Washington Law Review

Volume 97 | Number 4

12-1-2022

Wrongful Improvers as a Guiding Principle for Application of the FTC's IP Deletion Requirement

Emma Elder
University of Washington School of Law

WRONGFUL IMPROVERS AS A GUIDING PRINCIPLE FOR APPLICATION OF THE FTC'S IP DELETION REQUIREMENT

Emma Elder*

Abstract: The 2021 Federal Trade Commission (FTC) investigation into cloud storage app developer Everalbum resulted in a consent decree that required Everalbum to delete not only unlawfully collected data, but also algorithms created using that data. The FTC had imposed this kind of penalty only once before. Questions remain about how the FTC will apply this so-called intellectual property (IP) deletion requirement in the future. This Comment argues that situations where companies develop intellectual property from misappropriated consumer data are analogous to cases where courts seek to apply the property law rule of the wrongful improver, i.e., where one party knowingly improves another's property. The rule requires that courts grant title to the owner of the original property regardless of how much the value of the property has increased. Applying the wrongful improver rule can guide the FTC's future application of the IP deletion requirement in two ways. First, application of the rule suggests that the IP deletion requirement should apply regardless of what type of data (biometric or non-biometric) has been misappropriated. Second, the rule indicates that a company must forfeit not only rights to their particular copy of their IP, but also all the IP rights that attach to it. Application of this rule will thereby strengthen the FTC's power to punish offenders and more significantly deter companies from unlawfully collecting consumer data.

INTRODUCTION

In the internet age, many companies depend largely on two assets: consumer data[1] and intellectual property.[2] In particular, companies' dependence on consumers' personal data—generally defined as any

* J.D. Candidate, University of Washington School of Law, Class of 2023. Thank you to Professor Ryan Calo for his thoughtful guidance and feedback on this piece. I also want to extend thanks to those on the *Washington Law Review* who helped get this piece into a finished state, especially Harrison Simons and Caroline Humphreys. Thank you to my partner, Oliver, and my family for their endless support.

1. Michelle Evans, *Why Data Is the Most Important Currency Used in Commerce Today*, FORBES (Mar. 12, 2018, 7:04 AM), https://www.forbes.com/sites/michelleevans1/2018/03/12/why-data-is-the-most-important-currency-used-in-commerce-today/?sh=42ce4e8254eb [https://perma.cc/AN4H-Z6P7].

2. Charles Lew, *In a Digital World, Your Most Valuable Property Is Intellectual*, FORBES (May 11, 2020, 7:15 AM), forbes.com/sites/forbesbusinesscouncil/2020/05/11/in-a-digital-world-your-most-valuable-property-is-intellectual/?sh=6013b1253d2c [https://perma.cc/8KCV-SYTM]; Bruce Berman, *$21 Trillion in US Intangible Assets Is 84% of S&P Value – IP Rights and Reputation Included*, IP CLOSEUP (June 4, 2019), https://ipcloseup.com/2019/06/04/21-trillion-in-u-s-intangible-asset-value-is-84-of-sp-500-value-ip-rights-and-reputation-included/ [https://perma.cc/276C-WPC3].

information reasonably related to an identifiable person,[3] from date of birth to shopping habits—has been at the center of years of privacy concerns and developing privacy regulation. Naturally, in most cases where U.S. privacy enforcement has found a privacy violation, a company must divest itself of such ill-gotten data and, consequently, the value tied to data as an asset. On the other hand, privacy enforcement has historically failed to punish privacy violators by targeting its other most important asset: intellectual property (IP).[4] But the Federal Trade Commission's use of a "radical"[5] new tool has shifted this landscape. In an action brought by the FTC in January 2021, the developer of now-defunct photo storage app, Ever, was forced to forfeit both consumer data and intellectual property created using that data.[6]

Launched by app developer Everalbum in 2015, Ever allowed users to upload photos and videos to its cloud servers, providing organizational features and freeing up storage space on users' devices.[7] In its lifetime, the app was downloaded onto the devices of twelve million consumers.[8] Then, in 2017, Everalbum began constructing facial recognition technology by leveraging the faces visible in the photos that its users had uploaded.[9]

The FTC brought its 2021 complaint against Everalbum under section 5(a) of the FTC Act.[10] Notably, the FTC's complaint was not directed at Everalbum's use of the photos for developing its facial recognition technology.[11] Rather, it sought to penalize Everalbum for failing to delete the photos of users who had deleted their accounts despite

---

3. Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Protecting Consumer Privacy in the Digital Age: Reaffirming the Role of Consumer Control, Keynote Address at the Technology Policy Institute Aspen Forum (Aug. 22, 2016), https://www.ftc.gov/system/files/documents/public_statements/980623/ramirez_-_protecting_consumer_privacy_in_digital_age_aspen_8-22-16.pdf [https://perma.cc/XQ6T-DDZU].

4. "Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names, and images used in commerce. IP is protected in law by, for example, patents, copyright and trademarks . . . ." *What Is Intellectual Property?*, WORLD INTELL. PROP. ORG., https://www.wipo.int/about-ip/en/ [https://perma.cc/Q6S5-2JSE].

5. Tiffany C. Li, *Algorithmic Destruction*, SMU L. REV. (forthcoming 2022) ("What made this enforcement action radical was the new remedy introduced by the FTC as part of the settlement order.").

6. Decision and Order, Everalbum, Inc., No. C-4743, at 5 (F.T.C. May 6, 2021).

7. Complaint at 1, Everalbum, Inc., No. C-4743 (F.T.C. May 6, 2021).

8. *Id.*

9. *Id.* at 2.

10. *Id.* at 7.

11. Christian Auty, Jason Haislmaier & Paul Sudentas, *FTC Says that One Cannot Retain the Fruit of the Tainted Tree*, JD SUPRA (Mar. 18, 2021), https://www.jdsupra.com/legalnews/ftc-says-that-one-cannot-retain-the-9020400/ [https://perma.cc/K7JFP3C3].

proclamations that it would do so, and for applying its facial recognition technology to photos of users who had ostensibly turned off the feature.[12] Nevertheless, as part of the ultimate consent decree against Everalbum, the FTC required Everalbum to not only delete the data it collected from non-consenting users, but also to delete the facial recognition technology.[13] Specifically, the consent decree ordered Everalbum to "delete or destroy" all facial recognition models or algorithms developed using improperly obtained photos.[14] The order represents only the second time the FTC has required deletion of work product derived from ill-gotten data.[15] Acknowledging the move, former FTC Commissioner Rohit Chopra called this "an important course correction."[16]

This IP deletion requirement likely holds significant business consequences for Everalbum.[17] Prior to the FTC investigation, Everalbum decided to shut down the Ever app and its consumer cloud storage services.[18] However, it had already begun marketing and selling the facial recognition technology to private companies, law enforcement, and the military under the name Paravision.[19] By the time it shuttered the

12. Complaint, *supra* note 7, at 6.

13. Decision and Order, Everalbum, Inc., No. C-4743, at 4–5 (F.T.C. May 6, 2021).

14. *Id.*

15. 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/FUR3-GBDH]. Some sources cite *Everalbum* as the first time the FTC has required deletion of algorithms derived from ill-gotten data. Auty et al., *supra* note 11; Jason D. Haislemaier & Paul B. Sudentas, *FTC Breaks New Ground on Retention of Intellectual Property and Data in Everalbum App Settlement*, WASH. LEGAL FOUND. (June 24, 2021), https://www.wlf.org/2021/06/24/publishing/ftc-breaks-new-ground-on-retention-of-intellectual-property-and-data-in-everalbum-app-settlement/ [https://perma.cc/QY4Z-MMGD]. However, the FTC appears to have done so once before in the case of *Cambridge Analytica, LLC*, No. 9383, at 4 (F.T.C. Nov. 25, 2019).

16. FED. TRADE COMM'N, STATEMENT OF COMMISSIONER ROHIT CHOPRA *IN THE MATTER OF EVERALBUM* AND *PARAVISION*, COMMISSION FILE NO. 1923172 1 (Jan. 8, 2021) [hereinafter STATEMENT OF ROHIT CHOPRA], https://www.ftc.gov/system/files/documents/public_statements/1585858/updated_final_chopra_statement_on_everalbum_for_circulation.pdf [https://perma.cc/9CV2-VJNL].

17. While this Comment primarily focuses on how the IP deletion requirement can deter companies that collect consumer data, see Li, *supra* note 5, for a discussion of how algorithmic disgorgement intrinsically provides better protection for consumers.

18. Sarah Perez, *Ever, Once Accused of Building Facial Recognition Tech Using Customer Data, Shuts Down Consumer App*, TECH CRUNCH (Aug. 24, 2020, 11:23 AM), https://techcrunch.com/2020/08/24/ever-once-accused-of-building-facial-recognition-tech-using-customer-data-shuts-down-consumer-app/ [https://perma.cc/4XGZ-MKER].

19. Olivia Solon & Cyrus Farivar, *Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools.*, NBC NEWS (May 9, 2019, 8:10 AM), https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371 [https://perma.cc/AH83-X4BC].

consumer app Ever, Paravision had raised $29 million in venture capital.[20] Had the FTC merely required that Everalbum delete its ill-gotten data, the effects on Everalbum would have likely been minimal, given that the company's business model had already shifted away from gathering and using such data. But by requiring that Everalbum delete the facial recognition technology developed using that data, the FTC's consent decree threatens Everalbum's business even in its more lucrative[21] reincarnation as Paravision.

These consequences foreshadow how future use of the IP deletion requirement could hit tech companies where it hurts. Intellectual property is typically a tech company's most valuable asset;[22] it is an important factor for securing venture capital funding,[23] and the sale or licensing of IP often comprises tech companies' core business models.[24] Algorithms like Everalbum's are one example of technology that can be protected as IP.[25] And the development, or "training," of algorithmic systems requires personal consumer data.[26] So, for the many companies that derive their value from algorithms—or any other technology that relies in large part on the collection of consumer data—the IP deletion requirement also represents a major tool for deterrence.[27] Currently, the FTC lacks the ability to impose financial penalties for first time offenders.[28] Requiring that companies forfeit IP created from unlawfully gathered data could significantly assuage this limitation.

Importantly, the FTC has a history of introducing new consent decree

---

20. Perez, *supra* note 18.

21. Solon & Farivar, *supra* note 19.

22. Forbes Technology Council, *10 Effective Ways for Tech Companies to Protect Their Intellectual Property*, FORBES (May 4, 2022, 1:15 PM), https://www.forbes.com/sites/forbestechcouncil/2022/05/04/10-effective-ways-for-tech-companies-to-protect-their-intellectual-property/?sh=378030441e3d [https://perma.cc/3K46-PFGA].

23. Mary Juetten, *Do Venture Capitalists Care About Intellectual Property?*, FORBES (Aug. 11, 2015, 10:23 AM), https://www.forbes.com/sites/maryjuetten/2015/08/11/do-venture-capitalists-care-about-intellectual-property/?sh=697b75d65b87 [https://perma.cc/GBH7-9E9V].

24. Simone Ferriani, Elizabeth Garnsey, Gianni Lorenzoni & Lorenzo Massa, *The Intellectual Property Business Model (IP-BM): Lessons from ARM Plc.* (Ctr. for Tech. Mgmt., Working Paper Series No. 2, 2015), https://www.ifm.eng.cam.ac.uk/uploads/Research/CTM/working_paper/2015-02-Ferriani-Garnsey-Lorenzoni-Massa.pdf [https://perma.cc/PH29-MZG9].

25. Meghan J. Ryan, *Secret Algorithms, IP Rights, and the Public Interest*, 21 NEV. L.J. 61, 66 (2020).

26. Einaras von Gravrock, *Why Artificial Intelligence Design Must Prioritize Data Privacy*, WORLD ECON. F. (Mar. 31, 2022), https://www.weforum.org/agenda/2022/03/designing-artificial-intelligence-for-privacy/ [https://perma.cc/5M6E-N39Q].

27. Auty et al., *supra* note 11.

28. STATEMENT OF ROHIT CHOPRA, *supra* note 16.

provisions that then become standard practice.[29] As a result, the FTC develops its doctrine much like any common-law regime, even though many cases never result in judicial decisions.[30] Indeed, the FTC has already demonstrated a nascent pattern of imposing the IP deletion requirement. In 2019, two years before *Everalbum*, the FTC required political consultancy Cambridge Analytica to delete the data it had deceptively gathered about Meta (formerly Facebook) as well as any algorithms built using that data.[31] And as recently as March 2022, the agency did so again against WW International, formerly known as Weight Watchers, ordering the company to delete any algorithms it built using information collected from users of its Kurbo healthy eating app for kids.[32] But the FTC's use of the IP deletion requirement is still young, and leaves unanswered important questions about its future applications. First, what is the requirement's precise effect on a target's IP rights? Does the deletion requirement actually destroy intellectual property rights, meaning that the violator gives up its right to enforce its exclusive rights against others? Or does it simply mean that the violator cannot retain copies of its own IP?[33] Second, will the FTC continue to impose the penalty only where the consumer information collected was biometric in nature? Such was the case in each of *Cambridge Analytica*,[34] *Everalbum*, and *Kurbo*.[35] Alternatively, will it expand the scope of the penalty and impose it even where the ill-gotten data is not biometric?[36]

If the FTC were to answer these questions in the affirmative, it would broaden the already formidable deterrent posed by the IP deletion requirement and provide even stronger protection for consumers. This Comment discusses how these questions can be answered to provide outcomes that maximize consumer welfare. Specifically, this Comment

---

29. *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

30. *Id.*

31. Final Order, Cambridge Analytica, LLC, No. 9383, at 3–4 (F.T.C. Nov. 25, 2019).

32. United States v. Kurbo Inc., No. 22-cv-00946, at 8 (N.D. Cal. 2022) (stipulated order for permanent injunction, civil penalty judgment, and other relief).

33. Auty et al., *supra* note 11.

34. Avery Hartmans, *It's Impossible to Know Exactly What Data Cambridge Analytica Scraped from Facebook—But Here's the Kind of Information Apps Could Access in 2014*, BUS. INSIDER (Mar. 22, 2018, 11:19 AM), https://www.businessinsider.com/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3 [https://perma.cc/6NVX-7QQD] (noting that although it is unclear what information Cambridge Analytica collected from users, they likely had access to Facebook users' photos, which comprise biometric information).

35. Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 11, United States v. Kurbo, Inc., No. 22-CV-946 (N.D. Cal. Feb. 16, 2022) (noting that defendant Kurbo collected user information such as height, weight, food intake, and activity levels).

36. Auty et al., *supra* note 11.

analogizes to the wrongful improver rule in accession law, by which parties who create something new through willful incorporation of the property of another are not entitled to the improved property, nor to compensation for their labor.[37] Rather, the owner of the original, unimproved property is entitled to the improved property.[38] Principles underlying this doctrine not only lend support to the FTC's existing use of the IP deletion requirement but also demonstrate why the IP deletion requirement should (1) lead to actual destruction of IP rights (not just deletion); and (2) should be applied even in cases of non-biometric data.

Part I of this Comment provides an overview of the FTC's role as the United States' de facto privacy enforcer, and the importance of the *Everalbum* case in this context. Part II then describes the wrongful improver concept and the interests it protects. Finally, Part III demonstrates how the FTC's IP deletion requirement reflects the model of the wrongful improver, lending support to its continued use in *Everalbum*-like cases. Part III further argues that applying the wrongful improver rule to cases of data misappropriation not only answers the remaining questions around how to apply the requirement but also does so in a way that spells better protection for consumers. Part III also discusses potential limitations of applying this rule, and finally identifies potential bad actors who may be most affected by it.

I. DATA PRIVACY AND THE *EVERALBUM* CASE

This Part details the role of the Federal Trade Commission in privacy enforcement in the United States. Then, this Part explains the process of an FTC investigation, and why most FTC actions conclude in a consent decree. Finally, this Part examines the FTC's recent investigation and settlement against Everalbum, Inc. As one of the first three cases in which the FTC required deletion of intellectual property as part of a settlement, *Everalbum* serves as a touchpoint for questions regarding how the FTC will apply this requirement in the future.

A. The FTC's Role as De Facto Privacy Enforcer

While the United States lacks a comprehensive federal privacy statute, there is at least one broadly applicable federal statute that can be used to enforce privacy principles: the Federal Trade Commission Act.[39] Prior to the rise of the internet, section 5 of the FTC Act was used primarily to

37. Note, *Accession on the Frontiers of Property*, 133 HARV. L. REV. 2381, 2383 (2020).

38. *Id.*

39. Federal Trade Commission Act, 15 U.S.C. § 45.

punish businesses for false advertising and dangerous products.[40] However, the FTC began regulating consumer privacy issues in the mid-1990s at the urging of Congress, amidst the rapid growth of the internet.[41] The FTC entered this new role with the goal of enforcing self-regulation—that is, enforcing the rules that companies implemented themselves—instead of making its own rules.[42] This policy reflected a fear that regulation would inhibit the growth of online activity.[43] It also reflected industry players' natural preference for self-regulation[44] and the accompanying self-regulatory regimes that private organizations established throughout the 1990s, such as TRUSTe, a group that issued privacy "seals" to certify that a partnered site conformed to basic privacy standards.[45] In particular, the rise in privacy policies, both voluntarily implemented by website owners and encouraged by organizations like TRUSTe, gave the FTC a hook by which it could readily utilize its section 5 power.

Section 5 of the FTC Act prohibits "unfair or deceptive acts and practices."[46] The FTC finds a practice to be "deceptive" where there is a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[47] An "unfair" practice, on the other hand, is one that causes substantial injury that is not outweighed by any countervailing benefits to consumers or competition, and it must be an injury that consumers themselves could not reasonably have avoided.[48] In this way section 5 gives the FTC the power to enforce companies' privacy policies under both definitions. Of the two powers, "deception" provides a more straightforward path[49] to enforcement: there is liability where a website inadvertently or negligently fails to comply with its privacy policy, and

40. Solove & Hartzog, *supra* note 29, at 598.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.* at 592.

45. *Id.* at 593.

46. Federal Trade Commission Act, 15 U.S.C. § 45.

47. Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Com. (Oct. 14, 1983) (appended to Cliffdale Assoc. Inc., 103 F.T.C. 110, 174 (1984)).

48. Letter from Wendell H. Ford, Chairman, Fed. Trade Comm'n, to Hon. John C. Danforth, Ranking Minority Member, House Comm. on Com., Sci., & Transp. (Dec. 17, 1980) (appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984)).

49. G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMMS. & TECH. L. REV. 163, 171 (2012).

thereby misrepresents its practices to consumers.[50] Perhaps because of the clarity of this rule, the FTC began its practice of policing privacy policies through its "deception" power.[51] Yet, by requiring a company to fail to comply with its privacy policy, "deception" requires a "'gotcha' moment" that limits this rule's applicability.[52] In contrast, although the FTC's "unfairness" power is relatively less clear, it is more widely applicable in that it can proactively evaluate privacy policies without waiting for website operators to make a mistake.[53] Examples of violations that fall under one or both of these umbrellas include failing to encrypt consumer credit card information, selling email lists when a company claimed not to, or having a weak password policy that exposes consumer data to hackers.[54]

Through its focus on unfair and deceptive practices, section 5 gives the FTC the power to bring privacy cases even in the sectors left unregulated by the United States' patchwork of statutory law.[55] And there are a significant number of companies that fall outside such statutes. As a result, the FTC not only has vast jurisdiction for privacy matters,[56] but it is the sole method of privacy regulation in certain sectors.[57] For these reasons, many view the FTC as the de facto privacy enforcer in the United States.[58]

Notably, in order to hold an organization liable under section 5 of the FTC Act, the FTC does not need to demonstrate intent.[59] Still, the federal circuit courts allow the FTC to find individuals personally liable for their actions as a member of a target organization.[60] In such cases, the FTC

---

50. *Id.* at 171–72.

51. Solove & Hartzog, *supra* note 29, at 599.

52. Hans, *supra* note 49, at 173.

53. *Id.*

54. Jon L. Mills & Pedro M. Allende, *FTC Consent Decrees Are Best Guide to Cybersecurity Policies*, DAILY BUS. REV. (Sept. 21, 2015, 11:00 AM), https://www.law.com/dailybusinessreview/almID/1202737711574/?slreturn=20220408151843#ixzz3niw5jHOf (last visited Nov. 3, 2022).

55. Solove & Hartzog, *supra* note 29, at 588.

56. *Id.* ("The FTC reigns over more territory than any other agency that deals with privacy.").

57. The United States' sectoral approach to privacy law means that while many businesses fall squarely within an industry-specific privacy statute, many fall outside the scope of any specific privacy statute. In such cases, the FTC Act is the only relevant privacy law. *Id.*

58. *Id.* at 600.

59. *See, e.g.*, FTC v. Bay Area Bus. Council, Inc., 423 F.3d 627, 635 (7th Cir. 2005) ("The FTC is not, however, required to prove intent to deceive.").

60. *See, e.g.*, POM Wonderful, LLC v. FTC, 777 F.3d 478, 498–99 (D.C. Cir. 2015) (affirming decision to hold CEO of defendant company individually liable); FTC v. E.M.A. Nationwide, Inc., 767 F.3d 611, 636 (6th Cir. 2014) (affirming decision to hold corporation's founders individually

must show that the defendant knew or should have known of the deceptive conduct, and participated in or had authority to control the conduct.[61] The decision by the Court of Appeals for the Fourth Circuit in *Federal Trade Commission v. Ross*[62] demonstrates this rule. In that case, Innovative Marketing, Inc. (IMI) created ads encouraging consumers to conduct a computer scan to detect malicious viruses and spyware.[63] If consumers opted into the "scan," the ad would inevitably indicate the presence of viruses.[64] However, both the scan and detected viruses were bogus.[65] Users were then directed to buy IMI's software to ostensibly fix the situation.[66] In this case, the Vice President, Kristy Ross, was held personally liable because she (1) was recklessly indifferent to the deceptive advertising practices; and (2) had adequate control, given that she oversaw the design and approval of the advertisements.[67] Of course, requiring knowledge or constructive knowledge for personal liability under the FTC Act means the standard of proof in these cases is higher than in organizational liability cases, where no intent is required. Nevertheless, commentators suggest that the FTC would face little difficulty in meeting this standard and imposing personal liability on the CEOs of big tech companies like Meta and Google.[68] Such companies continue to be founder-controlled in a concrete sense, and there is evidence to suggest that the founders do not prioritize users' privacy interests.[69] For example, the FTC has uncovered emails from executives in which they discuss the predatory nature of information gathering.[70] As a result, such executives may demonstrate the reckless indifference and control necessary to be held personally liable under the FTC Act.

---

liable); FTC v. IAB Mktg. Assocs., LP, 746 F.3d 1228, 1233 (11th Cir. 2014) ("Individuals may be liable for FTC Act violations committed by a corporate entity."); FTC v. Ross, 743 F.3d 886, 892 (4th Cir. 2014) (holding company's Vice President personally liable for actions of the company).

61. *Ross*, 743 F.3d at 892.

62. 897 F.3d 886 (D. Md. 2012).

63. *Ross*, 743 F.3d at 890.

64. FTC v. Ross, 897 F. Supp. 2d 369, 378–79 (D. Md. 2012).

65. *Id.*

66. *Id.*

67. *Ross*, 743 F.3d at 894–95.

68. Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, But Not Without Help from Congress*, BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/6L24-QRLR].

69. *Id.*

70. *Id.*

B. The Lifecycle of an FTC Action

Any FTC enforcement action is necessarily preceded by an investigation into that company's practices. Such investigations are permitted under section 3 of the FTC Act, which authorizes the FTC to "gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce, excepting banks."[71] The preliminary stage of an investigation is typically informal; the FTC begins by reviewing publicly available information and reaches out to the company asking for voluntary cooperation.[72] This preliminary stage may begin in response to complaints from consumers or competitors, at the request of another agency, or of the FTC's own accord.[73] In most cases, the FTC decides to pursue a formal investigation, rather than drop the case, because it typically uncovers concerning information during the informal stage.[74]

In formal investigations, the FTC is permitted to issue subpoenas for oral testimony and written documents.[75] It may also issue civil investigative demands (CIDs) for these purposes, as well as require that the recipient "file written reports or answers to questions."[76] Further, the FTC may demand an entity file "annual or special . . . reports or answers in writing to specific questions" under what is known as a 6(b) order.[77] In some cases, the FTC will also request information from third parties such as the target company's banks, competitors, or customers.[78] Using these investigational powers, the FTC may require that the entity provide documents such as training materials, risk assessments, and information

71. Federal Trade Commission Act, 15 U.S.C. § 46(a).

72. David B. McConnell & Joseph G. Talbot, *FTC Investigations: What to Expect When the FTC Comes Calling*, PERKINS THOMPSON (July 27, 2015), https://www.perkinsthompson.com/ftc-investigations/#:~:text=If%20the%20FTC%20launches%20a,security%20plan%20and%20privacy%20policies [https://perma.cc/DT7M-S4T9]; Nick Oberheiden, *What to Do When the FTC Investigation Comes Knocking*, NAT'L L. REV. (Feb. 23, 2021), https://www.natlawreview.com/article/what-to-do-when-ftc-investigation-comes-knocking [https://perma.cc/795H-ZYMG].

73. McConnell & Talbot, *supra* note 72.

74. Oberheiden, *supra* note 72.

75. *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (May 2021) [hereinafter *A Brief Overview of the FTC Authority*], https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/J6TE-CN8U].

76. Federal Trade Commission Act, 15 U.S.C. § 57b-1(c)(1).

77. *Id.* § 46(b).

78. Oberheiden, *supra* note 72.

about the company's security and privacy plans.[79] Thus, the investigative powers of the FTC allow it to demand an extraordinary amount of information from target entities,[80] and opportunities to challenge such investigative demands are limited.[81] And while pre-complaint investigations are generally not public,[82] the targets of an investigation are not entitled to know the nature of the investigation.[83]

At the end of the investigation, the FTC will decide whether to pursue a formal enforcement action. If it does, the FTC usually sends the target company a written notification along with a draft complaint and a proposed settlement agreement, called a consent order.[84] The FTC can then decide to file the complaint as an administrative proceeding or in federal district court. [85] Administrative complaints are heard by an administrative law judge and proceed similarly to a federal court trial.[86] These cases are first appealable to the FTC Commission, and subsequently to a U.S. court of appeals.[87] However, most actions brought by the FTC result in consent decrees rather than judicial decisions.[88]

Certain stipulations regularly appear in such consent decrees.[89] For example, they usually impose a twenty-year period of FTC oversight, require companies to implement privacy and security programs, and perform regular independent assessments of the company's data practices.[90] Of course, consent decrees do not provide as much insight into the FTC Act's section 5 power as judicial opinions would.[91] Nevertheless, the FTC's pattern of enforcement has amounted to what may be

79. McConnell & Talbot, *supra* note 72.

80. Oberheiden, *supra* note 72.

81. *Id.*

82. *A Brief Overview of the FTC Authority*, *supra* note 75.

83. Oberheiden, *supra* note 72.

84. Christie Grymes Thompson & Jessica Rich, *FTC Consumer Protection Investigations and Enforcement*, THOMSON REUTERS PRAC. L., https://1.next.westlaw.com/Document/I5f7b89a7bc3f11e398db8b09b4f043e0/View/FullText.html?transitionType=SearchItem&contextData=(sc.Search) (last visited Feb. 10, 2022).

85. McConnell & Talbot, *supra* note 72.

86. *The Enforcers*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/enforcers [https://perma.cc/X7GC-VCF9].

87. *Id.*

88. Solove & Hartzog, *supra* note 29, at 585.

89. Joseph Jerome, *Can FTC Consent Orders Effectively Police Privacy?*, IAPP (Nov. 27, 2018), https://iapp.org/news/a/can-ftc-consent-orders-police-privacy/ [https://perma.cc/BD37-RN6N].

90. *Id.*

91. Jan M. Rybnicek & Joshua D. Wright, *Defining Section 5 of the FTC Act: The Failure of the Common Law Method and the Case for Normal Agency Guidelines*, 21 GEO. MASON L. REV. 1287, 1305 (2014).

considered a quasi-common law jurisprudence.[92] As a result, FTC actions and consent orders provide a critical roadmap for the types of conduct the FTC will seek to redress, and thereby informs the standard of acceptable privacy practices.[93] Indeed, the Court of Appeals for the Third Circuit in *FTC v. Wyndham Worldwide Corp.*[94] found that prior consent decrees offered fair notice about the type of practices and conduct that the FTC deems to be unfair or deceptive.[95] Accordingly, many companies use FTC actions and consent orders to inform their decisions regarding privacy practices.[96]

The common law-like development of FTC jurisprudence is demonstrated by the FTC's pattern of introducing a new stipulation in one case which it then continues to require in the consent orders of subsequent cases.[97] For example, in *In re Microsoft*[98] in 2001, the FTC found that Microsoft had been making overbroad claims about the privacy and security of information it collected in connection with its "Passport" web services.[99] As part of the consent order, the FTC required that Microsoft institute a "comprehensive information security program."[100] Among other things, such a program would need to include the designation of an employee to coordinate the program; a risk assessment protocol; and the implementation of reasonable security safeguards.[101] At the time, this was an unprecedented demand of an FTC consent order. Today, it is commonplace in FTC privacy actions.[102]

Through its common law-like framework, the FTC has been able to increase its power as a privacy enforcer slowly but significantly.[103] Considering the current state of privacy law, the FTC's ability to expand protection for consumer privacy in this way is crucial. Many companies fall outside the scope of sector-specific statutory law such that, in many cases, the FTC's section 5 power is the only mode of enforcement.[104] And

92. *See* Solove & Hartzog, *supra* note 29.

93. Mills & Allende, *supra* note 54.

94. 799 F.3d 236 (3d Cir. 2015).

95. *Id.* at 257.

96. *See* Solove & Hartzog, *supra* note 29.

97. *Id.*

98. Decision and Order, Microsoft Corp., No. 012-3240, at 4 (F.T.C. Dec. 24, 2002).

99. Complaint at 2–5, Microsoft Corp., No. 012-3240 (F.T.C. Dec. 24, 2002).

100. *Microsoft Corp.*, No. 012-3240, at 4.

101. *Id.*

102. *See generally* Decision and Order, Facebook, Inc., No. C-4365, at 5 (F.T.C. July 27, 2012); Decision and Order, Google, Inc., No. C-4336, at 4 (F.T.C. Oct. 13, 2011).

103. Solove & Hartzog, *supra* note 29, at 606.

104. *Id.* at 588.

though the FTC's jurisprudence develops slowly (as with any common law regime), Congress' efforts at enacting a comprehensive privacy bill are moving perhaps even more slowly,[105] an important consideration given that the risk of privacy violations seems to grow exponentially by the day.

However, the FTC's ability to punish offenders is limited in a significant way: the FTC lacks the general authority to issue civil penalties.[106] It is limited to fining companies who have violated a consent decree.[107] And even when the FTC does impose penalties, the amount must reflect the amount of consumer cost, which is often a mere drop in the bucket for large tech companies.[108] Of course, other factors may deter companies from committing privacy violations. Bad press is one such example, although reputational damage is often mitigated by the fact that the general public does not keep up with FTC privacy actions.[109] A greater disincentive is likely the possibility of FTC audits, a process which requires regular assessments detailing the agreed-upon safeguards and a certification of the effectiveness of the company's protections by a qualified, independent third party, among other things.[110] Exhaustive and demanding, the auditing process lasts for twenty years in most cases.[111] Nevertheless, the persistence of privacy violations suggests that the FTC's power of deterrence is still significantly limited.

C. The Everalbum *Case*

Despite the FTC's inability to issue financial penalties against first time offenders, the agency has recently indicated that it may begin imposing an even more powerful requirement: that companies who use data in violation of section 5 to develop algorithms or models must delete that intellectual property.[112] As one of three cases in which the FTC has imposed this penalty, *In re Everalbum, Inc.* serves as a touchpoint for discussion.

The FTC brought the action against app developer Everalbum for data

---

105. 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/ (last visited Nov. 2, 2022).

106. STATEMENT OF ROHIT CHOPRA, *supra* note 16.

107. Solove & Hartzog, *supra* note 29, at 605.

108. *Id.* at 605.

109. *Id.* at 606.

110. *Id.*

111. *Id.*

112. Auty et al., *supra* note 11.

collection and use practices of its photo and storage app, Ever.[113] The company made Ever available both for iOS and Android, and garnered approximately twelve million consumers.[114] The first count in the complaint was directed to Ever's misrepresentation of users' ability to control when facial recognition was used on their photos.[115] In 2017, Everalbum implemented a "Friends" feature on the app which utilized face recognition to group users' photos by the faces of the people who appear in the photos, allowing the user to easily apply tags to the photos.[116] Initially, this feature was automatically turned on for all Ever uses.[117] But in May 2018, Everalbum introduced a pop-up message to users located in Texas, Illinois, Washington, and the EU, whereby they could deactivate the feature.[118] Accordingly, Everalbum turned off the feature as those users indicated.[119] Beginning in July 2018, Ever had posted in the "Help" section of its website, everalbum.com, that all users could enable or disable facial recognition.[120] But it did not roll out the ability to disable facial recognition for users outside of Texas, Illinois, Washington, and the EU until April 2019.[121] As a result, for users outside of those jurisdictions, this message was false and misleading until April 2019.[122]

The second count of the FTC's complaint alleged that Ever had misrepresented that users' photos would be deleted upon deactivation of their accounts.[123] On multiple occasions, Everalbum had conveyed that account deactivation would lead to permanent deletion of all photos and videos stored on a user's account. [124] Contrary to these statements, Everalbum did not delete the photos associated with deactivated accounts until at least October 2019.[125]

In addition to operating the app for consumer use, Everalbum used photos uploaded by its users in conjunction with publicly available databases to develop a facial recognition algorithm, as well as data sets

113. Complaint at 1, Everalbum, Inc., No. C-4743 (F.T.C. May 6, 2021).
114. *Id.*
115. *Id.* at 6.
116. *Id.* at 2.
117. *Id.*
118. *Id.*
119. *Id.*
120. *Id.* at 3.
121. *Id.* at 2.
122. *Id.*
123. *Id.* at 6.
124. *Id.* at 5.
125. *Id.* at 6.

used for training that algorithm.[126] Everalbum then used the facial recognition technology to build the facial recognition services offered by its enterprise brand, Paravision.[127] Notably, the complaint did not include a specific count regarding Everalbum's development of the facial recognition technology, but merely included a description of that process.[128]

The FTC was able to reach a settlement with Everalbum in May of 2021.[129] The consent order included provisions that expressly addressed the counts of its complaint: a requirement to obtain consumers' express consent before using facial recognition technology on their files and photos, and a requirement to delete the photos and videos of users who had deactivated their accounts.[130] Relatedly, it also required that Everalbum obtain express consent from users before using biometric information collected from them.[131] But the consent order also included a provision that had been used only once before.[132] This provision required Everalbum to delete all the models, datasets, and algorithms that it made using data collected from its users.[133] *Everalbum* thus represents one of the first times the FTC required deletion of IP as part of a consent order.[134]

Given the common law-like nature of FTC actions, it seems likely that the FTC will at least continue to require the deletion of algorithms, if not other types of intellectual property, in future cases.[135] After *Everalbum*, FTC Commissioner Rebecca Kelly Slaughter commended the "innovative disgorgement remedy," saying "we should require violators to disgorge

126. *Id.* at 3.

127. *Id.* at 4. In 2019, Everalbum rebranded itself as Paravision. Perez, *supra* note 18. Its website describes the service it offers as "a comprehensive, industry-leading face recognition product suite [that] offers all of the development tools necessary to build and deploy mission critical biometric verification and identification solutions across a wide range of applications and use cases." *A Higher Standard for Face Recognition*, PARAVISION, https://www.paravision.ai/product/face-recognition/ [https://perma.cc/4D33-HSUU].

128. Complaint at 3–6, Everalbum, Inc., No. C-4743 (F.T.C. May 6, 2021).

129. *FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology*, FED. TRADE COMM'N (May 7, 2021), https://www.ftc.gov/news-events/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse [https://perma.cc/WCY7-77GC].

130. Decision and Order, Everalbum, Inc., No. C-4743, at 5 (F.T.C. May 6, 2021).

131. *Id.*

132. Kaye, *supra* note 15.

133. *Everalbum*, *Inc.*, No. C-4743, at 5.

134. Although some sources report *Everalbum* as the first time the FTC has ordered deletion of work product, see Auty et al., *supra* note 11.

135. So far, the FTC has only applied the provision to require destruction of algorithms created from ill-gotten data. Li, *supra* note 5 (noting that the FTC has required disgorgement in only three cases: *Cambridge Analytica*, *Everalbum*, and *Kurbo*).

not only the ill-gotten data, but also the benefits—here, the algorithms—generated from that data."[136] And the FTC imposed what some call "algorithmic destruction"[137] again in March 2022, against the developer of children's weight loss app Kurbo and its parent company WW International (formerly Weight Watchers).[138] Indeed, as former FTC Commissioner Rohit Chopra noted in his statement after issuing the *Everalbum* complaint, the proposed order required Everalbum to "forfeit the fruits of its deception."[139] Such a broad characterization may indicate broad use in the future: as long as a company deceptively or unfairly acquires data in some way, the FTC could require IP created using that data to be forfeited, even if it was created otherwise lawfully.

D. Possible Paths and Implications of Future Applications of the IP Deletion Requirement

Just how broadly the FTC chooses to apply the IP deletion requirement will determine the level to which companies are deterred. Intellectual property is among the most valuable assets of many technology companies.[140] A startup's ability to secure venture capital funding may in large part depend on its ability to get protection for its IP.[141] And tech companies may base their entire business model on their ability to license their IP.[142] Algorithms like Everalbum's are a particularly popular focus of IP protection in the technology sector.[143] But algorithms and artificial intelligence develop by being trained on personal data.[144] Likely, this incentivizes companies developing algorithms to gather consumer data, even if doing so is unlawful.

Given the importance of IP in the tech sector, the FTC's decision to apply the IP deletion requirement liberally would broadly deter unlawful collection of consumer data, encouraging companies to follow both

136. Rebecca Kelly Slaughter, Acting Chairwoman, Fed. Trade Comm'n, Protecting Consumer Privacy in a Time of Crisis, Remarks at the Future of Privacy Forum (Feb. 10, 2021), https://www.ftc.gov/system/files/documents/public_statements/1587283/fpf_opening_remarks_210_.pdf [https://perma.cc/3JFC-BHWN]. The FTC actually imposed this requirement initially in *Cambridge Analytica* in 2018. *See* Final Order, Cambridge Analytica, LLC, No. 9383, at 4 (F.T.C. Dec. 6, 2019).

137. Li, *supra* note 5; Kaye, *supra* note 15.

138. United States v. Kurbo Inc., No. 22-cv-00946, at 8 (N.D. Cal. 2022) (stipulated order for permanent injunction, civil penalty judgment, and other relief).

139. STATEMENT OF ROHIT CHOPRA, *supra* note 16.

140. Lew, *supra* note 2.

141. Juetten, *supra* note 23.

142. Ferriani et al., *supra* 24.

143. Ryan, *supra* note 25, at 66.

144. von Gravrock, *supra* note 26.

sector-specific privacy statutes and their own privacy policies.[145] Indeed, a broad application may more than compensate for the fact that the FTC cannot issue financial penalties upon first-time violations.[146] As former Commissioner Chopra noted in his statement following *Everalbum*, the FTC had previously allowed companies to retain IP created using ill-gotten data.[147] Specifically, in a 2019 settlement with YouTube and Google, the FTC imposed a financial penalty against the companies for illegally gathering data from children; yet, since the defendants were not required to delete the algorithms that the companies created with that data, the companies were nevertheless able to profit off of the illegally obtained data.[148] Such a result suggests that the IP deletion requirement poses an even more robust deterrent for tech companies than financial penalties. To many consumer advocates, such a strong disincentive would be very welcome, especially considering the backdrop of the United States' patchwork federal privacy regime.[149]

But important questions remain. Perhaps the easiest question to answer is, will the FTC continue to use this mechanism in the future? Given the FTC's pattern of quasi-common law jurisprudence,[150] its now three-case history of imposing the penalty,[151] and the FTC's increasingly tough stance on Big Tech,[152] the answer seems to be yes. But questions about how and when the provision will be applied are tougher to answer.

For example, commentators wonder whether the FTC will apply the IP deletion requirement in cases where the ill-gotten data was not biometric

145. Auty et al., *supra* note 11.

146. STATEMENT OF ROHIT CHOPRA, *supra* note 14.

147. *Id.*

148. *Id.*

149. Kim Hart, *Americans Don't Trust Tech Companies on Data Privacy*, AXIOS (Apr. 23, 2018), https://www.axios.com/distrust-social-media-firms-to-protect-privacy-survey-8b95db51-f137-46e3-a239-a5f304f0ac1b.html [https://perma.cc/Z2M8-CJ2W].

150. *See* Microsoft Corp., No. C-4069, at 2–3 (F.T.C. Dec. 24, 2002) (ordering the creation of comprehensive privacy programs for the first time); Sears Holding Corp., F.T.C. No. C-4264, at 5 (Aug. 31, 2009) (requiring the deletion of ill-gotten data for the first time).

151. Li, *supra* note 5, at 19 ("One is an example, two is a coincidence, three is a trend. . . . This lasting trend, backed by statements from FTC Commissioners, shows what is likely becoming a new push from the FTC to establish algorithmic disgorgement as a routine privacy remedy.").

152. FED. TRADE COMM'N, STATEMENT OF CHAIR LINA M. KHAN REGARDING THE REPORT TO CONGRESS ON PRIVACY AND SECURITY (Oct. 1, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf [https://perma.cc/2NZ5-6T35].

in nature.[153] Though privacy statutes vary somewhat in their definitions,[154] biometric data is generally understood as information that stems from measurements of human physiology such as fingerprints, retinal scans, facial features, voice patterns, and DNA scans.[155] Biometric data is also understood to include behavioral data, which is a broad category that includes information about someone's habits, actions, or personality.[156] Given the highly personalized nature of biometric data, it poses privacy risks that other types of information do not. For example, where biometric data is used for the purpose of identification, disclosure of biometric data may pose serious risks of identity theft, considering that an individual cannot change their biometric information the way they could change a password.[157] Further, advances in medical technologies may also enable the use of biometric data to draw conclusions about the health of a person.[158] As a result, biometric information is typically considered a more sensitive category of data, and subject to greater protection under Europe's General Data Protection Act[159] and the California Consumer Privacy Act,[160] which are among the toughest privacy laws in the world.[161] Nevertheless, biometrics are increasingly used for authentication, with the global biometric authentication market expected to reach $44.1 billion by 2026.[162] Given that biometric data is more sensitive—and potentially more valuable—than other types of data, commentators wonder whether

153. Auty et al., *supra* note 11.

154. Bryan Cave Leighton Paisner, *Is the CCPA's Definition of "Biometric Information" Broader than the Definition Used by Other States?*, JD SUPRA (Apr. 13, 2020), https://www.jdsupra.com/legalnews/is-the-ccpa-s-definition-of-biometric-64996/ [https://perma.cc/3599-VTU3].

155. Jonathan Herpy, *Staying in Compliance with Biometric Privacy Laws as a Business*, FORBES (Apr. 5, 2021, 9:00 AM), https://www.forbes.com/sites/forbesbusinesscouncil/2021/04/05/staying-in-compliance-with-biometric-privacy-laws-as-a-business/?sh=26b4ad373123 [https://perma.cc/6SBF-9CS2].

156. Danny Ross, *Processing Biometric Data? Be Careful, Under the GDPR*, IAPP (Oct. 31, 2017), https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/ [https://perma.cc/NFE2-3F4B].

157. Jorden Bailey & Matthijs van Bergen, *Using Biometric Data? Sensitive Under the GDPR!*, LEGAL ICT (Oct. 18, 2017), https://www.ictrecht.nl/en/blog/using-biometric-data-sensitive-under-the-gdpr [https://perma.cc/6F26-2WPB].

158. *Id.*

159. General Data Protection Regulation, art. 9, 2016 O.J. (L 679).

160. California Consumer Privacy Act, CAL. CIV. CODE § 1798.140.

161. Robert Bateman, *How the CCPA Is Different from the GDPR*, TERMSFEED (July 1, 2022), https://www.termsfeed.com/blog/ccpa-different-gdpr/ [https://perma.cc/63UR-VALS].

162. Glob. Indus. Analysts, Inc., *Global Biometrics Market to Reach $44.1 Billion by 2026*, PR NEWSWIRE (July 13, 2021, 11:00 AM), https://www.prnewswire.com/news-releases/global-biometrics-market-to-reach-44-1-billion-by-2026—301331369.html [https://perma.cc/CL5R-R5V4].

the FTC will reserve the IP deletion requirement for cases where biometric data has been misappropriated because these cases are more egregious.[163] Alternatively, the FTC could choose to apply the provision regardless of the type of data misappropriated. How the FTC chooses to proceed on this question will no doubt determine the extent to which the IP deletion requirement acts as a deterrent against privacy violations for data-hungry businesses.

It is also unclear specifically how the IP deletion requirement will affect the IP rights of a company like Everalbum. The consent decree in *Everalbum* required the company to "delete or destroy" the work product created using the misappropriated data.[164] Similar language was used in the *Cambridge Analytica* and *Kurbo* orders.[165] But it is unclear which rights are implicated in a "delete or destroy" mandate. Having trade secret protection in an algorithm or piece of software, could a company still exercise rights to that technology even after deleting its own copies? Under the view that trade secret law includes at least the rights to use one's protected information, transfer or make exclusive grants of that information, and recover damages for harm caused by illicit use or disclosure of that information,[166] a narrow construction of the IP deletion requirement would only impact a company's rights to use. *Everalbum* illustrates the business implications of this distinction. If its trade secret protection remains intact after destroying its algorithms, Everalbum could presumably retain the right to transfer and thus could continue to earn profits on licenses to the algorithms that it granted before deletion. Similarly, Everalbum would be able to bring enforcement actions against entities that misappropriated that information. One could also imagine a scenario where an entity is required to delete work product protected by copyright law, such as software.[167] But again, would this entail forfeiture of all the rights enshrined by copyright,[168] or simply deletion of the company's copies of the software? Just like the trade secret owner, if the copyright owner is merely prohibited from personally owning and using their copyrighted work then they could continue to generate profits

163. Auty et al., *supra* note 11.

164. Final Order at 5, Everalbum, Inc., No. C-4743 (F.T.C. May 6, 2021).

165. Final Order at 4, Cambridge Analytica, LLC, No. 9383 (F.T.C. Nov. 25, 2019); Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief at 8, United States v. Kurbo Inc., No. 3:22-cv-00946-TSH (N.D. Cal. 2022).

166. Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 25 (2007).

167. *Copyright Protection of Computer Software*, WORLD INTELL. PROP. ORG., https://www.wipo.int/copyright/en/activities/software.html [https://perma.cc/FKB7-DY3F].

168. Copyright includes such rights as the right to reproduce and distribute copies of the work, and to create works based on the original. Copyright Act of 1976, 17 U.S.C. § 106.

through licensing efforts.[169] They could also generate profits by litigating their rights.[170] Indeed, the same question arises if the ill-gotten data is used to protect an invention protected by patent law. A company—forced to destroy copies of a patented invention—could still presumably thrive by leveraging its patent-enshrined rights.[171] A proliferation of businesses called non-practicing entities, or NPEs, own patented subject matter but do not use or sell their inventions. [172] Rather, their business model is to generate profit in two ways: by licensing their patented technology and enforcing their patent rights in litigation.[173] So, if an entity subject to the IP deletion requirement retained its patent rights, then it could nevertheless monetize its IP much like an NPE.

How the FTC chooses to answer these questions through future use of the IP deletion requirement will impact the scope of deterrence for companies, and, accordingly, protection for consumers.[174] For example, should the requirement only apply to companies that create IP using biometric data, the IP deletion requirement will be significantly limited in application. Similarly, should companies be able to sell or license the resulting IP, the financial penalty underlying the IP deletion requirement would be limited. Given the FTC's common-law-like jurisprudence with regard to its section 5 powers, the FTC may be able to look to other common law doctrines for inspiration in ways that it cannot when enforcing statutory law.

II. THE LAW OF ACCESSION AND THE WRONGFUL IMPROVER

These questions can be answered by analogizing to the wrongful improver rule under the law of accession. Accordingly, this Part provides useful background on the doctrine. Accession law allocates interests in personal property that has been created by combining different parties' property or by transforming one party's property into something else by

169. *Id.* ("[T]he owner of copyright under this title has the exclusive rights to . . . transfer of ownership, or by rental, lease, or lending.").

170. 17 U.S.C. § 501 (granting copyright owners the right to sue for infringement).

171. For example, the right to exclude others, 35 U.S.C. § 154(a)(1), and the right to convey patents to others, 35 U.S.C. § 261.

172. Robin Feldman, *The Pace of Change: Non-Practicing Entities and the Shifting Legal Landscape*, 18 CHAP. L. REV. 635, 635–36 (2015).

173. *Id.*

174. For a further discussion of how using misappropriated data in algorithms harms consumers, see Li, *supra* note 5, at 11 ("algorithmic shadows" persist even after data is deleted and can cause harm both to an individual and to groups that relate to that individual).

another.[175] In other words, accession law determines whether the changed property belongs to the owner of its principal parts or to the person who transformed it.[176]

In an accession law analysis, courts first determine whether accession applies. First, they ask whether there has been a combination or transformation of property.[177] If the property of two persons has been combined, then the court will next ask whether the materials in question are physically detachable without damage.[178] If they are, then accession does not apply.[179] For example, the Vermont Supreme Court held that accession did not apply to a wagon whose wheels and axles had been added by the plaintiff, since the wheels and axles were severable from the wagon.[180]

Courts may find that there has been a transformation sufficient to apply accession law on two grounds: either because the original property has changed in identity, or because the defendant has significantly increased its value.[181] Courts typically hold that transformation occurs where the change in an item of property is so great that the original materials cannot be reproduced out of the resulting articles.[182] For example, transformation has been found where clay was turned into bricks, since the process of burning necessarily changes the qualities of the clay.[183]

If accession applies, courts then determine title to the property.[184] In cases where property is combined, accession dictates that the property rights vest in the owner of the principal part of the materials in the product.[185] Various ship-building cases illustrate this rule: if a shipbuilder combines his labor and materials with those of another, the owner of the materials that make up the keel of the ship acquires title because the keel is considered to be the principal component of the ship.[186] In cases where property is transformed, the law of accession typically vests title in the

175. Jay L. Koh, *From Hoops to Hard Drives: An Accession Law Approach to the Inevitable Misappropriation of Trade Secrets*, 48 AM. U. L. REV. 271, 321 (1998).

176. *Id.*

177. *Id*. at 322.

178. *Id.*

179. *Id.*

180. Clark v. Wells, 45 Vt. 4, 5 (1872).

181. Koh, *supra* note 174, at 325.

182. 1 THOMAS MUSKUS, C.J.S. ACCESSION § 12 (2022).

183. Lampton's Ex'rs v. Preston's Ex'rs, 24 Ky. 454, 465–66 (Ky. App. 1829).

184. Koh, *supra* note 175, at 328.

185. *Id.*

186. *Id.* at 328; Glover v. Austin, 23 Mass. (6 Pick.) 209, 209 (1828); Appeal of Coursin, 79 Pa. 220, 229 (1875).

transformer.[187]

For example, in the 1871 case of *Wetherbee v. Green*,[188] the Supreme Court of Michigan considered whether a defendant was entitled to the barrel hoops he had created using the plaintiff's lumber.[189] In that case, the defendant Wetherbee had cut down lumber on land he believed that he had license to use.[190] Indeed, the license had been originally granted to Wetherbee by the plaintiff's tenant-in-common, Sumner.[191] However, Sumner had sold his interest in the land before Wetherbee chopped down the lumber, and Green argued that the license had been revoked.[192] However, the trial court refused to allow testimony that Wetherbee's entry onto the land had been in good faith, and that he believed that he still had license to enter.[193] The court then reviewed the general rule of accession law, while noting that "in the case of a willful appropriation, no extent of conversion can give to the willful trespasser a title to the property so long as the original materials can be traced in the improved article."[194] The court remanded the case for a new trial in which the defendant would be allowed to show that he acted in good faith.[195] Such a result, the court notes, would "influence the courts in recognizing a change of title," that is, Wetherbee would be entitled to the hoops, minus damages for his unintentional trespass.[196]

While the application of accession law looks slightly different in combination and transformation cases, the principle can broadly be described as awarding title to the party with the more valuable interest.[197] As a result, a plaintiff may lose property rights simply because another made something more valuable using that property. But accession law also requires that the party who is awarded title must compensate the other party for the value of the other party's interest.[198]

In this way, accession law seeks to resolve a puzzle of competing property interests. Yet accession may award the party with the greater property interest only where that party gained the other's property

187. Koh, *supra* note 175, at 329.

188. 22 Mich. 311 (1871).

189. *Id.* at 312–13.

190. *Id.* at 312.

191. *Id.*

192. *Id.* at 313.

193. *Id.*

194. *Id.* at 315.

195. *Id.* at 322.

196. *Id.* at 321.

197. *Accession on the Frontiers of Property*, *supra* note 37, at 2382.

198. *Id.*

innocently.[199] That is, a party must act in good faith to get the benefit of accession law.[200] Where a party uses the property for a transformation or combination in a way that is both wrongful and willful, they cannot retain interest in the property.[201] They must either transfer title to the innocent party or compensate that party with the reasonable value of the property in its improved state.[202] This is the rule even when the wrongful party substantially improved the value of the property by transforming or combining it.[203] For example, in *Wetherbee v. Green*, the plaintiff's lumber was valued at twenty-five dollars.[204] The defendant then increased the value to seven-hundred dollars by turning the lumber into barrel hoops.[205] Although accession applied in that case because the defendant acted innocently,[206] the plaintiff would have received the full seven-hundred-dollar benefit had the defendant acted in bad faith, by application of the bad faith principle. Situations where accession law would be applicable due to the combination or transformation of property interests, but is ultimately not applied, are often governed by what will be hereafter referred to as the "wrongful improver rule."

Against the context of accession law, analysis according to the wrongful improver rule can be summarized as follows. First, the facts must be such that a court would recognize that accession law poses a potential solution, such as where the materials and labor of two parties are combined, or where one party improves the property of another.[207] Second, the court must consider whether the party that added their labor or materials to the other's property (hereafter called the "improver") acted in bad faith.[208] Bad faith attaches anywhere the improver knew that the property that they were improving was owned by someone else.[209] Finally, if bad faith is present, the court must apply what this Comment has termed the wrongful improver rule.[210] Analytically, it is in this step that the court declines to apply accession law even though it would help in sorting out property interests. Applying the wrongful improver rule requires the court

199. Koh, *supra* note 175, at 326.

200. *Id.*

201. *Id.*

202. 1 THOMAS M. FLEMING, N.Y. JUR.: ACCESSION § 7 (2d ed. 2022).

203. Koh, *supra* note 175, at 325.

204. Wetherbee v. Green, 22 Mich. 311, 313 (1871).

205. *Id.*

206. *See* Koh, *supra* note 175, at 325.

207. *Id.* at 322.

208. *Id.* at 326.

209. *Id.*

210. *Id.* at 327.

to award the improved property to the innocent party, that is, the party who did not do the improving, even if the property has become much more valuable through improvement.[211]

The wrongful improver rule is illustrated in the case of *Union Naval Stores Co. v. United States*.[212] In that case, the United States brought an action against the Union Naval Stores Company to claim turpentine and rosin, products that Union Naval's supplier, Rayford, had created by extracting sap from trees on government lands.[213] Before beginning the process of "boxing" the trees for sap extraction, Rayford was informed by a third party, Freeland, that Freeland had applied for a homestead entry on the land but that entry remained unperfected; thus, the land remained the property of the U.S. government.[214] Nevertheless, Rayford moved forward with his sap extraction operations upon the Freeland homestead, justifying his actions by saying "there is no law against turpentining a piece of homestead land as long as you are on it."[215] In fact, Rayford's assumption was incorrect: the court pointed out that nothing in the letter or policy of the Homestead Act[216] permitted the boxing and chipping of trees required for sap extraction.[217] By conducting his operations on the homestead with notice that the land was the property of the U.S. government, the court found Rayford to be a willful trespasser and that his act of distilling the gum taken from the government's land was "a continuing act of trespass that did not devest the United States of its property, but left it still entitled to the manufactured products."[218] The court noted that Rayford's mistake of law was insufficient to excuse him.[219] Further, the court allocated the turpentine to the U.S. government even though Rayford had mixed the ill-acquired turpentine with his own lawfully acquired stock.[220]

The wrongful improver rule is also illustrated in *Snyder v. Vaux*.[221] In that case, the Supreme Court of Pennsylvania upheld a judgement against a defendant who had knowingly trespassed onto the plaintiff's land and

211. *See id.* at 333 n.375.

212. 240 U.S. 284 (1916).

213. *Id.* at 285–86.

214. *Id.* at 286–87.

215. *Id.* at 286.

216. Homestead Act, §§ 1–2, 12 Stat. 392 (repealed 1976) (allowing citizens to claim up to 160 acres of public land provided they live on it, improve it, and pay a registration fee).

217. *Union Naval Stores*, 240 U.S. at 289.

218. *Id.* at 290.

219. *Id.*

220. *Id.* at 291–92.

221. 2 Rawle 423 (Pa. 1830).

cut down timber that he then turned into rails and posts.[222] Notably, the defendant argued that by turning the trees into rails and posts, their identity had been so altered that the action of replevin—that is, to recover the property itself[223]—could not be maintained.[224] The court disagreed.[225] In response, it said, "[a] wilful [sic] trespasser cannot acquire title to property, merely by changing it from one article into another, as by working trees cut down into shingles, or into cord word, logs or rails."[226] As a result, and because the defendant had known at the time that he was trespassing, the court awarded ownership of the rails and posts to the plaintiff.[227]

III. ANALOGIZING THE IP DELETION REQUIREMENT TO THE WRONGFUL IMPROVER RULE

In his statement following the *Everalbum* settlement, former FTC Commissioner Rohit Chopra described the IP destruction provision as requiring Everalbum to "forfeit the fruits of its deception."[228] The same principle motivates the wrongful improver rule in accession law. And much like the concepts of unjust enrichment and disgorgement, which other scholars have argued should be the basis for privacy remedies,[229] analogy to the wrongful improver rule provides a useful lens for evaluating the IP deletion requirement. This Part first explains how the analogy to this rule functions. Then, this Part explores how the wrongful improver rule can inform future applications of the IP deletion requirement in FTC privacy actions, answering questions that linger from the *Cambridge Analytica*, *Everalbum*, and *Kurbo* cases. This Part next explores limitations associated with the proposed analogy, and why those limitations should not preclude application of the rule. Finally, this Part explores additional consumer-focused benefits of using the wrongful improver rule to guide applications of the IP deletion requirement.

---

222. *Id.* at 427.

223. *See id.*

224. *Id.*

225. *Id.*

226. *Id.*

227. *Id.*

228. STATEMENT OF ROHIT CHOPRA, *supra* note 16.

229. *See generally* Li, *supra* note 5 (discussing algorithmic disgorgement as a remedy in FTC privacy cases); Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L. REV. 653, 654 (2019) (arguing that courts should consider restitution as the quintessential remedy choice for privacy matters).

A. Applying the Wrongful Improver Framework to Cases Like Everalbum

The law of accession is used to address the specific problem of dividing property interests when one's property and another's labor have been combined.[230] It would seem, therefore, that accession law could be applied to evaluate the IP rights created through the use of others' data. However, when applying the analytical framework to situations like those in *Everalbum*—that is, a business having used consumer data unlawfully—it is more apt to use the wrongful improver rule, which applies when the scenario fits but accession itself does not.

Applying the wrongful improver framework proceeds in three steps.[231] First, the facts must present a scenario where accession law could be of use, such as where the materials and labor of two parties are combined to produce something new.[232] Second, the court must consider whether the "improver"—that is, the party that added their labor or materials to the other's property—acted in bad faith.[233] The quintessential bad faith scenario is one where the improver knew that the property they were improving belonged to someone else.[234] Finally, assuming there is bad faith at play, the court must apply the wrongful improver rule.[235] Analytically, this is the step in which the court declines to apply the rules of accession on the basis of bad faith, despite being a case where such a rule poses a potential solution.[236] Doing so requires the court to award the improved property to the innocent owner of the unimproved property, even if the improver has greatly increased the value of the property.[237]

These steps clearly map onto a case like *Everalbum*. First, the app users who unknowingly contributed volumes of images and facial data may be viewed as the owners of the unimproved property. In this way, user data can be viewed similarly to an input material. In contrast, Everalbum improved and increased the value of that data[238] by contributing their labor and skill, as well as the property that they had lawfully acquired, such as

230. *See supra* Part II.

231. *See supra* Part II.

232. *See supra* Part II.

233. *See supra* Part II.

234. *See supra* Part II.

235. *See supra* Part II.

236. *See supra* Part II.

237. *See supra* Part II.

238. While the value of data increases as it is incorporated into intellectual property, it should be noted that the value of the data itself also increases simply by being in the hands of a company, rather than the consumer. Scholz, *supra* note 229, at 677.

the public datasets of facial images. By combining the "material" of user data with skilled labor, Everalbum was thus able to produce its proprietary facial recognition technology.

Of course, this comparison is somewhat limited in that users do not lose all rights to their personal data when it is misused. For example, the users whose images were collected in *Everalbum* still presumably have rights to privacy of that data. On the other hand, had the court in *Wetherbee* found that accession applied, the plaintiff would have lost all rights in the proprietary bundle of sticks, including the rights to possess, control, exclude, and transfer. But similar to the plaintiff in *Wetherbee*, the users of Everalbum suffered an injury to a valuable, integral asset. Simply being compensated for that injury does not restore the integrity of their privacy, or the damage of having their privacy violated, just as being compensated for the value of their trees does not restore the damage of trespass and conversion. Both assets have been irreversibly destroyed in the process of creating something new.

Applying the second step of the wrongful improver framework to Everalbum requires identifying bad faith. Specifically, the court would ask whether a defendant had knowingly violated the privacy rights of its users. Notably, the FTC does not need to find intent, such as a knowing violation, to find liability under section 5.[239] As a result, application of the wrongful improver framework suggests that the rule would not be appropriate in every case. Nevertheless, it is likely that the wrongful improver rule would be applicable in many cases, based on how federal courts find personal liability. In personal liability cases, the FTC must show that the defendant, typically an executive of a target corporation, (1) was directly involved in or had authority to control the alleged misconduct, and (2) knew or was recklessly indifferent to the alleged misconduct.[240] And commentators suggest that executives of companies like Google and Meta could be found liable readily under this rule, where evidence of knowledge can be found through repeated disregard for the privacy of consumers.[241] Imputing a corporate officer's knowledge to the

239. FTC v. Bay Area Bus. Council, Inc., 423 F.3d 627, 635 (7th Cir. 2005) ("The FTC is not, however, required to prove intent to deceive.").

240. FTC v. Ross, 743 F.3d 886, 892 (4th Cir. 2014).

241. Eliot Van Buskirk, *Report: Facebook CEO Mark Zuckerberg Doesn't Believe in Privacy*, WIRED (Apr. 28, 2010, 1:47 PM), https://www.wired.com/2010/04/report-facebook-ceo-mark-zuckerberg-doesnt-believe-in-privacy/ [https://perma.cc/4JAT-DN3A]; Richard Esguerra, *Google CEO Eric Schmidt Dismisses the Importance of Privacy*, ELEC. FRONTIER FOUND. (Dec. 10, 2009), https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy [https://perma.cc/ENW7-XYR2].

corporation through agency law,[242] knowledge would therefore attach to the organization itself. But despite the heightened burden imposed by the knowledge requirement, it is likely that bad faith would be present in many cases.

Application of the wrongful improver rule comprises the final leg of the analogy. In a case like *Everalbum*, the wrongful improver rule would require the defendant to forfeit their intellectual property rights or pay the full value of their intellectual property. Given that IP plays such a huge role in the ability of tech companies to grow and acquire funding,[243] it is likely that forfeiting IP rights better serves to discourage improper data privacy practices than merely paying a monetary fine equal to the value of that property. Accordingly, this Comment focuses primarily on the forfeiture of rights as the outcome in such cases.

Although the wrongful improver rule cannot be applied perfectly in cases like *Everalbum*, it can nevertheless guide future FTC enforcement efforts.

B. Analogy to the Wrongful Improver Rule Indicates Forfeiture of IP Rights

Lingering in the wake of *Everalbum* is the question: what exactly does the IP destruction requirement entail? The language of the consent order requires Everalbum to "delete or destroy any Affected Work Product,"[244] where "Affected Work Product" is defined as "any models or algorithms developed in whole or in part using Biometric Information" that Everalbum collected form users of the Ever mobile app.[245] One could interpret this language to mean that Everalbum must simply delete models and facial recognition algorithms from its platforms, preventing Everalbum from continuing to use them in its products.[246] But a broader interpretation might also apply—one that would require Everalbum to forfeit all intellectual property rights to the technology.[247] This would include forfeiting the right to enforce any trade secret rights that the

242. CLARK BOARDMAN CALLAGHAN, 3 FLETCHER CYCLOPEDIA OF THE L. OF CORPS. § 790 (2021) ("[T]he general rule is well established that a corporation is charged with constructive knowledge, regardless of its actual knowledge, of all material facts of which its officer or agent receives notice or acquires knowledge while acting in the course of employment within the scope of his or her authority, even though the officer or agent does not in fact communicate the knowledge to the corporation.").

243. *See* Juetten, *supra* note 23.

244. Decision and Order at 5, Everalbum, Inc., No. C-4743 (F.T.C. May 6, 2021).

245. *Id.* at 2.

246. *See* Auty et al., *supra* note 11.

247. *See id.*

company had acquired in its models or algorithms.[248] This would also mean that Everalbum must forfeit the ability to license these assets to other entities. Similarly, Everalbum would not be able to transfer its rights in a sale. Thus, the settlement order could require mere IP deletion, or total destruction of IP rights.

Application of the wrongful improver rule to this scenario indicates the latter. Where the rule is applied and bad faith improvers must give the improved property to the plaintiff, the defendant sacrifices ownership of the property;[249] that is, they sacrifice every property right in the proverbial "bundle of sticks"[250] associated with ownership of that property. For example, in *Snyder v. Vaux*, the defendant had to convey to the plaintiff all the wooden posts and rails that he had created from the trees he cut on the plaintiff's land.[251] Presumably, this included the right to otherwise transfer those same rails and posts in a sale to another party. Similarly, application of the wrongful improver rule to cases like *Everalbum* would indicate that a defendant must forfeit rights to license or sell any technology they have developed using ill-gotten data. Applying the rule would also indicate that a defendant like Everalbum would forfeit the ability to enforce any trade secret, copyright, or patent rights in its technology to prevent another party from misappropriating that technology. By conveying to the plaintiff the rails and posts that the defendant had produced using the plaintiff's timber, the defendant in *Snyder* likewise gave up his rights to exclude others from using those materials, such as claims of conversion or trespass to chattels. Therefore, applying the wrongful improver rule would demand that defendants forfeit all rights in IP developed using ill-gotten data, not just simply delete it.

The implications of this result are significant. Licensing of IP assets is a popular way for companies, particularly in the technology sector, to create new income streams.[252] As a result, a defendant required by the FTC to merely delete its IP, but not forfeit all rights in that IP, could still theoretically license that technology and continue profiting from it. This

---

248. *Id.*

249. *See supra* Part II.

250. CECILY FUHR & MICHAEL N. GIULIANO, 73 CORPUS JURIS SECUNDUM: PROPERTY § 1 (2022) ("A common idiom describes property as a 'bundle of sticks,' i.e., collection of individual rights which, in certain combinations, constitute property . . . .").

251. Snyder v. Vaux, 2 Rawle 423, 427 (Pa. 1830).

252. Chor Meng Tan, *Driving Innovation Through Intangible Assets and Intellectual Property Rights*, FORBES (June 1, 2021, 7:00 AM), https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2021/06/01/driving-innovation-through-intangible-assets-and-intellectual-property-rights/?sh=7d66c26763af [https://perma.cc/WKT5-JRWU].

would fundamentally conflict with the sentiment behind both the wrongful improver rule and the IP deletion requirement in *Everalbum*. In his statement regarding the then-proposed settlement order with Everalbum, former Commissioner Chopra noted a prior similar case with Google, wherein the company was allowed "to profit from its conduct" of illegally collecting data from children, despite entering into a settlement agreement with the FTC.[253] It is clear that application of the wrongful improver rule, which would prevent companies from continuing to profit through IP licensing, would provide the desired outcome for these cases. As a result, companies collecting data from users would be more heavily incentivized to comply with privacy regulations and their own public privacy statements

C. Analogy to the Wrongful Improver Rule Indicates IP Destruction in Cases of Non-Biometric Data

The *Everalbum* case involved collection of facial images,[254] which are a type of biometric data.[255] *Cambridge Analytica*[256] and *Kurbo*[257] involved biometric information as well. In general, biometric data is considered to be a more sensitive type of personal data and is often subject to higher privacy standards than other types of personal data.[258] As a result, practitioners wonder whether the FTC will apply the IP deletion requirement even in cases where non-biometric (i.e., less sensitive) data has been unlawfully collected and used by defendants to create intellectual property.[259]

The wrongful improver rule applies "even if there is great change in the nature of the property or great increase in its value."[260] For example, the court in *Wetherbee* was prepared to award the plaintiff with the

253. STATEMENT OF ROHIT CHOPRA, *supra* note 16, n.3.

254. Complaint at 4, Everalbum, Inc., No. C-4743 (F.T.C. May 6, 2021).

255. Claire Gartland, Opinion, *Biometrics Are a Grave Threat to Privacy*, N.Y. TIMES (July 5, 2016, 3:21 AM), https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy [https://perma.cc/QE4D-6Y8U].

256. Hartmans, *supra* note 34 (noting that although it's unclear precisely what information Cambridge Analytica collected from users, they likely had access to Facebook users' photos, which contain biometric information).

257. Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 11, United States v. Kurbo, Inc. et al., No. 22-CV-946 (N.D. Cal. Feb. 15, 2022) (noting that defendant Kurbo collected user information such as height, weight, food intake, and activity levels).

258. *See generally* General Data Protection Regulation, art. 9, 2016 O.J. (L 679); California Consumer Privacy Act, CAL. CIV. CODE § 1798.140; Biometric Information Privacy Act, 740 ILCS 14.

259. *See* Auty et al., *supra* note 11.

260. Koh, *supra* note 175, at 333.

defendant's barrel hoops in the event that bad faith was found on remand,[261] even though the defendant increased the value of the hoops from twenty-five dollars to seven-hundred dollars.[262] One can infer, further, that the result would have been the same had the disparity in value been even greater. Thus, application of the wrongful improver rule suggests that IP deletion would be appropriate even in cases where the data collected is not biometric; that is, where the "input material" is of lesser value and, consequently, the disparity between the input and output is even greater.

In this way, application of the wrongful improver rule to cases of misappropriated data broadens the scope of the IP deletion requirement. It would make IP deletion available as a settlement provision no matter the type of data involved. Therefore, it would provide broad deterrence, encouraging lawful data collection practices amongst every company that collects data on its users, instead of only those engaged in gathering biometric data. Such an effect would no doubt motivate an environment of greater data privacy for consumers online.

D. Limits of Analogizing to the Wrongful Improver Rule

As noted above, there are certainly imperfections in the analogy suggested. For example, application of the wrongful improver rule demands that the defendant either return the improved property to the plaintiff or compensate them for their original, unimproved property.[263] Though this Comment argues for application of the rule where property must be returned, neither possible outcome may be fully effectuated in reality. To convey a single facial recognition algorithm to countless users whose information had been used in its creation would create a mess of ownership rights. Of course, this limitation of the analogy is minimal: to actually convey the IP to the users likely would not provide them much benefit and would not serve to deter companies from committing privacy violations any more than having their IP rights simply destroyed. The impossibility of compensating users for their data as "input material" for resulting IP is another limitation of the analogy. It may be difficult to place a value on the facial data of a person's photos, although valuation may be informed by the prices charged by data aggregators in selling such data. But even if such compensation could be valued, it would be impossible to implement this prong of the analogy because the FTC currently does not

261. Wetherbee v. Green, 22 Mich. 311, 315–16 (1871).

262. *Id.* at 313.

263. *See supra* Part II.

have the ability to issue fines for first time penalties under the FTC Act.[264] But again, even given this limitation, analogy to the wrongful improver rule would result in the two major deterrents to companies collecting user data: complete IP destruction and application in cases of non-biometric data.

Another broader potential limitation of applying the wrongful improver rule comes from the fact that there are some risks in viewing personal data as property.[265] For example, treating data as property implicates potential problems of commodification.[266] Specifically, the idea of the digital self can be viewed as created in terms of our data: our phone calls, credit card transactions, age, voting record, mouse clicks, and more.[267] Under this view, trading and selling data as property is akin to alienating ourselves (both in the property and psychological sense) from ourselves and undermining our identities.[268] Opponents of the privacy-as-property formulation prefer to view data protection as a civil rights issue.[269] In an explanation by one scholar, for those who embrace this view, "the notion of protecting personal data by commodifying it would likely be as obnoxious as the notion of protecting the voting franchise by commodifying it."[270]

In truth, the reality is that consumer data is already being commodified because corporations have a practice of treating data as a transferrable, sellable resource.[271] Indeed, "an unimaginable amount of information . . . is aggressively traded . . . by data aggregators."[272] Refusing to view personal data as property reserves the benefit of this view for businesses that can profit off of gathering and selling consumer data, while leaving consumers with no ability to claim rights that would similarly enable them to do so.[273] Failing to provide individuals with

264. Solove & Hartzog, *supra* note 29, at 605.

265. *See generally* Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TELECOMMS. TECH. L. REV. 367, 398 (2012).

266. *Id.*

267. *Id.*

268. *Id.*

269. *See* Pamela Samuelson, *A New King of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 772 (1999) (reviewing PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996)).

270. *Id.*

271. *See* Steve Kroft, *How You're Tracked Online – and What You Can Do About It*, CBS NEWS (Mar. 31, 2018, 10:56 AM), https://www.cbsnews.com/news/how-youre-tracked-online-facebook-google-amazon-uber-what-you-can-do-about-it/ [https://perma.cc/V9MZ-TMGM].

272. Baron, *supra* note 265, at 400.

273. *Id.*

property rights to personal information enhances the power of others, "in whose hands the information is solely a commodity."[274]

Furthermore, it may be that viewing information as akin to property would resonate more from the U.S. perspective, given the country's history of jealously guarding property rights and comparative resistance to recognizing civil rights. For example, it has long been the case that an action for trespass may entitle a plaintiff to damages even if the defendant caused no actual damage to the plaintiff's property.[275] In contrast, the United States has historically been, and continues to be, reluctant to recognize fundamental human rights.[276] Treating personal information like property would appeal to values that are more ingrained in U.S. law, albeit regrettably, and may thus be a more effective way to gain recognition.

Moreover, there is precedent for the overlap of privacy and property rights. The right to privacy in the United States began as an outgrowth of property rights.[277] As demonstrated by Fourth Amendment[278] jurisprudence, the right to be free from unreasonable searches and seizures was originally tied to one's property, in that it applied when one was in their home.[279] But the Supreme Court has broadened its interpretation of the Fourth Amendment to bar unreasonable searches and seizures in the context of cell phones because doing so would involve accessing a wealth of information about a person.[280] In this way, U.S. privacy law is contiguous with property law. Viewing privacy issues with a property doctrine is not an unprecedented idea, and courts are likely to be familiar with the overlap between these areas of laws and the interests they are

274. *Id.* at 398.

275. 7 AMERICAN LAW OF TORTS § 23:37 (Stuart M. Speiser et al. eds., 2022).

276. *See, e.g.*, *Introduction to Transgender Rights in the United States*, HOW. UNIV. SCHOOL OF L., https://library.law.howard.edu/civilrightshistory/transgender [https://perma.cc/V7Y4-NQC5] (highlighting the battle for recognition of transgender rights); *Racial Discrimination in the United States*, HUM. RTS. WATCH (Aug. 8, 2022), https://www.hrw.org/report/2022/08/08/racial-discrimination-united-states/human-rights-watch/aclu-joint-submission [https://perma.cc/JEW6-U5F4] (outlining the past and present of racial discrimination in the U.S.).

277. Mary Chlopecki, *The Property Rights Origins of Privacy Rights*, FOUND. FOR ECON. EDUC. (Aug. 1, 1992), https://fee.org/articles/the-property-rights-origins-of-privacy-rights/[https://perma.cc/3D8D-5KHW]. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). This was a seminal article that argued for and precipitated the idea that certain property offenses, including defamation and breach of confidence, are better viewed as harms to a right to privacy.

278. U.S. CONST. amend. IV.

279. *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967) (holding that use of wiretapping to acquire evidence in a criminal investigation was not a Fourth Amendment violation because it was not a physical invasion of the suspect's home).

280. *See* Riley v. California, 573 U.S. 373, 386 (2014).

designed to protect.

Courts are no strangers to importing ideas from one area of law to another.[281] They understand that doing so does not necessitate importing every idea from that area of law or viewing two areas of law identically. As a result, even if viewing data as property risks commodification of the self, applying the wrongful improver rule to IP created with unlawfully collected data likely does not run the same risk.

Lastly, it is important to note that compliance with IP deletion requirements would be costly and would have the potential to chill innovation, particularly among smaller companies.[282] As a result, "[t]hese policies could counterintuitively help further entrench outsized market power from Big Tech companies."[283] However, as the FTC develops its application of the IP deletion requirement, it could establish exceptions for nonprofits, small startups, and companies with limited resources.[284]

E. Looking Forward: Potential Applications of the Wrongful Improver Rule

The wrongful improver rule can provide greater deterrence for privacy violators who use consumer data to create IP because it applies so long as the company or at least one of its executives has knowledge or constructive knowledge of the wrongdoing. So, who could be subject to this rule in the near future?

Potential subjects abound. A crowded category of targets consists of companies engaged in developing artificial intelligence (AI). AI, although a very broad term, generally means a group of algorithms that can modify its own algorithms and create new ones based on input data.[285] For companies developing AI, consumer data is critical to improving functionality.[286] Should companies gather this data unlawfully, application of the wrongful improver rule would trigger forfeiture of

---

281. *See, e.g.*, Global-Tech Appliances, Inc. v. SEB S.A., 563 U.S. 754, 768 (2011) (importing the willful blindness standard from criminal law into patent law, specifically contributory patent infringement).

282. Li, *supra* note 5, at 24.

283. *Id.*

284. *See id.*

285. Kaya Ismail, *AI vs. Algorithms: What's the Difference?*, CMSWIRE (Oct. 26, 2018), https://www.cmswire.com/information-management/ai-vs-algorithms-whats-the-difference/ [https://perma.cc/C4H4-8VKA].

286. *See* Andrew Ng & Michael Chui, *How Artificial Intelligence and Data Add Value to Businesses*, MCKINSEY (Mar. 26, 2018), https://www.mckinsey.com/featured-insights/artificial-intelligence/how-artificial-intelligence-and-data-add-value-to-businesses (last visited Oct. 8, 2022).

some, if not all, of such algorithms, as in the *Everalbum* case.[287] Virtually all of the world's tech giants are currently racing to develop their AI technology, including Meta, Google, and Apple.[288] Meta, for example, has made it clear that it may continue to use its facial recognition technology, DeepFace, in its upcoming metaverse products, despite abandoning the tool for use on Facebook and Instagram.[289] Continuing to offer the tool would likely mean that Meta continues to develop the tool with user images, as it did when it first started offering the tool in 2010.[290] Such new iterations of its DeepFace technology would thus represent a potential target for the IP deletion requirement, should Meta collect its users' images unlawfully.

Firms that develop behavioral biometric tools for authentication represent another potential target. These tools, which are frequently used by banks and online retailers, track the individual gestures a person makes as they interact with computers and smartphones to determine whether a person is who they claim to be.[291] One such developer, Forter, uses a database with profiles on 175 million people to develop this technology.[292] Application of the wrongful improver doctrine in future cases would no doubt motivate companies like Forter to collect such information lawfully.

Considering the emphasis that consumer data plays in the widespread efforts to develop AI, the FTC would be well served by using the wrongful improver rule to encourage proper privacy practices.

CONCLUSION

The IP deletion requirement imposed by the FTC in *Everalbum* introduced a level of severity rarely seen before in FTC privacy actions. Questions that remain unanswered about how the requirement will be

---

287. *See supra* section III.B.

288. Bernard Marr, *The 10 Best Examples of How Companies Use Artificial Intelligence in Practice*, FORBES (Dec. 9, 2019, 12:26 AM), https://www.forbes.com/sites/bernardmarr/2019/12/09/the-10-best-examples-of-how-companies-use-artificial-intelligence-in-practice/?sh=243d9da67978 [https://perma.cc/4JQR-UHA9].

289. Rebecca Heilweil, *Facebook Is Backing Away from Facial Recognition. Meta Isn't.*, VOX (Nov. 3, 2021, 2:20 PM), https://www.vox.com/recode/22761598/facebook-facial-recognition-meta [https://perma.cc/ZJ3B-NZLJ].

290. Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, N.Y. TIMES (Nov. 5, 2021), https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html (last visited Oct. 8, 2022).

291. Stacy Cowley, *Banks and Retailers Are Tracking How You Type, Swipe and Tap*, N.Y. TIMES (Aug. 13, 2018), https://www.nytimes.com/2018/08/13/business/behavioral-biometrics-banks-security.html (last visited Oct. 8, 2022).

292. *Id.*

applied in the future leave the door open to possibilities which provide the FTC with an even farther-reaching tool of deterrence. The wrongful improver rule, derived from U.S. accession law, demonstrates how courts deal with property disputes that bear keen resemblance to the facts of *Everalbum*, where a defendant willfully used data about its users to develop IP. Applying this rule directly to *Everalbum*-like cases demonstrates doctrinal support for resolving these remaining questions in the most far-reaching way. First, applying the rule indicates that the IP deletion requirement should be interpreted to mean complete destruction of IP rights, thereby eliminating the possibility that a company licenses, sells, or enforces any trade secret, copyright, or patent rights. Second, applying the rule indicates that the IP deletion requirement should be used even in cases where non-biometric data has been misappropriated.

Through the March 2022 *Kurbo* case as well as official statements, FTC leadership has indicated that it intends to continue implementing more rigorous punishment for companies who disregard their users' privacy. Should the agency consider answering the aforementioned questions in upcoming cases, it should look to the wrongful improver rule for doctrinal justification and answers that provide the best protection for consumers nationwide.