AMERICA’S NEXT “STOP MODEL!”: MODEL DELETION

Jevan Hutson* & Ben Winters**

TABLE OF CONTENTS

INTRODUCTION .................................................................................. 125

I. MODEL DELETION ............................................................................ 128
   A. As Remedy and Right ................................................................. 130
   B. As Requirement ......................................................................... 132

II. SEEKING MODEL DELETION .......................................................... 134
   A. Federal Enforcement Agencies .................................................. 134
      1. Federal Trade Commission (FTC) ........................................ 134
      2. Other Federal Agencies ...................................................... 138
   B. State Attorneys General ........................................................... 139
   C. Legislative Bodies ................................................................. 140
   D. Global Data Protection Authorities ......................................... 142

III. MODEL DELETION REQUIRES BROADER PRIVACY REGULATION ... 142
   A. Data Minimization .................................................................... 142
   B. Audits & Impact Assessments .................................................. 143
   C. Data Mapping & Provenance Requirements .............................. 144
   D. Private Right of Action .......................................................... 144

IV. CHALLENGES OF MODEL DELETION ......................................... 144

* Associate Attorney at Hintze Law PLLC, Seattle, WA. University of
   Washington School of Law, J.D. 2020. The views expressed in this article
   are his own and do not necessarily reflect the positions of any current or
   former employer or client.

** Senior Counsel at Electronic Privacy Information Center (EPIC) and
   lead of EPIC’s AI and Human Rights Project, Washington, D.C. Benjamin
   N. Cardozo School of Law, J.D. 2019.

This work was previously presented at the 2023 Privacy Law Scholars
Conference at the University of Colorado School of Law and 2022
WeRobot Conference at the University of Washington School of Law.
Special thanks to Meg Leta Jones and Stav Zeitouni for presenting our work
and to Emily McReynolds, Margot Kaminski, Lawrence Solum, Woodrow
Hartzog, Mona Sloane, Tiffany Georgievski, and others for helpful and
insightful comments. We are also indebted to Meredith Whittaker, Sarah
Myers West, Cedric Whitney, and Danica Noble for their support, insights,
and guidance. We acknowledge Tiffany C. Li for her important, initial work
on algorithmic destruction, and thank the leadership of the Federal Trade
Commission for their continued pursuit against unfair and deceptive
practices in artificial intelligence and machine learning.
INTRODUCTION

Famed American model and television personality Tyra Banks once wrote, “Love me or hate me I promise that it will never make or break me...<3.” Fortunately, the same cannot be said for harmful artificial intelligence (AI) and machine learning (ML) models. Indeed, harmful AI and ML models can and should be broken and more specifically, deleted.

It could be marketing materials or privacy policies that mislead users about whether uploaded photos are used to train facial recognition models, or a mobile application that fails to get verifiable parental consent to collect minors’ data and use it to train nutrition models. Businesses causing algorithmic harm should face deletion—effectively destruction—of significant portions of their

---

2 Examples of unfair AI and its harms have been well documented. See generally AI Now Inst., AI Now 2019 REPORT (2019); see, e.g., Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender, 81 PROC. MACH. LEARNING RESCH. 1 (2018); Inioluwa Deborah Raji, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee & Emily Denton, Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing (Jan. 3, 2020), https://arxiv.org/abs/2001.00964 [https://perma.cc/PKL9-9XVH]; see also Os Keyes, The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition, 2 PROC. ACM ON HUM.-COMPUT. INTERACTION 1 (2018) (analyzing the harms of automated gender recognition in the context of bathrooms); see infra Part V.
AI and ML related work products, including datasets, algorithms, models, and materials affected by the illegally acquired data.

With the advent of AI tools in the absence of adequate AI regulations, algorithmic harm is rampant. AI systems can cause bodily harm, discrimination, loss of opportunity, and dignitary harms, among others. For example, in 2020, Epic Health Systems marketed the Epic Sepsis Model as an algorithm that could predict when patients were experiencing sepsis—a life-threatening emergency. The Epic Sepsis Model, an automated decision-making system that uses proprietary statistical models, was adopted widely by hospitals throughout the country and marketed as 76–83% accurate. But when validated independently, the system’s accuracy was significantly lower. Researchers found that the tool failed to identify risk in 67% of the patients who actually experienced sepsis and generated alarming results for 18% of all hospital patients, most of whom did not turn out to have sepsis. The over-inclusive and under-inclusive nature of the model contributed to “alert fatigue” among hospital staff. In this case, the use of an automated decision-making system that was not properly validated could have (and indeed, may have) caused physical harm to individuals.

The Epic Sepsis Model is not the only one to cause algorithmic harm. A recent study of health records for 57,000 people found that an algorithm used in determining eligibility and prioritization for kidney transplants unfairly prevented Black patients from receiving transplants. As another example, students are also constantly subjected to unavoidable automated decision-making and analysis. A wide range of educational systems have adopted automated exam

---

7 See sources cited in supra note 2.
9 Cull et al., supra note 8, at 1. Wong et al., supra note 8.
10 Cull et al., supra note 8, at 1.
11 Id.
monitoring, communications screening on school-mandated laptops, and surveillance through proctoring systems.\textsuperscript{13} These systems claim to use automated decision-making systems that can accurately detect indicators of cheating by tracking factors like student speech, eye movements, mouse clicks, and pacing.\textsuperscript{14} In reality, they are prone to bias and error, placing students' academic standing in jeopardy. For example, a Florida teenager was flagged for potential cheating by Honorlock's automated proctoring system when she looked away from her screen during a test.\textsuperscript{15} As a result, the student received a zero on the exam.\textsuperscript{16} These intrusive monitoring systems, like other commercial surveillance technologies, can force students to carefully regulate how they act to avoid adverse automated decisions—even if their behavior is innocuous.

Model deletion, as this Essay advocates, presents a unique and viable enforcement option that may meaningfully deter bad corporate actions. Illegally collected and curated data should not only lead to regulatory inquiries and hefty fines but also the destruction of all work-product tied back to it. If, for example, particular models that are core to a company's services are irredeemably contaminated, model deletion would require the company to destroy the contaminated model and start from scratch. In some instances, this may effectively shut down a company.

In the bigger picture, model deletion is “an innovative...remedy”\textsuperscript{17} because it may not only cure underlying AI harms but also “reverse structural incentives to maximize information collection and abuses.”\textsuperscript{18} As a remedy and lever for law enforcement, model deletion would deter harmful AI and the broader

\textsuperscript{13} See Kashmir Hill, Accused of Cheating by an Algorithm, and a Professor She Had Never Met, N.Y. TIMES (May 27, 2022), https://www.nytimes.com/2022/05/27/technology/college-students-cheating-software-honorlock.html [https://perma.cc/2GGX-XQ9W].


\textsuperscript{15} Hill, supra note 13.

\textsuperscript{16} Id.

\textsuperscript{17} Kelly Slaughter, Acting Chairman, Fed. Trade Comm’n, Remarks at the Future of Privacy Forum: Protecting Consumer Privacy in a Time of Crisis (Feb. 10, 2021) [hereinafter Slaughter Remarks].

\textsuperscript{18} Samuel Levine, Director, Bureau Consumer Prot., Keynote Remarks at the Cleveland-Marshall College of Law Cybersecurity and Privacy Protection Conference (May 19, 2022) [hereinafter Levine Remarks].
A framework of surveillance capitalism because it would disincentivize wanton data extractionism and incentivizes dataset accountability. A business’s entire AI work product would be on the line if it does not get data collection, security, provenance, and hygiene right. Dataset and model accountability would be the cost of doing business.

This Essay explores the emergence of model deletion—the compelled destruction or dispossession of certain data, algorithms, models, and associated work products created or shaped by illegal means—as a remedy, right, and requirement for harmful applications of AI and ML systems. Part I examines model deletion’s emergence as a consumer protection remedy and its conception as a positive right and regulatory requirement. Part II considers the constellation of federal and state actors, such as federal and state enforcement agencies and legislative bodies, who might seek model deletion to address particular AI and ML harms. Part III underscores the need to legislate broader privacy and data protection regulation to bolster the effectiveness of model deletion. Part IV reflects on the challenges of model deletion, including the scope and enforcement of model deletion orders and logistical issues for companies undergoing model deletion. Finally, Part V imagines how model deletion would apply to a company whose product has caused immense algorithm harm—Clearview AI.

I. MODEL DELETION

“Model deletion,” also referred to interchangeably as model or algorithmic disgorgement, algorithmic destruction, and model destruction, is the compelled destruction or dispossession of data,

22 Li, supra note 6.
algorithms, models, and associated work products that are created or shaped by illegal means. Its techniques offer a potential solution to address training corpus data defects by eliminating not only improperly used data but also the effects of such data on any component of an ML model. These techniques can help “reduce[e] bias and toxicity, increase[e] fidelity, and ensure[e] responsible usage of intellectual property.”

In practice, model deletion has been applied as a remedy to consumer protection violations. In legal and technical scholarship, model deletion has been conceived as a potential remedy to a privacy violation as well as a potential industry or statutory requirement for ML practitioners. As both a legal and technical matter, model deletion operates on a spectrum: from localized machine unlearning or selective forgetting—where the affected data is a small fraction

24 “Illegal means” have thus far involved violations of Section 5 of the FTC Act (unfair or deceptive acts or practices) and the Children’s Online Privacy Protection Act (COPPA).
25 See generally Alessandro Achille, Michael Kearns, Carson Klingenberg & Stefano Soatto, AI Model Disgorgement: Methods and Choices 1 (Apr. 7, 2023), https://arxiv.org/pdf/2304.03545.pdf [https://perma.cc/7LVW-JYYM] (“Developers of large models should understand their options for implementing model disgorgement, and novel methods to perform model disgorgement should be developed to help ensure the responsible usage of data.”).
26 Id. at 1.
27 Slaughter et al., supra note 21, at 5.
28 See infra Part I.A.
29 See infra Part I.B.
30 See Achille et al., supra note 25 (“If the cohort of data that triggers the need for [model disgorgement] is a small fraction of the overall training data, it may be possible to characterize and eliminate its influence on the trained model without the need to retrain the model.”); see also Yinzhi Cao & Junfeng Yang, Towards Making Systems Forget With Machine Unlearning, IEEE SYMP. ON SEC. & PRIV. 463, 468–80 (2015); Antonio Ginart, Melody Guan, Gregory Valiant & James Zou, Making AI Forget You: Data Deletion in Machine Learning, ADVANCES NEURAL INFOR. PROCESSING SYS. 3518 (2019); Aditya Golatkar, Alessandro Achille, Avinash Ravichandran, Marzia Polito & Stefano Soatto, Mixed-Privacy Forgetting in Deep Networks, PROC. IEEE/CVF CONF. ON COMPUT. VISION AND PATTERN RECOGNITION 792 (2021); Aditya Golatkar, Alessandro Achille & Stefano Soatto, Eternal Sunshine of the Spotless Net: Selective Forgetting in Deep Networks, PROC. IEEE/CVF CONF. ON COMPUT. VISION AND PATTERN RECOGNITION 9304 (2020); Aditya Golatkar, Alessandro Achille & Stefano Soatto, Forgetting Outside the Box: Scrubbing Deep Networks of Information Accessible from Input-Output Observations, EUROPEAN CONF. ON COMPUT. VISION 383 (2020).
A. As Remedy and Right

Model deletion first arose as a remedy in the context of federal consumer protection law as a tool in the Federal Trade Commission’s (FTC) tool belt. The first application of model deletion by the FTC was the agency’s 2019 final order in *In re Cambridge Analytica, LLC*, in the context of harvesting information from Facebook users for voter profiling and targeting.\(^32\) In May 2021, the FTC again ordered model deletion in its decision and order in *In re Everalbum, Inc.* in the context of facial recognition technology.\(^33\) In March 2022, the FTC affirmed model deletion as an active consumer protection enforcement remedy in *United States v. Kurbo*, in the context of children’s privacy rights.\(^34\)

\(^{31}\) Li, *supra* note 6, at 498.


\(^{33}\) See Decision and Order at 5, *In re Everalbum, Inc.*, No. C-4743 (FTC May 6, 2021) (“Within ninety (90) days after the issuance of this Order, delete or destroy any Affected Work Product, and provide a written statement to the Commission, sworn under penalty of perjury, confirming such deletion or destruction.”) where “Affected Work Product” is defined as “any models or algorithms developed in whole or in part using Biometric Information Respondent collected from Users of the ‘Ever’ mobile application.”) [hereinafter Everalbum Order]; see also Press Release, Fed. Trade Comm’n, FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology (May 7, 2021), https://www.ftc.gov/news-events/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse [https://perma.cc/ED67-3XJ5] (“As part of the settlement with the FTC, Everalbum, Inc. must obtain consumers’ express consent before using facial recognition technology on their photos and videos. The proposed order also requires the company to delete the photos and videos of Ever app users who deactivated their accounts and the models and algorithms it developed by using the photos and videos uploaded by its users.”).

\(^{34}\) See Kurbo Order at 8, *supra* note 5 (“Within ninety (90) days of entry of this Order, delete or destroy any Affected Work Product, and provide a
In each of the cases, the FTC conceptualized model deletion as a remedy to consumer protection violations. As FTC Commissioner Rebecca Slaughter, Janice Kopec & Mohamad Batal explained, “when companies collect data illegally, they should not be able to profit from either the data or any algorithm developed using it.”35 In discussing model deletion, Slaughter analogizes its underlying principle to that of monetary disgorgement:

We routinely obtain disgorgement of ill-gotten monetary gains when consumers pay for a product that is marketed deceptively. Everalbum shows how we can apply this principle to privacy cases where companies collect and use consumers’ data in unlawful ways: we should require violators to disgorge not only the ill-gotten data, but also the benefits—here, the algorithms—generated from that data.36

Thus, model deletion functions as forms of retrospective, non-monetary relief. It remedies past harms—whether a violation of children’s privacy laws or consumer protection harms like data collected by deceptive policy representations—by destroying the work products that cause such harms.

Furthermore, while not yet applied in such a manner, model deletion can also function as a form of prospective, permanent injunctive relief. If a particular ML model is violating or about to violate the FTC Act’s prohibitions on unfair and deceptive practices, seeking model deletion would address the ongoing and future consumer protection harms posed by that particular ML system.

written statement to the Commission, sworn under penalty of perjury, confirming such deletion or destruction,” where “Affected Work Product” is defined as “any models or algorithms developed in whole or in part using Personal Information Collected from Children through the Kurbo Program.”); see also Press Release, Fed. Trade Comm’n, FTC Takes Action Against Company Formerly Known as Weight Watcher for Illegally Collecting Kids’ Sensitive Health Data (Mar. 4, 2022), https://www.ftc.gov/news-events/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers [https://perma.cc/J3W4-A6MB] (“The settlement order also requires the companies to destroy all personal information previously collected that did not comply with the COPPA Rule’s parental notice and consent requirements unless the companies’ obtained subsequent parental consent to retain such data. The settlement also requires the companies to destroy any affected work product that used data illegally collected from children in violation of COPPA.”).

35 Slaughter et al., supra note 21, at 39.

36 Slaughter Remarks, supra note 17.
Used in this way, model deletion would function as a “preventative” remedy that seeks to discourage, avert, and literally undo the technological means of harm and deprive defendants of the benefit of wrongful acts.\textsuperscript{37} As a non-compensatory remedy, it is designed to change the behavior of both people and machines. Not only would it change the decisions people must make in the course of developing AI and ML technologies, but it would also invariably change the performance and deployment of those very technologies. Model deletion, therefore, offers a counterpoint to Scholars Mark Lemley and Bryan Casey’s contention that “remedial mechanisms used to shape human behavior cannot be relied upon to do the same when machines, not people, engage in harmful conduct.”\textsuperscript{38}

Beyond its conceptualization as either a retrospective or prospective remedy, legal scholars have further conceived of model deletion as a potential positive right for individuals.\textsuperscript{39} To address the panoply of privacy harms presented by AI and ML—such as group privacy harms, indirect privacy harms, and proxy privacy harms—Tiffany Li, privacy law scholar, considers model deletion as a positive privacy right.\textsuperscript{40} Similarly, model deletion may be useful as a positive right in addressing algorithmic harms. While no current U.S. nor global privacy data protection law includes a right to model deletion, Li contends that legislating model deletion as a right may shift risks and incentives in favor of more responsible and accountable AI and ML practices.\textsuperscript{41}

B. As Requirement

Turning to another framework, AI and ML practitioners have conceived of model deletion as a technical best practice that may form the basis of an industrial, technical, or legal design requirement for AI and ML systems. Researchers Alessandro Achille, Michael Kearns, Carson Klingenberg, and Stefano Soatto define model disgorgement as “the elimination of not just the improperly used data, but also the effects of improperly used data on any component

\textsuperscript{37} \textsc{Douglas Laycock, Modern American Remedies} 3 (2010); see also Mark A. Lemley & Bryan Casey, \textit{Remedies for Robots}, 86 U. Chi. L. Rev. 1311, 1378–95 (2019).

\textsuperscript{38} Lemley & Casey, supra note 37.

\textsuperscript{39} See Li, supra note 6, at 503.

\textsuperscript{40} See id. at 504.

\textsuperscript{41} See id. at 503 (“Introducing algorithmic disgorgement as a privacy right in privacy law would increase the potential compliance burdens on companies but could also increase the deterrent effect, raising the risks to such an extent that companies would be encouraged to be even more careful with their use of data and machine learning.”).
of an ML model[]."

They contend that model disgorgement, as a possible solution for training corpus data defects, can “address a wide range of issues, such as reducing bias or toxicity, increasing fidelity, and ensuring responsible usage of intellectual property.”

As such, they introduce a variety of technical methods to effectuate model disgorgement, including reactive disgorgement, proactive disgorgement, and preemptive disgorgement.

Similarly, emerging risk management policy frameworks suggest a need for AI and ML systems to be halted or deprecated when exceeding risk parameters or causing harm. The National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI RMF) centers decommissioning and phasing out AI systems as core to baseline AI governance as well as post-deployment AI system monitoring plans.

In particular,

42 See generally Achille et al., supra note 25.
43 Id. at 1.
44 See id. at 2 (“Large-scale neural networks can be trained on datasets that comprise web-scale data. In such cases, the need for model disgorgement may arise from, among other things, errors in the data collection and curation process.”).
45 See id. at 3 (“Given that even the tightest standards of data curation can be imperfect at the scale of the datasets in use today, it may be worthwhile to train ML models in preparation for possible MD. That is, the ML models could be trained in such a way that MD can be later performed with minimal impact on the overall trained model. We call this proactive disgorgement.”).
46 See id. at 4 (“Preemptive disgorgement refers to modifications of the training process that, by design, ensure that ‘unique information’ contained in any cohort of samples in the training data is bounded by a small value selected by the system designer.”); see also Hrayr Harutyunyan, Alessandro Achille, Giovanni Paolini, Orchid Majumder, Avinash Ravichandran, Rahul Bhotika & Stefano Soatto, Estimating Informativeness of Samples With Smooth Unique Information, INT’L CONF. ON LEARNING REPRESENTATIONS (2021).
47 See NAT’L INST. OF STANDARDS AND TECH., U.S. DEP’T OF COM., NIST AI 100-1, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) (2023) (“GOVERN 1: Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively . . . . GOVERN 1.7: Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization’s trustworthiness . . . . MANAGE 4: Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly . . . . MANAGE 4.1: Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.”).
subsection 1.7 of the “Govern” framework recommends “[p]rocesses and procedures [to be] in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization’s trustworthiness,” and subsection 4.1 of the “Manage” framework prescribes that “[p]ost-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.”48

As a requirement, model deletion would thus function as a narrow, ad-hoc technical mitigation strategy for problematic data and the models they impact. It would also function as a broader design expectation for practitioners building AI and ML systems, under which models would be expected to be dischargeable in the first instance and disgorged if the system exceeds a particular risk tolerance threshold.

II. SEEKING MODEL DELETION

We argue that a variety of federal and state actors should seek model deletion in certain circumstances. For the purposes of this Essay, we focus in chief on consumer protection enforcers, namely the FTC, the Consumer Financial Protection Bureau (CFPB), and state attorneys general, as actors who should seek model deletion in enforcing laws under their purview. However, we also consider the potential authority of other federal agencies, such as the Department of Justice (DOJ), Equal Employment Opportunity Commission (EEOC), and Securities and Exchange Commission (SEC), as well as the authority of legislative bodies and global data protection authorities.

A. Federal Enforcement Agencies

1. Federal Trade Commission (FTC)

The Federal Trade Commission Act (FTC Act) prohibits “unfair or deceptive acts or practices” and authorizes the Commission to enforce the prohibition.49 It affords the Commission both its own

48 Id. at 22–23, 32–33 (emphasis added).
administrative proceedings, as set forth in section 5 of the Act, and internal court actions related to exercise of this authority.

In 1973, Congress amended section 5(l) of the FTC Act to authorize district courts to award civil penalties against respondents who violate final cease and desist orders, and to “grant mandatory injunctions and such other and further equitable relief as they deem appropriate in the enforcement of such final orders of the Commission.” In 1975, Congress enacted section 19 of the Act, which authorizes district courts to grant “such relief as the court finds necessary to redress injury to consumers,” including through the “refund of money or return of property.” However, Congress specified that remedy available under section 19 could be sought only against those who have “engage[d] in any unfair or deceptive act or practice.”

Scholars have written about how such authority makes the Commission the preferred regulatory agency for protecting consumers who buy and interact with harmful AI and ML systems because such systems may constitute “unfair and deceptive practices.” Given its remedial authorities in sections 5 and 19, the FTC may be authorized to seek model deletion in three ways. First, the FTC is authorized to seek model deletion in its course of settling with persons, partnerships, or corporations under investigation, as in

---

50 AMG Capital Mgmt., LLC v. Fed. Trade Comm’n, 141 S. Ct. 1341, 1345–46 (2021). Justice Breyer aptly summarizes these administrative proceedings: “[T]he Commission has ‘reason to believe’ that a party ‘has been or is using any unfair method of competition or unfair or deceptive act or practice,’ it can file a complaint against the claimed violator and adjudicate its claim before an Administrative Law Judge. The ALJ then conducts a hearing and writes a report setting forth findings of fact and reaching a legal conclusion. If the ALJ concludes that the conduct at issue was unfair or misleading, the ALJ will issue an order requiring the party to cease and desist from engaging in the unlawful conduct. The party may then seek review before the Commission and eventually in a court of appeals, where the ‘findings of the Commission as to the facts’ (if supported by the evidence) ‘shall be conclusive.’ If judicial review favors the Commission (or if the time to seek judicial review expires), the Commission’s order normally becomes final (and enforceable).” Id. at 1346 (citing 15 U.S.C. §§ 45(b), (c), (g)).


52 Id. § 45(l).

53 Id. § 57(b).

54 Id. § 57(b)(a)(2).

In remarks shortly after the *Kurbo* settlement was announced, Samuel Levine, the Director of the Bureau of Consumer Protection at the FTC, said:

> When we bring enforcement actions, we are committed to obtaining strong, forward leaning remedies that not only cure the underlying harm but also reverse structural incentives to maximize information collection and abuses. This starts with the simple principle that companies should not be able to profit from illegal data practices. That’s why we are committed to not only requiring the deletion of unlawfully obtained data, but also the deletion of algorithms and other work products derived from the data.\(^{57}\)

The FTC showing proactive interest in using the remedy is encouraging, but the agency needs more support and more teeth to do it effectively.\(^{58}\)

Second, the FTC is arguably authorized to seek model deletion when persons, partnerships, or corporations violate final orders, rules, or injunctions of the commission.\(^{59}\) The Supreme Court in *AMG Capital Management, LLC v. Federal Trade Commission* highlighted sections 5(l) and 19 of the FTC Act as empowering district courts “to impose limited monetary penalties and to award monetary relief in cases where the Commission has issued cease and desist orders, i.e., where the Commission has engaged in administrative proceedings. In these provisions, Congress explicitly provided for ‘other and further equitable relief’ and for the ‘refund of money or return of property[.]’”\(^{60}\)

To be sure, following the Court’s ruling in *AMG Capital Management*, the FTC may face arguments that it is not authorized to seek model deletion under section 13(b) of the FTC Act.\(^{61}\) Indeed, the *AMG* ruling has significantly impeded the FTC’s capacity to secure monetary relief for unfair and deceptive practices, depriving the agency of its “most potent tool to aid consumers.”\(^{62}\) However,

\(^{56}\) See *Kurbo* Order, *supra* note 5; *Everalbum* Order, *supra* note 33.

\(^{57}\) Levine Remarks, *supra* note 18.

\(^{58}\) See infra Parts II.B–II.D, III.


\(^{60}\) *AMG Capital Mgmt, LLC v. Fed. Trade Comm’n*, 141 S. Ct. 1341, 1348–49; § 57b(b).

\(^{61}\) See *AMG Capital Mgmt, LLC*, 141 S. Ct. at 1350.

model deletion is critically not monetary. And in the wake of this ruling, the FTC has sought legislative action from Congress to bolster its enforcement authority and has sought alternative non-monetary enforcement methods.\textsuperscript{63}

Third, the FTC is authorized to promulgate rules—pursuant to its rulemaking authority under section 18 of the FTC Act\textsuperscript{64}—and seek action in federal court against those who violate them.\textsuperscript{65} Indeed, the FTC has already initiated an attempt at promulgating rules regarding model deletion and deletion as a remedy for the agency in its Advanced Notice of Proposed Rulemaking (ANPR) on commercial surveillance and data security.\textsuperscript{66} Specifically, the FTC asks the following with respect to remedies available to the agency:

How should the FTC’s authority to implement remedies under the Act determine the form or substance of any potential new trade regulation rules on commercial surveillance? Should new rules enumerate specific forms of relief or damages that are not explicit in the FTC Act but that are within the Commission’s authority? For example, should a potential new trade regulation rule on commercial surveillance explicitly identify algorithmic deletion, a remedy that forbids companies from profiting from unlawful practices related to their use of automated systems, as a potential remedy? Which, if any, other remedial tools should new trade regulation rules on commercial surveillance explicitly identify? Is there a limit to the Commission’s authority to implement remedies by regulation?\textsuperscript{67}


\textsuperscript{64} 5 U.S.C § 57b(b).

\textsuperscript{65} Insofar as the FTC promulgates a rule under 15 U.S.C § 57b(b), it may 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.” 15 U.S.C § 57b(b).


\textsuperscript{67} Id. at 13.
2. Other Federal Agencies

Other federal agencies should also consider using model deletion in the enforcement of laws pursuant to their authorities. For example, the CFPB’s mandate to protect against harms in consumer financial services lends itself naturally to using model deletion. Indeed, the CFPB published a circular in May of 2022, confirming that the federal consumer finance laws and adverse action requirements it is empowered to enforce apply to AI and ML technologies.

For example, section 1055 of the Dodd-Frank Wall Street and Consumer Protection Act authorizes the CFPB to seek "all appropriate legal and equitable relief" for violations of federal consumer financial laws. Such power gives the CFPB the authority to seek deletion of ill-gotten gains. Indeed, the CFPB has used its authority to seek monetary disgorgement in several high-profile cases. To take one, in December 2022, the agency ordered Wells Fargo Bank to pay more than $2 billion in consumer redress for its widespread mismanagement of auto loans, mortgages, and deposit accounts. Given the parallel principles underlying monetary disgorgement and model deletion, the CFPB should also have the authority under this section to order model deletion.

Similarly, the DOJ is also positioned well to wield model deletion in enforcing laws. Indeed, in April 2023, DOJ’s Civil Rights Division, alongside heads of the CFPB, EEOC, and FTC, jointly pledged to “uphold America’s commitment to the core principles of fairness, equality and justice as emerging automated systems, including those sometimes marketed as ‘artificial intelligence’ or ‘AI,’ become increasingly common in our daily lives – impacting civil rights, fair competition, consumer protection and equal opportunity.” Under DOJ’s authority to enforce Title VI of the

---


71 Press Release, Dep’t of Just., Justice Department’s Civil Rights Division Joins Officials from CFPB, EEOC and FTC Pledging to Confront Bias and Discrimination in Artificial Intelligence (Apr. 25, 2023),
Civil Rights Act, the DOJ should consider model deletion as a viable enforcement tool. Because a variety of algorithms are federally funded, adopting model deletion would expand the DOJ’s ability to address algorithms used to discriminate based on race and other protected categories.

B. State Attorneys General

Model deletion, while not yet wielded at the state level, is arguably also available to state attorneys general. Specifically, state attorneys general may bring actions under unfair and deceptive acts or practices (UDAP) statutes, which service as mini-FTC Acts for each state.72 These statutes empower state attorneys general offices, and, in some cases, private litigants to enforce consumer protection laws.73 While state UDAP statutes parallel the language of section 5 of the FTC Act, they often have more teeth in terms of enforcement, such as allowing private rights of action, affording minimum and multiple damages, and awarding attorney’s fees for the prevailing consumer plaintiff.74 State attorneys general could wield model deletion in the enforcement of their respective state’s UDAP statutes. Again, model deletion could function as a lever for either retrospective non-monetary relief or prospective and permanent injunctive relief. As detailed in Part V, the Vermont Attorney General has a pending unfair and deceptive practices suit against data abuser and facial recognition company Clearview AI.75 This suit would be one in which deletion is an appropriate remedy, and


73 See generally CARTER, supra note 72.

74 See generally id.

75 See infra Part V.
represents the role of state attorneys general in adopting model deletion.

C. Legislative Bodies

In Part II, we argued that model deletion is, at least, implicitly supported by state and federal laws, particularly those prohibiting unfair, deceptive, and abusive acts and practices, and should be available as a remedy to parties empowered by those laws. However, one of the many reasons there has been a consistent failure to hold companies accountable for their harmful AI and ML practices is how clunky, squishy, insufficient, and politically tenuous the process of piecemeal enforcement is. While hopeful, Kurbo may be characterized as an exception: the FTC’s success was in part attributable to the extent to which the harms were obvious, the obligations were clear, and the social context was less up for debate or political interference. It was also brought under Children’s Online Privacy Protection Act (COPPA), which does not apply to algorithmic harms on adults. Similarly, the other cases leading to violations were particularly egregious practices that were obvious and at the top of the news cycle for months.76

Meaningful consumer protection means making strong enforcement actions routine, not spectacular. Thus, state and federal legislative bodies should consider additional legislative interventions that would wield model deletion as a method to address algorithmic harms expressly by statute—as a remedy, right, or requirement.77

First, state and federal legislatures can enshrine model deletion as a remedy or right by statute within new or existing consumer protection law. They can also enshrine model deletion as a remedy by statute within domains beyond consumer protection laws, including anti-discrimination and intellectual property laws. As Li explicitly argues that “we should consider model deletion as a


77 Li unpacks the limitations and potential of algorithmic destruction as both right and remedy. Our consideration of legislative action to enshrine algorithmic destruction, either by right or remedy, is a direct extension of Prof. Li’s work. See Li, supra note 6.
privacy right to be included in privacy laws,“78 statutory regulations of AI and ML technology should also consider model deletion as a right included in AI laws. Second, as a remedy, state and federal governments should explicitly include model deletion or other mechanisms for decommissioning systems by design as a remedy to consumer protection laws.

Finally, they should enshrine model deletion as a requirement. This would differ from model deletion’s role as a remedy in that model deletion as a requirement would include mandating data mapping and provenance requirements for systems of a certain size.79 It is imperative for developers of models to be aware of model deletion options and to develop novel methods to ensure responsible data usage. Developers must carefully collect and document data, respect intellectual property and individual privacy, and use data ethically. As ML models have grown in size and complexity, the large amount of required training data makes it difficult to manually inspect each datum for defects despite sophisticated controls on training data. This cannot be an excuse. Regulators must ensure “too big to destroy” does not become an option. Effectively, legislators may and should constrain the development of harmful AI and ML achieved through obfuscated, manipulative, or otherwise abusive data collection.

Frameworks for designing these systems can be guided by the NIST AI RMF80 and the Blueprint for an AI Bill of Rights,81 which both include urges to document the data lifecycle extensively, continually evaluate, and proactively decommission tools that exceed certain defined risk tolerances. These documents, prepared at the highest levels of the federal government, both explicitly include recommendations that embody the principles of model deletion.82

---

78 Id. at 23.
79 See infra Part III.C.
80 NAT’L INST. OF STANDARDS AND TECH., supra note 47.
Governments should integrate these sets of recommendations into prerequisites for their own purchase or use of AI systems and extend certain requirements for any systems, schools, hospitals, and law enforcement agencies that are funded by government money. Doing so could also influence the behavior of companies developing or using AI tools to do better diligence when deciding how to build models or which AI tool vendor to contract with.

D. Global Data Protection Authorities

Model deletion, as a remedy, right, and requirement, is not limited to the U.S. Given the repeated use of model deletion by the FTC, a comparatively weak and underfunded data protection authority relative to global peers, as well as receptive commentary by civil society to its application, it stands to reason that the deletion of models and AI work product could and should also be used by global data protection authorities—such as the French CNIL, UK ICO, South Korean PIPC—in enforcement actions against entities that commit transnational and international algorithmic harms.

III. MODEL DELETION REQUIRES BROADER PRIVACY REGULATION

Model deletion cannot act alone: responsible data use and privacy protection is crucial in any ML implementation. Indeed, AI and ML harms often include privacy harms, which consist of economic, emotional, or bodily harms. This Part outlines some principles of responsible data use and privacy protection to supplement model deletion.

A. Data Minimization

Data minimization is a principle requiring a data collector to “limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose” and "retain the data only for as long as is necessary to fulfill that purpose.” Data minimization would not only reduce the number of cases in which model deletion would be necessary, but it would also allow enforcement agencies to use failure to minimize data as a violation on its own and as a basis for model deletion. The FTC, for example, may mandate data minimization through a section 5 rulemaking.

B. Audits & Impact Assessments

Audits and impact assessments are vehicles for transparency about how algorithms work and how they are used. Whereas audits evaluate the accuracy and bias of a system based on the model(s) they are using, impact assessments deal with more systemic questions, such as what kind of data is being used and how it is being collected. While they can take various formats, several civil society organizations, such as AI Now, Algorithmic Justice League, and Data & Society, have proposed best practices. These mechanisms

---


for transparency, in tandem with data mapping and provenance requirements, are essential for meaningful enforcement.

**C. Data Mapping & Provenance Requirements**

In addition to ordering model deletion, regulators and legislators must also require some baseline data mapping and provenance requirements to facilitate the study, investigation, and enforcement of models.

Data mapping and provenance requirements are essential to making the threat of a deletion remedy real.\textsuperscript{87} As detailed further in Part V, enforcing the deletion remedy necessitates rules that map the lifecycle of data and track the relationships. To make sure the fruit of the poison tree can be identified as poison, we have to know what seeds it came from, what it has been mixed with, and any additives or GMOs that may have been added.

Companies are at different stages of data provenance, and there needs to be independent, government-funded entities that have the power to trace what is applicable to a deletion order and confirm that it has been deleted. Inadequate or irresponsible data provenance must not be a safe harbor. So, the FTC should carry this out through enforcement orders, Magnuson-Moss rulemaking, or rulemaking pursuant to implementing legislation like the American Data Privacy and Protection Act (ADPPA). California and Colorado, which have passed privacy laws that are currently being implemented through rulemaking, should also include these requirements into their rulemakings or in their enforcement mechanisms.

**D. Private Right of Action**

To fill in the gaps and empower, in particular, marginalized communities that may otherwise not be represented by state authorities, a private right of action in consumer protection or civil rights law is essential. When people are harmed in clear and recognizable ways through unlawful or discriminatory data collection or processing, any law addressing harmful AI or supplementing model deletion should include a private right of action.

**IV. CHALLENGES OF MODEL DELETION**

There is no panacea for algorithmic harm. Given the iterative nature of AI and automated decision-making systems,\textsuperscript{88} a solution

\textsuperscript{87} See generally Khan & Hanna, supra note 20.

\textsuperscript{88} See Li, supra note 6.
necessitates a series of logistical questions. If the remedy is to delete the fruit of the poison tree—any algorithm or model derived from ill-gotten data—how is the fruit defined? Interesting as an academic question but troubling as a logistical one. For example, if a defendant is working off pre-trained models provided by one of the Big Tech companies, how are the companies involved and how is it clear that the underlying model is not to blame? If the model is, should the different actors mentioned above investigate all companies using it? Would that be possible? As the AI Now Institute explains:

Currently only a handful of companies with incredibly vast resources are able to build [algorithmic models]. That’s why the majority of existing large-scale AI models have been almost exclusively developed by Big Tech, especially Google (Google Brain, Deepmind), Meta, and Microsoft (and its investee OpenAI). This includes many off-the-shelf, pretrained AI models that are offered as part of cloud AI services, a market already concentrated in Big Tech players, such as AWS (Amazon), Google Cloud (Alphabet), and Azure (Microsoft). Even if costs are lower or come down as these systems are deployed at scale (and this is a hotly contested claim), Big Tech is likely to retain a first mover advantage, having had the time and market experience needed to hone their underlying language models and to develop invaluable in-house expertise.89

In this Part, we break the discussion into three categories of challenges: the scope of the deletion order, the method by which the enforcer must require the violator to carry out the deletion, and how the enforcer can verify appropriate deletion. We use examples from the FTC, but the considerations persist for all enforcement bodies interested in levying deletion for meaningful equitable relief.

A. Scope

Past FTC settlements have used fairly broad language to order model deletion. For example, in Kurbo, the FTC settlement defined the “affected work product” as “any models or algorithms developed in whole or in part using Personal Information Collected from Children through the Kurbo Program.”90 In EverAlbum, “affected work product” was defined as “any models or algorithms developed


90 Kurbo Order, supra note 5, at 2.
in whole or in part using Biometric Information Respondent collected from Users of the ‘‘Ever’’ mobile application.”91 In Cambridge Analytica, the FTC ordered the company to:

Delete or destroy all Covered Information collected from consumers through GSRApp, and any information or work product, including any algorithms or equations, that originated, in whole or in part, from this Covered Information. Such deletion must occur within ten (10) days of the effective date of this Order, or if such information is in the possession of a government regulatory or law enforcement agency, including the United Kingdom’s Information Commissioner’s Office, as of the effective date of this Order, within ten (10) days after the Covered Information is returned to Respondent. Provided, however, that such Covered Information, or any information that originated in whole or in part from such Covered Information, need not be deleted or destroyed for so long as requested by a government agency or otherwise required by regulation, court order or other legal obligation; and C. Provide a written statement to the Commission, sworn under penalty of perjury, confirming the foregoing. This statement must be provided: (1) within thirty (30) days after the effective date of the Order; or, if applicable, (2) within thirty (30) days after the Covered Information is returned to Respondent from a government regulatory or law enforcement agency, or within thirty (30) days after any legal obligation to preserve the Covered Information has ended.92

In writing future orders, agencies must be more prescriptive and specific to address the challenges in enforcement in a way that addresses the layered and concentrated nature of AI power. The agencies must specify the specific algorithms or products they know to be affected to facilitate meaningful deletion. More resources, in terms of both money and staff, is essential to being able to do this correctly.

B. The Off-the-Shelf Problem

Many industry uses of AI are built off a few large models and data sets offered by the Big Tech Companies: Amazon (AWS, Rekognition), IBM (IADM diversity in Faces), Microsoft (Azure),

91 Everalbum Order, supra note 33, at 2.
92 Cambridge Analytica Order, supra note 32, at 4.
and Alphabet (Google Cloud). Some use these “off-the-shelf” products as is and integrate them into their workflow, but many build on top of the pre-trained models or algorithms.

In terms of model deletion, the “off-the-shelf” dynamic begs the following question: does every company that uses a “poisoned” data set, model, or algorithm have to change its product? Or would that leave the enforcement agency chasing all other purchasers of these products?

To help ameliorate the effects of this problem, “off-the-shelf” products of a certain size or market share should be subject to rigorous testing to obviate the responsibility of the wrongdoing. There will need to be careful investigation into the precise cause of the underlying harm, which will logically flow from the required data governance and provenance requirements that are sorely needed.93

The threat of deletion can and should be a stick for data provenance improvements at data-based companies of all levels. Still, identifying every data point that has gone into training, maintaining, or using a model/algorithm over several years is a daunting task. This difficulty cannot be an excuse though, and if a company is unable to undergo the task of mapping their data, that cannot insulate them from liability when those unmapped systems cause harm. Critically, some companies buy models pre-built from larger companies and may augment them, which may lead to under-inclusiveness in interpreting a deletion order—even in good faith.

Companies must also decide how broadly they will assert privileges such as trade secrets or other commercial protections that may hinder enforcement meaningfully carried out.

C. Retention

Deletion means deletion: gone forever and no longer usable. However, there are a myriad of reasons for why there should be both (1) a process similar to an escrow to separate tainted or unpoisoned data and preserve the companies’ other products and (2) a historical and public record of tainted data, models, and algorithms for educational, deterrence, and future investigation purposes.

Creating such a Hall of Retired Models Past94 for enforcement and research purposes can serve dual purposes of deleting the model and putting others on notice that this practice or data set or model or algorithm is off-limits. Federal agencies regularly publish guidance on the laws they enforce as well as their recent enforcement actions. So, while a model and its affected work product must be destroyed

---

93 See supra Part III.C.
94 Thank you in particular to workshop participants at WeRobot 2022 for this idea.
or deleted in practice, that should not deter law enforcement agencies from preserving relevant information about these systems to deter future misconduct. Further, companies themselves must also preserve their own records to disincentive reengagement with harmful AI practices. For example, as part of the Kurbo settlement order, the company was required to provide a written statement confirming deletion sworn under penalty of perjury and to keep records demonstrating compliance for ten years.

V. ENVISIONING MODEL DELETION: SPECULATIVE CASE STUDY

This Part describes one company—Clearview AI—whose practices cause clear algorithmic harm, and imagines how an equitable remedy like model deletion would apply. We conclude that if applied, the impact on Clearview AI would be massive in comparison to past FTC deletion orders, and the company likely would not be able to exist.

In early 2020, a New York Times investigation revealed that Clearview AI had quietly scraped data about millions of people, including biometric and other personal, sensitive information, to build one of the most powerful facial recognition systems. The company had covertly amassed more than three billion photos from the Internet—far more than the 411 million photos in the Federal Bureau of Investigation (FBI)’s own facial-recognition system. Further, in doing so, it did not disclose its activity or the purpose of the scraping, nor did it provide any opportunity for users to opt out of having their data processed for that purpose. Given such a vast database, several different actors have used Clearview AI’s product for their own ends. For example, political groups have used it for “extreme opposition research.” Corporations, such as Madison Square Garden and Macy’s, have also used the tool. And both local

99 See Ryan Mac, Caroline Haskins & Logan McDonald, Clearview’s Facial Recognition App Has Been Used by the Justice Department, ICE,
and national law enforcement agencies have used it to find real-time information about any individual.

Clearview AI’s practices are likely illegal. As Vermont’s Attorney General alleged in a March 2020 lawsuit against the company, the company violated Vermont’s unfair and deceptive trade practices law. More precisely, the complaint claimed that Clearview AI’s unfair practices included:

- Screen scraping billions of photographs without the consent of their owners, many of which had been uploaded subject to Terms of Service of websites which limited how they could be used;
- Collecting, storing, analyzing and distributing the photographs of minors without the consent of their parents or guardians;
- Invading the privacy of consumers;
- Failing to provide adequate data security for the data it has collected;
- Exposing consumers’ sensitive personal data to theft by foreign actors and criminals;
- Violating the civil rights of consumers by chilling their freedoms of assembly and political expression;
- Violating the rights of consumers as to the display and distribution of their photographs and other property rights; and
- Exposing citizens to the threat of surveillance, stalking, harassing, and fraud.

As for the deceptive practices, they consisted of:

- The ways that Vermont consumers can assert their privacy rights to opt out of its product;
- That Clearview’s processing of consumers’ personal data does not unduly affect their interests or fundamental rights and freedoms;
- The strength of its data security;
- That the product is only used by law enforcement agencies and is not publicly available;

---


101 Id. at 24.
That it removes consumers from its database to comply with relevant laws;

- The accuracy of its facial recognition matching product; and

- Its success in assisting law enforcement investigations.\(^\text{102}\)

Given the range of algorithmic harms listed above, Clearview AI is as good a case as any for model deletion. If applied, model deletion would demand destruction of its work product at a far larger scale than in the previous FTC orders. This is because of the relationship between the victim and the company. In *Kurbo*, the victims signed up or attempted to sign up for the service,\(^\text{103}\) and in *Cambridge Analytica*, although they did not know that Cambridge Analytica was harvesting personal information from Facebook, they did sign up and use Facebook’s services.\(^\text{104}\) In the case of Clearview AI, anyone can be a victim so long as they have any online presence.\(^\text{105}\) A staff photo for your job, a photo posted by your school celebrating your achievement, or a picture of attendees of a concert all can be fed to Clearview AI’s algorithm to enrich the company, assist law enforcement, and serve as a tool of mass surveillance.

However, if applied, the integrated nature and size of the facial recognition may make model deletion logistically difficult, and the different ways different clients of Clearview AI use the system could complicate enforcement actions. For example, the authority attempting to apply model deletion to Clearview AI’s algorithm will likely not able to isolate the affected work product to only certain photos and use cases. Further, how, both politically and legally, would the fact that police departments are many of the customers affect enforcement? When the product is sold to a variety of different entities, it is not only the company’s own tree that is poisoned, but also that of their client.

These considerations further support the dire importance of data mapping, provenance, separation, and documentation.\(^\text{106}\) They also emphasize the need for greater due diligence for companies purchasing tools. Such diligence may lead existing clients to simply not use Clearview AI’s tool—or facial recognition altogether—anymore. Strict and punitive enforcement would likely lead clients to consider their own roles and agreements when purchasing technology.

\(^{102}\) *Id.* at 25.


\(^{104}\) See Complaint ¶, *In re* Cambridge Analytica, LLC, No. 9383 (FTC July 24, 2019).

\(^{105}\) See Gershgorn, *supra* note 97.

\(^{106}\) See *supra* Part III.C.
CONCLUSION

In an increasingly data-driven world, model deletion can be an important legal remedy and potential legal right and requirement. In this Essay, we considered the legislative instantiation of model deletion within the domain of consumer protection law, where it has marked utility, and its application to other legal domains such as anti-discrimination law. At minimum, in order for tools like model deletion to remedy consumer harm and disincentivize needless data collection and abuse, jurisdictions must adopt laws, under which egregious violations can yield model deletion.

Model deletion serves as important AI governance enablers. Incentivizing dataset and model accountability across the AI and ML lifecycle is critical, and meaningful deletion substantially improves the value of the remedies. This needs to come in the form of greater diligence and care at the point of data collection, with a consistent focus on those implicated in datasets as well as comprehensive mapping of data flows and ML systems.

Model deletion levels the playing field for law enforcement. It helps to break the asymmetry of information and power between state and federal law enforcement agencies (i.e., state attorneys general, the FTC, etc.) and technology companies that develop and use AI and ML. It also allows for both quicker and more politically ironclad enforcement actions. As of now, beyond having to prove an unfair or deceptive trade practice, there needs to be decisions that a majority of the FTC at a given time agree with. With black and white violations, model deletion reduces political interference with consumer protection enforcement.

Critics consider model deletion to be a “blunt” tool, much like a hammer. And there is a kernel of truth to this contention. However, blunt should not be mistaken for haphazard nor misguided. Rather, blunt is a function of eviscerating structural incentives to collect and manipulate massive amounts of data with carefree abandon.\(^\text{107}\) It is blunt because it hurts, not like a hammer on the thumb, but like an overdue intervention with your loved ones. Accountability hurts, at first, but is necessary. So, yes, perhaps model deletion is blunt like a hammer, and, thankfully, U.S. federal consumer protection authorities are working to build a roof over our heads.

U.S. federal agencies, including the FTC, CFPB, DOJ, and EEOC, continue to align on not only the application and enforcement of existing law to AI and ML systems but also a broader strategy and commitment to enforce those laws. This Essay argued that model

\(^{107}\) As Samuel Levine underscores, model disgorgement is about changing incentives. See Levine Remarks, supra note 18.
deletion ought to be a part of the regulatory toolkit to achieve this mission and, more broadly, the regulatory imagination that seeks to eradicate AI and ML harms.