app-kids_ca_5d5595e1e4b056fafd08ac0a [https://perma.cc/ZK59-75PN].

[129] Claire Fahy, *Weight Watchers App Gathered Data from Children, F.T.C. Says*, N.Y. TIMES (Mar. 8, 2022), https://www.nytimes.com/2022/03/08/business/weight-watchers-data-children.html [https://perma.cc/QC7Z-NZV6].

[130] *WW International, Inc. (WW) CEO Sima Sistani on Q2 2022 Results - Earnings Call Transcript*, SEEKING ALPHA (Aug. 6, 2022, 7:16 PM), https://seekingalpha.com/article/4530916-ww-international-inc-ww-ceo-sima-sistani-on-q2-2022-results-earnings-call-transcript/ [https://perma.cc/NS6X-MJDB].

[131] Kate Kaye, *The FTC's new enforcement weapon spells death for algorithms*, PROTOCOL (Mar. 14, 2022), https://www.protocol.com/policy/ftc-algorithm-destroy-data-privacy [https://perma.cc/QL4G-AGG2].

gotten monetary gains."[132] Still, the majority of the FTC's actions against improper data usage or collection end with a settlement[133] and given the cost and lengthy process of litigation, the pattern of seeing algorithmic disgorgement primarily in consent orders is likely to continue. Additionally, settlements may be preferable to the FTC because it "can often obtain remedies via settlement . . . that it might not be able to obtain based on a court order."[134]

B. The FTC's Authority to Order Destruction of AI Algorithms

[28] The FTC has not yet had to justify its ability to seek algorithmic disgorgement to a court because none of the companies which were subject to an algorithmic disgorgement order have challenged the FTC's authority to order the destruction of algorithms.[135] Therefore, while it is impossible to say for sure under what authority the FTC would be able to obtain such orders, we can try to infer the possible venues the FTC may seek in establishing the legal basis for the new remedy based on public statements of FTC officials and analysis of the statutory language of the FTC Act. The possible sources for the FTC's authority to order algorithmic disgorgement under the FTC Act are (1) the power to issue cease and desist orders under Section 5(b),[136] (2) the ability to order both temporary and permanent

[132] Slaughter, *supra* note 113, at 2.

[133] Alexander E. Reicher & Yan Fang, *FTC Privacy and Data Security Enforcement and Guidance Under Section 5*, 25 COMPETITION 89, 93 (2016).

[134] Gesser et al., *supra* note 11.

[135] *See* Sorenson, *supra* note 109 (discussing various instances of companies settling with the FTC instead of challenging the merits of an algorithmic disgorgement order).

[136] 15 U.S.C. § 45(b).

injunctions and restraining orders under Section 13(b)[137] and (3) the FTC's rule-making authority under Section 18.[138] This Part considers possible arguments for finding the power to order algorithmic disgorgement under Sections 5(b) and 13(b) and concludes that neither Section 5(b) nor 13(b) may prove to be a sufficient legal basis for the FTC's power to order algorithmic disgorgement. It submits that Section 18 rule-making might be the best viable path for the FTC to implement a new remedy that will survive courts' scrutiny.

1. Section 5(b) Cease and Desist Orders

[29] Under Section 5(b), when the FTC has reason to believe that a company has engaged in unfair or deceptive practices, it may issue an order requiring the company to cease and desist from using the unfair method or practice.[139] According to FTC Commissioner and former Acting Chair Rebecca Slaughter, the "authority to seek this type of remedy comes from the Commission's power to order relief reasonably tailored to the violation of the law."[140] Commissioner Slaughter cites to several cases, noted below, discussing the breadth of injunctions which the FTC is able to enforce through Section 5(b) cease and desist orders,[141] suggesting that the FTC might seek to obtain algorithmic disgorgement orders under its ability to obtain cease and desist orders. While the FTC has relatively wide latitude

[137] *Id.* § 53(b).

[138] *See id.* § 57a (describing the authority of the commission to prescribe rules as well as the applicable procedures).

[139] *Id.* § 45(b).

[140] Slaughter et al., *supra* note 1, at 39.

[141] *Id*.

for the type of orders it can seek to impose through an ALJ,[142] Section 5(b) cease and desist orders must not go "beyond elimination of the specific misrepresentations which were made and also beyond what in fairness could be deemed necessary to deter future unlawful conduct."[143] Cease and desist orders must also generally be an order to "stop committing a specific act or practice."[144] Such cease and desist orders have a wide scope and Commissioner Slaughter cites various "fencing in" remedies, which look to stop conduct "broader than the conduct that is declared unlawful."[145] Such orders have been used to require a company to substantiate its advertising claims prior to making them;[146] to prohibit the use of certain words and formatting on debt collection forms;[147] and to order a set of corporations to

[142] *See, e.g.*, FTC v. Ruberoid Co., 343 U.S. 470, 473 (1952) ("[T]he Commission is not limited to prohibiting the illegal practice in the precise form in which it is found to have existed in the past. . . . [I]t must be allowed effectively to close all roads to the prohibited goal[.]"); Jacob Siegel Co. v. FTC, 327 U.S. 608, 611 (1946) ("The Commission has wide discretion in its choice of a remedy deemed adequate to cope with the unlawful practices in this area of trade and commerce.").

[143] Standard Oil Co. of Cal. v. FTC, 577 F.2d 653, 662 (9th Cir. 1978).

[144] *See* LabMD, Inc. v. FTC, 894 F.3d 1221, 1236 (11th Cir. 2018) (explaining how a cease and desist order was unenforceable because it did not instruct the party to stop committing a specific act or practice).

[145] Slaughter et al, *supra* note 1, at 39 n.115 (citing Telebrands Corp. v. FTC, 457 F.3d 354, 357 n.5 (4th Cir. 2006).

[146] *See Telebrands Corp.*, 457 F.3d at 356–357 ("[T]he complaint alleged that Telebrands had made unsubstantiated claims that the Ab Force caused loss of weight, inches or fat, caused well-defined abdominal muscles, and was an effective alternative to regular exercise.").

[147] *See* Floersheim v. FTC, 411 F.2d 874, 876–877 (9th Cir. 1969) (discussing how the FTC issued a complaint because the use of certain words and formatting on the plaintiff's debt collection forms caused the forms to be misleading).

stop participating in price fixing.[148] All of these, however, are prospective in nature, limiting or prohibiting a company's future actions. Algorithmic disgorgement orders go beyond the permissible scope of such cease and desist orders.

[30] Such algorithmic disgorgement orders do not direct a company to stop committing a specific act or practice, but instead require said company to destroy the work product of an already committed act. In the WW settlement, for example, the violations alleged in the complaint were the lack of notice and consent from parents about Kurbo's "information collection practices" and the indefinite retention of children's data.[149] Each of these violations would have ceased once Kurbo stopped collecting data without proper notice and consent and stopped the retention of data for longer than required. Both results could be achieved by a proper cease and desist order directing stoppage of improper data collection and retention.

[31] Further, even if the FTC can show that the actual development of the algorithms, and not just the collection of the data, violates rules against deceptive practices, a cease and desist order would be limited to enjoining the further development or use of such algorithms. Ordering algorithmic disgorgement would still fall outside the scope of a cease and desist order, which must "not . . . punish or . . . fasten liability on respondent for past conduct but to ban specific practices for the future."[150] Once developed, AI algorithms fall outside of the scope of cease and desist orders. Therefore, it

[148] *See* United States v. Phelps Dodge Indus., Inc., 589 F. Supp. 1340, 1345 (S.D.N.Y. 1984) ("The complaint charges that the defendants violated a 1936 Federal Trade Commission cease and desist order, which prohibited price fixing and coordination in the paper cable industry.").

[149] Complaint at 13, United States v. Kurbo Inc., No. 22-CV-00946 (N.D. Cal. Feb. 16, 2022).

[150] FTC v. Cement Inst., 333 U.S. 683, 706 (1948).

seems unlikely that the FTC can rely on Section 5(b) as a viable justification for ordering algorithmic disgorgement.

2. Section 13(b) Injunction

[32] Section 13(b) of the FTC Act grants the FTC the ability to order both temporary and permanent injunctions as well as restraining orders for violations of the FTC Act.[151] As discussed above, the FTC has historically used this language to seek equitable monetary remedies, such as monetary disgorgement. However, in *AMG*, the Supreme Court ruled that "[Section] 13(b) as currently written does not grant the Commission authority to obtain equitable monetary relief."[152] Following the *AMG* decision, the FTC may only use Section 13(b) to grant solely non-monetary injunctive relief.[153]

[33] When discussing algorithmic disgorgement, FTC officials have repeatedly analogized it to monetary disgorgement, saying that algorithmic disgorgement is akin to "disgorgement of ill-gotten monetary gains."[154] By claiming that algorithmic disgorgement is similar to monetary disgorgement and is "in line with both the FTC's legal enforcement authority as well as existing FTC precedent" which is "similar [to] traditional disgorgement,"[155] the FTC appears to be stating that its authority to obtain algorithmic disgorgement stems from the same authority under which the agency can obtain traditional monetary relief. The FTC used Section 13(b) to obtain monetary relief as standard practice and it was described as a "critical tool

[151] 15 U.S.C. § 53(b).

[152] AMG Cap. Mgmt., LLC v. FTC, 141 S. Ct. 1341, 1352 (2021).

[153] *Id.* at 1348.

[154] *See* Slaughter, *supra* note 113.

[155] Tiffany C. Li, *Algorithmic Destruction*, 75 SMU L. REV. 479, 502–03 (2022).

in support of [the FTC's] enforcement missions."[156] The *AMG* decision is relatively recent, having been published in late April of 2021, after the FTC statements likened algorithmic disgorgement to its monetary counterpart. Prior to the *AMG* decision, the FTC would have likely sought to obtain algorithmic disgorgement under Section 13(b) under the same principles that it was obtaining monetary disgorgement, which could explain why officials equated the two in public statements. Following the *AMG* decision, however, this is no longer productive.

[34] The *AMG* holding "is narrow, limited to the question of whether [Section] 13(b) authorizes the FTC to seek and be awarded equitable *monetary* relief such as restitution or disgorgement"[157] and does not directly limit the FTC's ability to obtain non-monetary relief using this section of the Act. Because the FTC is not permitted to obtain monetary remedies under Section 13(b), it will likely seek to distance algorithmic disgorgement from monetary disgorgement. Instead, the FTC might argue that algorithmic disgorgement is a form of permanent injunction permitted by Section 13(b). Algorithmic disgorgement concerns algorithms, not money, and analysts have already picked up on this distinction.[158] However, even if the FTC

[156] FTC, THE URGENT NEED TO FIX SECTION 13(B) OF THE FTC ACT: BEFORE THE COMMITTEE ON ENERGY AND COMMERCE SUBCOMMITTEE ON CONSUMER PROTECTION AND COMMERCE 2 (2021), https://www.ftc.gov/system/files/documents/public_statements/1589400/p180500house13btestimony04272021.pdf [https://perma.cc/4GDH-5PWK].

[157] FTC v. Neora LLC, 552 F. Supp. 3d 628, 634 (N.D. Tex. 2021).

[158] Mary Ashley Salvino, *ANALYSIS: FTC Privacy Authority Is Poised for Breakthrough Year*, BLOOMBERG L. (Nov. 13, 2022, 9:00 PM), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-ftc-privacy-authority-is-poised-for-breakthrough-year [https://perma.cc/9FSL-PYJS] (arguing that algorithmic disgorgement is a "non-monetary mechanism to obtain redress" and an alternative to the now prohibited monetary remedies); *see also* Shelia A. Millar & Tracy P. Marshall, *WW International to Pay $1.5 Million Civil Penalty for Alleged COPPA Violations*, 12 NAT'L L. REV. 88 (Mar. 29, 2022) https://www.natlawreview.com/article/ww-international-to-pay-15-million-civil-

pivots away from its previous claims that algorithmic disgorgement is comparable to monetary disgorgement, the FTC still has not established that Section 13(b) authorizes the use of algorithmic disgorgement. The Court stated in *AMG* that Section 13(b) concerns "prospective injunctive relief, not retrospective monetary relief."[159] Algorithmic disgorgement could fall in between these categories as retrospective non-monetary relief. Still, Section 13(b) does not authorize retrospective relief, be it monetary or injunctive.The Court emphasized the prospective nature of the Section, relying on language in the FTC Act which uses the present and future tense—the Commission may request relief when a company "is violating" or is "about to violate" the FTC Act.[160]

[35] Since algorithmic disgorgement generally seeks to remedy harms that have already happened at the time when data was improperly collected, a court would likely find algorithmic disgorgement (insofar as it is used to remedy improper data collection that has already occurred) incompatible with the language of Section 13(b), which authorizes prospective relief only. The FTC can instead argue that the use of algorithms derived from illegally obtained data is an ongoing violation of FTC rules. FTC officials, however, have not used this analysis. Instead, the FTC has stated that the purpose of algorithmic disgorgement is for a company to "forfeit the fruits of its deception"[161] and has further expressed the opinion that a company should "not be able to profit from" illegally collected data.[162] Commentators

penalty-alleged-coppa-violations [https://perma.cc/R5Z9-5J5E] ("Following the [AMG decision] . . . the FTC has used other enforcement tool, including . . . a renewed willingness to use algorithmic disgorgement[.]").

[159] AMG Cap. Mgmt., LLC v. FTC, 141 S. Ct. 1341, 1343 (2021).

[160] *Id*.

[161] FTC, *supra* note 2.

[162] Slaughter et al., *supra* note 1.

have also noted that algorithmic disgorgement is a "way to penalize companies" and to "make companies think twice about using data collected through unscrupulous means."[163] As of yet, there has been no talk from the FTC about algorithmic disgorgement as a way to address ongoing harms. If the FTC were to make such an argument, it is not likely to be successful—algorithmic disgorgement, by its nature, is a retrospective remedy, seeking to either punish companies because they obtained data improperly, dissuade other companies from doing the same, or to disgorge algorithmic profits which come from illegal data collection. None of these reasons address a specific and active unfair or deceptive practice by a company that could be stopped by the ordered deletion of algorithms.

[36] The FTC can also argue that by ordering algorithmic destruction it prevents further use of improperly obtained data. The FTC would have to show that the data is still being "used" by algorithms once they have already been trained. To be sure, the data on which algorithms are trained still "lives on" in the algorithm, as the algorithm only exists in its current form because it has analyzed and trained itself on the data.[164] The data, however, is anonymized, combined, and impossible to extrapolate from the model.[165] The data is no longer present in the form it was collected—only its "influence" remains. Does this constitute the "use" of the data? That is a hard, almost philosophical, query. As of now, the FTC has not stated its opinion on the question, instead opting to think of algorithms as the product of the data, and not a separate use of the data.

---

[163] Kaye, *supra* note 131.

[164] Amal Joby, *What Is Training Data? How It's Used in Machine Learning*, G2 (July 30, 2021), https://learn.g2.com/training-data [https://perma.cc/R5UZ-DNVF].

[165] Abigail Goldsteen, *AI goes anonymous during training to boost privacy protection*, IBM: RSCH. BLOG (Jan. 25, 2021), https://research.ibm.com/blog/ai-privacy-boost [https://perma.cc/Q7VZ-T5B9].

3. Section 18 Rule-Making Authority

[37] The most compelling authority through which the FTC could obtain the power to order algorithmic disgorgement is through its Section 18 rule-making.[166] If the FTC promulgates a rule, it can ask a court to "grant such relief as the court finds necessary to redress injury to consumers or other persons, partnerships, and corporations resulting from the rule violation or the unfair or deceptive act or practice, as the case may be."[167] The FTC has already taken the first step to adopting such rules by issuing an Advanced Notice of Proposed Rulemaking ("ANPR").[168] The ANPR states that the FTC is looking to pass new rules intended to enhance privacy protections and "restrict how businesses collect and use consumer data"[169] and is considering whether "a potential new trade regulation rule on commercial surveillance [should] explicitly identify algorithmic disgorgement . . . as a potential remedy."[170] Such rules must lay out specific acts that are considered to be "unfair or deceptive."[171] Once adopted, the FTC can essentially skip the Section 5(b) cease and desist process for companies that break the rules.[172] The FTC may commence a civil action against any

[166] 15 U.S.C § 57b(b).

[167] *Id.*

[168] *See* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022).

[169] Brian Fung, *FTC weighs sweeping new rules on 'commercial surveillance' and Big Data*, CNN BUS. (Aug. 11, 2022, 4:40 PM), https://www.cnn.com/2022/08/11/tech/ftc-new-rules-big-data [https://perma.cc/8F4A-CS9W].

[170] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. at 51, 273.

[171] 15 U.S.C. § 57a.

[172] *See id.* § 57b(a)(1).

company which violates a rule, and seek to obtain any relief "as the court finds necessary to redress injury . . . resulting from the rule violation."[173] This relief includes, but is not limited to, "rescission or reformation of contracts, the refund of money or return of property, the payment of damages, and public notification."[174] Since this non-exhaustive list of available remedies includes non-prospective injunctive relief, algorithmic disgorgement is likely a permissible relief available to the FTC for rule violations.

C. Possible Form of Future Orders

[38] So far, the language in algorithmic disgorgement consent agreements has been "profoundly vague,"[175] requiring the destruction of "any models or algorithms developed in whole or in part" using the improperly collected data.[176] This open-ended approach to algorithmic disgorgement orders provides "little detail about how the company must comply or how the FTC will know for sure it did."[177] The orders also do not limit the extent of what is required to be deleted and as "outputs of many models serve as the inputs for other models,"[178] a vaguely worded

[173] *Id.* § 57b(b).

[174] *Id.*

[175] Kate Kaye, *The FTC's 'profoundly vague' plan to force companies to destroy algorithms could get very messy*, PROTOCOL (Mar. 17, 2022), https://www.protocol.com/enterprise/ftc-algorithm-data-model-ai [https://perma.cc/L88A-VEME].

[176] *See* Decision and Order, *supra* note 5; Final Order, *supra* note 87; *see also* Stipulated Order, *supra* note 5.

[177] Kaye, *supra* note 175.

[178] Gesser et al., *supra* note 11.

algorithmic disgorgement order could be read to require deletion chains destroying algorithms that are almost entirely disconnected from the improperly obtained data. This result might not be entirely unintended by the FTC, which has taken a somewhat negative view of AI and data collection in recent years,[179] and the FTC might be seeking to discourage mass data collection in general. This could be due to the fact that in recent years, the FTC has been faced with a "wide range of concerns about commercial surveillance practices"[180] and a "growing body of evidence that some surveillance-based services may . . . lead to a wide variety of mental health and social harms."[181]

[39] If the FTC does adopt new rules, it is hard to predict if and how such rules will codify algorithmic disgorgement. As pointed out by Commissioner Noah Phillips in his dissenting statement regarding the ANPR, the ANPR "provides no notice whatsoever of the scope and

[179] *See, e.g.*, Press Release, FTC, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (June 16, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems [https://perma.cc/P8GY-JTT5]; Andrew Smith, *Using Artificial Intelligence and Algorithms*, FTC: BUS. BLOG (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms [https://perma.cc/2CJR-ZJUW]; *see also* Khari Johnson, *The FTC Is Closing in on Runaway AI*, WIRED (Sept. 12, 2022, 7:00 AM), https://www.wired.com/story/ftc-ai-regulation/ [https://perma.cc/AT2N-38GL].

[180] PRESS RELEASE, FTC, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices [https://perma.cc/TSN8-WHJR].

[181] *Id*.

parameters of what rule or rules might follow"[182] and it is "impossible to discern from this sprawling document . . . the number and scope of rules the Commission envisions."[183] The vagueness of the ANPR might suggest that language in any rules adopted by the FTC codifying algorithmic disgorgement might be as broad as that of the settlement orders that have preceded such rule-making.

[40] Still, it is possible to imagine that a codified and commonly used form of algorithmic disgorgement might have limits and guidelines on its use, both to protect from unintended consequences that might arise out of the ordered deletion of algorithmic models and to prevent arguments of vagueness and difficulty in enforcement.

IV. RISKS AND REWARDS OF ALGORITHMIC DISGORGEMENT

[41] Algorithmic destruction as a remedy by the FTC is fairly new and has only been used in limited circumstances.[184] The FTC has ordered algorithmic disgorgement only three times, always in settlements, and with companies that were in the midst of bankruptcy or restructuring by the time of the settlement or soon after.[185] This limited agency practice, combined

[182] FTC, DISSENTING STATEMENT OF COMM'R NOAH JOSHUA PHILLIPS: REGARDING THE COMMERCIAL SURVEILLANCE AND DATA SECURITY ADVANCE NOTICE OF PROPOSED RULEMAKING (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf [https://perma.cc/7LUX-XPKP].

[183] *Id.*

[184] Kaye, *supra* note 131.

[185] Nicholas Confessore & Matthew Rosenberg, *Cambridge Analytica to File for Bankruptcy After Misuse of Facebook Data*, N.Y. TIMES (May 2, 2018), https://www.nytimes.com/2018/05/02/us/politics/cambridge-analytica-shut-down.html [https://perma.cc/C2SF-9J3R] (reporting that Cambridge Analytica filed for bankruptcy

with the difficulty of predicting the shape of future orders, makes it hard to predict with any certainty what effects widespread use of algorithmic disgorgement by the FTC would bring. Nonetheless, this Part ventures to foresee the possible effects of the widespread use of algorithmic disgorgement orders and provides an overview of arguments both for and against its use.

A. The Case for Algorithmic Disgorgement

[42] The most obvious and direct benefit of algorithmic disgorgement is the deterrent effect it could have on improper data collection Even before *AMG* and the FTC's loss of its ability to seek monetary remedies under Section 13(b) of the FTC Act, the FTC wasn't always able to prevent the reappearance of improper data collection from repeat offenders who would pay the fines and then continue to commit infringing behavior in a different area.[186] So, while the FTC has levied massive fines on companies for

prior to the FTC settlement); *WW International, Inc. (WW) CEO Sima Sistani on Q2 2022 Results*, *supra* note 133 (stating that WW shut down Kurbo only months after the settlement); Joe Rossignol, *Photo Storage Service 'Ever' Shutting Down and Deleting All Photos and Videos on August 31*, MACRUMORS (Aug. 24, 2020, 10:00 AM), https://www.macrumors.com/2020/08/24/everalbum-shutting-down/ [https://perma.cc/GVL6-Z35H] (stating that Ever had already shut down by the time the FTC agreement was reached).

[186] *See, e.g.*, PRESS RELEASE, FTC, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (Jul. 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook [https://perma.cc/4MBC-E9ML]; Bailey Schulz, *Facebook sued over allegations it sidestepped Apple's privacy protections to collect user data*, USA TODAY (Sept. 22, 2022, 1:35 PM), https://www.usatoday.com/story/tech/2022/09/22/facebook-meta-lawsuit-apple-privacy-data/8080826001/ [https://perma.cc/2H96-UH85] (discussing how Facebook was once again faced with a class action suit accusing it of deceptive data collection practices just three years after the $5-billion penalty was imposed by the FTC); Craig Timberg & Tony Romm, *The U.S. government fined the app now known as TikTok $5.7 million for illegally collecting children's data*, WASH. POST

deceptive practices connected to data collection, such fines generally proved to be ineffective in addressing privacy concerns.[187] Algorithmic disgorgement might be a more effective deterrent than monetary penalties, as the loss of important models and algorithms could affect a company's ability to earn future revenue, or even cease certain operations.[188] Algorithmic disgorgement is a potentially much more effective deterrent than a simple monetary fine, which can be internalized by an offender as cost of doing business.[189] Given the propensity of large companies to ignore

(Feb. 27, 2019, 4:13 PM), https://www.washingtonpost.com/technology/2019/02/27/us-government-fined-app-now-known-tiktok-million-illegally-collecting-childrens-data/ [https://perma.cc/862R-S2ZK] (discussing how TikTok received an FTC penalty for similarly illegal data collection practices).

[187] *See, e.g.*, David Shepardson, *Two senators call for FTC probe into TikTok over U.S. data access*, REUTERS (July 5, 2022, 9:38 PM), https://www.reuters.com/business/media-telecom/two-senators-call-ftc-probe-into-tiktok-over-us-data-access-2022-07-05/ [https://perma.cc/5XY8-9YN8] (discussing how TikTok is again under scrutiny for the improper data collection less than three years after settling an almost $6 million FTC suit over the same issue).

[188] Kaye, *supra* note 131.

[189] *Id.* ("When it comes to today's data-centric business models, algorithmic systems and the data used to build and train them are intellectual property, products that are core to how many companies operate and generate revenue."); Heather Federman, *Tainted fruit: Disgorgement of data from the FTC and beyond*, IAPP (Apr. 27, 2021), https://iapp.org/news/a/tainted-fruit-disgorgement-of-data-from-the-ftc-and-beyond/ [https://perma.cc/P5BP-A4AS] ("While monetary fines and privacy/security program requirements have been helpful, some regulators, including Slaughter, have argued that such measures have not gone far enough. Strong relief for consumers may mean hitting companies where it hurts the most, requiring them to give up the data that powers their services in the first place."); David Carroll (@profcarroll), TWITTER (Oct. 6, 2021, 9:46 AM), https://twitter.com/profcarroll/status/1445747229256347650 [https://perma.cc/2QT6-RWCQ] ("Big fines are the cost of doing business. Algorithmic disgorgement traced to illicit data collection/processing is an actual deterrent.").

not just FTC rules against deceptive practices but also existing orders,[190] the threat of algorithmic disgorgement might increase compliance with FTC orders and settlements.

[43] Ordered deletion of models built with improper data might also alleviate some privacy concerns from the individuals whose data was collected. Professor Tiffany Li argues that even if data is deleted, an "imprint from the individual users" still remains as an "algorithmic shadow" in the algorithms trained on the data.[191] The persistence of this shadow means that "some measure of privacy loss cannot be undone" by simply deleting the data while allowing the algorithm to remain.[192] Once an algorithm has been trained on a user's data, Professor Li argues that the continued use of that algorithm poses some privacy harm to the user, even if their individual data is no longer distinguishable or in active use by the algorithm; only the deletion of the algorithm ensures that this privacy harm is removed.[193]

[44] Indirect benefits could also arise out of the increased use of algorithmic disgorgement. To best insulate themselves from the possibility of FTC enforcement, companies are encouraged to preemptively build governance and compliance models, track the usage of data, and increase vendor diligence.[194] While these measures are meant to reduce the risk of an

[190] *See, e.g.*, Lesley Fair, *Twitter to pay $150 million penalty for allegedly breaking its privacy promises – again*, FTC: BUS. BLOG (May 25, 2022), https://www.ftc.gov/business-guidance/blog/2022/05/twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again [https://perma.cc/2L47-BKK6].

[191] Li, *supra* note 155, at 498.

[192] *Id.*

[193] *Id.* at 502–03.

[194] Gesser et al., *supra* note 11.

FTC algorithmic disgorgement order or to mitigate the damage done by one, increased internal control, compliance, and record-keeping systems by data collectors also help bolster data security and privacy through oversight and monitoring.

[45] Arguments are also made that the destruction of algorithms is good for its own sake. AI algorithms come with a host of issues, ranging from unintended issues like racial[195] and gender[196] bias to intentional misuse for cyberattacks and spreading disinformation.[197] Some legislators have proposed bills to outright ban the use of algorithmic systems in certain cases, including for children,[198] and in the EU a proposed regulation would ban the use of AI for credit scoring systems and mass surveillance.[199] With

[195] Jinyan Zang, *Solving the problem of racially discriminatory advertising on Facebook*, BROOKINGS (Oct. 19, 2021), https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/ [https://perma.cc/7SNG-6GEX].

[196] Carmen Niethammer, *AI Bias Could Put Women's Lives at Risk – A Challenge for Regulators*, FORBES (Mar. 2, 2020, 4:19 AM), https://www.forbes.com/sites/carmenniethammer/2020/03/02/ai-bias-could-put-womens-lives-at-riska-challenge-for-regulators/?sh=3ab0088d534f [https://perma.cc/4CDR-9V3W].

[197] Vincent Boulanin & Charles Ovink, *Civilian AI is Already Being Misused by the Bad Guys*, IEEE SPECTRUM (Aug. 27, 2022), https://spectrum.ieee.org/responsible-ai-threat [https://perma.cc/TJ4V-4VMJ].

[198] Jon Brodkin, *Proposed law in Minnesota would ban algorithms to protect the children*, ARS TECHNICA (Mar. 18, 2022, 2:46 PM), https://arstechnica.com/tech-policy/2022/03/proposed-law-in-minnesota-would-ban-algorithms-to-protect-the-children/ [https://perma.cc/4XHZ-DFGN].

[199] James Vincent, *The EU is considering a ban on AI for mass surveillance and social credit scores*, THE VERGE (Apr. 14, 2021, 8:55 AM), https://www.theverge.com/2021/4/14/22383301/eu-ai-regulation-draft-leak-surveillance-social-credit [https://perma.cc/L57J-L3WC].

tech companies being accused of deeply consequential societal harms,[200] arguments are being advanced by some commentators that the destruction of certain algorithms and the disincentivizing of the creation of new ones, especially from companies that have a history of violating data privacy rules, will have a net positive effect on the world.[201]

B. The Case Against Algorithmic Disgorgement

[46] Despite the potential issues noted above, AI algorithms have become ubiquitous in our daily lives—including the billions of users relying on services such as Google search,[202] financial service firms using AI for risk management and fraud prevention,[203] and military uses such as the Iron Dome, to name a few.[204] Services relying on AI have become intertwined

[200] *See, e.g.*, *Facebook harms children and weakens democracy: ex-employee*, BBC NEWS (Oct. 6, 2021), https://www.bbc.com/news/world-us-canada-58805965 [https://perma.cc/8799-7GY6].

[201] *See, e.g.*, Press Release, Amnesty Int'l, Facebook and Google's Pervasive Surveillance Poses an Unprecedented Danger to Human Rights (Nov. 21, 2019), https://www.amnesty.org/en/latest/press-release/2019/11/google-facebook-surveillance-privacy/ [https://perma.cc/CKS7-6PZG].

[202] *See* Prabhakar Raghavan, *How AI is powering a more helpful Google*, GOOGLE BLOG (Oct. 15, 2020), https://blog.google/products/search/search-on/ [https://perma.cc/MT9B-TN4E]; *Google.com*, SIMILARWEB, https://www.similarweb.com/website/google.com/#overview [https://perma.cc/87EH-F6CV].

[203] *See* Eleni Digalaki, *The impact of artificial intelligence in the banking sector & how AI is being used in 2022*, BUS. INSIDER (Feb. 2, 2022, 2:04 PM), https://www.businessinsider.com/ai-in-banking-report [https://perma.cc/MT9B-TN4E].

[204] *See* Joanna van der Merwe, *Iron Dome Shows AI's Risks and Rewards*, CTR. FOR EUROPEAN POL'Y ANALYSIS (June 1, 2021), https://cepa.org/article/iron-dome-shows-ais-risks-and-rewards/ [https://perma.cc/KE3L-8HGG].

with their traditional, non-AI counterparts, and the loss or disruption of certain critical services could have widespread disastrous effects.

[47] These effects have not been felt yet because the violators targeted by the FTC have been relatively small, inconsequential companies that used AI as limited internal tools without much public-facing usage. Unfortunately, due to the high cost and access necessary to collect the massive amount of data required by AI algorithms, the most egregious violators of data collection rules are also the same companies whose AI tools are relied upon by most people.[205] Google may be bad for our data privacy—but if it was ordered to delete algorithms obtained from bad data, we could lose everything from effective Google Maps[206] to Google Translate.[207] Further, services such as Google Translate have been

[205] *See e.g.*, Press Release, FTC, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples [https://perma.cc/5PJ7-2MQW]; Natasha Singer & Kate Conger, *Google is Fined $170 Million for Violating Children's Privacy on YouTube*, N.Y. TIMES (Sept. 4, 2019), https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html [https://perma.cc/2XA3-PJNR]; PRESS RELEASE, FTC, FTC STAFF REPORT FINDS MANY INTERNET SERVICE PROVIDERS COLLECT TROVES OF PERSONAL DATA, USERS HAVE FEW OPTIONS TO RESTRICT USE (Oct. 21, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-staff-report-finds-many-internet-service-providers-collect-troves-personal-data-users-have-few [https://perma.cc/8X9K-8U9V]; Patience Haggin, *Lawmakers Want FTC to Investigate Apple, Google Over Mobile Tracking*, WALL ST. J. (June 24, 2022, 4:26 PM), https://www.wsj.com/articles/lawmakers-want-ftc-to-investigate-apple-google-over-mobile-tracking-11656077945 [https://perma.cc/2S4F-MUWZ].

[206] Russell Dicker, *A smoother ride and a more detailed Map thanks to AI* , GOOGLE: THE KEYWORD (May 18, 2021), https://blog.google/products/maps/google-maps-101-ai-power-new-features-io-2021/ [https://perma.cc/5KXB-PZWH].

[207] Nick Statt, *Google's AI translation system is approaching human-level accuracy*, THE VERGE (Sept. 27, 2016, 2:07 PM), https://www.theverge.com/2016/9/27/13078138/

consistently training with new data for over half a decade.[208] Under the broad language of current algorithmic disgorgement orders, the FTC could require that all of the algorithms on which such services are built be destroyed if any of the data used to train the model over the years is found to be improperly collected. This type of over-burdensome and disproportionate enforcement could potentially cause more harm than the violations it is trying to rectify.

[48] Further, as algorithmic disgorgement is targeted toward improper data *collection*, there is the uncertainty of what occurs when a data broker is found to have improperly collected data that is then sold to third parties.[209] Requiring companies which acquired bad data in good faith to delete algorithms built on it would be fundamentally unfair, costly, and only give more advantages to companies that have the means and ability to collect their own data. On the other hand, allowing for complete good faith buyer protection would simply incentivize brokers to collect bad data and companies to use third-party brokers. Algorithmic disgorgement would not be an effective deterrent for either the data brokers, which mainly sell data[210]

google-translate-ai-machine-learning-gnmt [https://perma.cc/2AMW-LTWY].

[208] Barak Turovsky, *Found in in translation: More accurate, fluent sentences in Google Translate*, GOOGLE: THE KEYWORD (Nov. 15, 2016), https://blog.google/products/translate/found-translation-more-accurate-fluent-sentences-google-translate/ [https://perma.cc/LLC7-ZCEM].

[209] *See, e.g.*, PRESS RELEASE, FTC, 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 [https://perma.cc/YS27-N7GV].

[210] *See* Justin Sherman, *Data Brokers Know Where You Are – and Want to Sell That Intel*, WIRED (Aug. 23, 2021, 7:00 AM), https://www.wired.com/story/opinion-data-brokers-know-where-you-are-and-want-to-sell-that-intel/ [https://perma.cc/5GK2-ZDWN].

and have no algorithms to destroy, or the buyers, who would be protected as good faith purchasers.

[49] Other than the possible deterrent effect, the ordered destruction of algorithms does not offer much privacy protection to users whose data was improperly harvested. Once an algorithm trains on data, that data is no longer needed for the algorithm to operate, and deleting the data will not make the algorithm "forget" what it learned.[211] While the individual training data undoubtedly influences the algorithm after it has been trained, in most cases the underlying data can be safely deleted resulting in the individual user data used to train the algorithm no longer being identifiable.[212] In these situations, the ordered deletion of trained models because of improperly obtained data would be akin to revoking someone's driver license because they learned to drive on a stolen car.

[50] Finally, there are obstacles that make compliance with and enforcement of algorithmic disgorgement orders difficult. Companies do not always have the best internal control mechanisms for collected data,[213] and while this lack of controls comes with its own privacy concerns, it

[211] Tom Simonite, *Now That Machines Can Learn, Can They Unlearn?*, WIRED (Aug. 19, 2021, 7:00 AM), https://www.wired.com/story/machines-can-learn-can-they-unlearn/ [https://perma.cc/VB9G-BGN8].

[212] *See id. But see* Niv Haim et al., *Reconstructing Training Data from Trained Neural Networks*, ARXIV (Dec. 5, 2022), https://arxiv.org/abs/2206.07758 [https://perma.cc/E2XY-2YLZ] (stating that researchers were able to reconstruct parts of a training dataset from a neural network).

[213] *Businesses Collect More Data Than They Can Handle, Reveals Gemalto*, THALES GRP. (July 10, 2018), https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/businesses-collect-more-data-than-they-can-handle-reveals-gemalto [https://perma.cc/8QGG-47WJ] ("[T]wo in three companies (65%) are unable to analyze all the data they collect and only half (54%) of companies know where all of their sensitive data is stored").

makes it hard to identify what specific algorithms were trained with what data. Further, other than a "written statement to the Commission, sworn under penalty of perjury" which confirms that the ordered algorithms were, in fact, deleted, there might not be a way for the FTC, or anyone else, to verify that all algorithms trained with the data in question were actually destroyed.[214] It is possible that neither the FTC nor the company itself would be able to correctly identify all algorithms which were trained on partly tainted data. This would leave it up to the FTC to list specific algorithms that are ordered to be destroyed, which could lead to the inclusion of AIs which were not trained on the bad data. An alternative would be to allow the companies themselves to determine which algorithms should be destroyed, but that could lead to algorithms beings spared when they shouldn't be, as there is no way for the FTC to verify exactly what data was used to train a given algorithm. However, more active involvement by the FTC earlier in the process could be a potential solution. A requirement like a "bill of data materials" for companies to monitor and document their data collection practices could be an effective tool to identify specifically what data is used to train individual algorithms. Requiring companies to keep records of their data collection practices and to track what algorithms collected data is used to train would allow for a more efficient auditing process and more effective compliance with any rules dealing with data collection.

C. Towards a Fair and Effective Algorithmic Disgorgement Policy

[51] Algorithmic disgorgement is perhaps one of the most effective post-*AMG* tools the FTC has to police improper data collection and usage,

[214] Decision and Order, *supra* note 5; *see also* Kaye, *supra* note 175 ("[T]he order provides little detail about how the company must comply or how the FTC will know for sure it did.").

"punching right at the heart" of tech firms.[215] While the use of algorithmic disgorgement orders is still sparse for now, it is "here to stay,"[216] and it emerges as a "compelling enforcement mechanism in need of clearer regulator guidance in terms of its actual application."[217]

[52] Proper usage of algorithmic disgorgement should balance its effectiveness as an enforcement tool with the far-reaching and potentially negative consequences the deletion of AI algorithms can cause. Instead of requiring full-scale destruction of all models obtained from tainted data, the FTC should instead focus on only those algorithms which are directly derived from improperly collected data and pose the most serious privacy risks. Further, the FTC should take efforts to phrase its orders in such a way that companies, to the extent technologically possible,[218] would be able to comply by making the machines "forget" the improper data without having to delete the entire algorithm.[219]

---

[215] Kaye, *supra* note 93.

[216] *Id.*

[217] Eda Uludere, *Fruits of Deception: Model Destruction as an Enforcement Tool*, DATAETHICS (July 13, 2022), https://dataethics.eu/deceptive-data-practices-can-lead-to-ai-model-destruction/ [https://perma.cc/Y2NR-VYM8].

[218] See *infra* notes 220–223 and accompanying text.

[219] *See* Simonite, *supra* note 211 ("Unlearning" is the middle ground between deleting just the data and deleting the entire algorithm. Its goal is "to remove all trace of a particular person or data point from a machine learning system, without affecting its performance," essentially leaving algorithms in the state they would have been if they were only trained on part of the data. For algorithms that were trained with partially "good" data and partially "bad" data, disgorgement orders which allow the algorithms to remain if they "unlearn" the bad data would solve the privacy concerns while allowing potentially useful algorithms to keep functioning. Unlearning is relatively new and not always possible, but progress is being made on making it a viable solution.).

[53] It is currently hard, if not impossible, to make a machine learning model "forget" the data that it was trained on.[220] For "many standard [machine learning] models, the only way to completely remove an individual's data is to retrain the whole model from scratch on the remaining data."[221] This process is time-consuming and not always feasible. However, researchers have recently begun developing methods to "efficiently delet[e] individual data points from trained machine learning models."[222] While this technology is still in the early stages, it could allow for a more measured implementation of algorithmic disgorgement orders. In cases where such "unlearning" can be done, it would allow for the deletion of the privacy-concerning "algorithmic shadow" without having to destroy the entire algorithm.[223] In other words, a company that received an algorithmic disgorgement order would no longer have to destroy the entire algorithm, but simply make it "forget" the training data which was improperly obtained. This would allow for the continuing operation of an AI even after an algorithmic disgorgement order.

[54] Further, even if "unlearning" is unfeasible in a particular situation, a critical amount of improperly collected data should be required in order to trigger an algorithmic disgorgement order. Many algorithms are trained on millions of data points obtained from a large variety of sources. To prevent the destruction of algorithms that were trained with overwhelmingly good data because a small subset of the data was obtained improperly, the FTC should look at each algorithm on a case-by-case basis

[220] Antonio A. Ginart et al., *Making AI Forget You: Data Deletion in Machine Learning,* 33 PROC. NEURAL INFO. PROCESSING SYS. 1, 9 (2019).

[221] *Id.* at 1.

[222] *Id.*; *see also* Matthew Hutson*, Researchers Can Make AI Forget You*, IEEE SPECTRUM (Jan. 15, 2020), https://spectrum.ieee.org/researchers-can-make-ai-forget-you [https://perma.cc/22AZ-5PPV].

[223] *Id.*

and decide whether algorithmic disgorgement is an appropriate remedy. Many algorithms, like those powering Google Search or Translate, are invaluable and have been training on data for years. If Google is found to have violated the privacy rights of a small subset of its users, it would be impractical to order the deletion of all its tainted algorithms, causing potentially millions in damages and leaving billions of users without essential tools. By establishing internal guidelines for when algorithmic disgorgement is appropriate, the FTC can ensure that the remedy is not used overeagerly or doing more damage than the initial privacy violations it is intended to remedy.

[55] Similarly, a statute of limitations-like time limit would prevent the tool from being overly zealous. Improper data collection is sometimes only discovered years after the behavior ended and forced deletion could lead to algorithms that were initially trained on improper data but have long switched to other data sources being destroyed. FTC limiting the use of algorithmic disgorgement to only those models that are found to use data that was impurely collected during a recent time period (for example, within the last three years) would still leave the FTC with an effective enforcement tool without being overburdensome.

V. CONCLUSION

[56] Algorithmic disgorgement is an effective tool that adds bite to the FTC's enforcement of laws and rules against deceptive data collection practices. But with the importance that AI plays in today's most commonly used technological services, the deletion of AI algorithms and models could have widespread unintended effects that outweigh the privacy benefits of the deletion. The FTC must carefully balance the privacy protections that algorithmic disgorgement offers with the costs of its regular use, including the stagnation of AI development and the possible loss or disruption of useful services. As the FTC looks to promulgate rules which standardize and codify algorithmic disgorgement, it should also build in protections and

backstops which ensure that the remedy is used in only the most egregious circumstances and with as little unintended harm as possible.