

November 21, 2022

To: Federal Trade Commission

Re: Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022) (Document No. 2022-17752)

The Institute for Policy Integrity at New York University School of Law (Policy Integrity)¹ respectfully submits the following comments to the Federal Trade Commission (FTC or the Commission) regarding the above-referenced Advanced Notice of Proposed Rulemaking (Notice). Policy Integrity is a non-partisan think tank dedicated to improving the quality of government decisionmaking through advocacy and scholarship in the fields of administrative law, economics, and public policy.

In the Notice, the Commission seeks “comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data.”² The Commission reports that “consumers have little to no actual control over what happens to their information once companies collect it,” pointing to companies’ “use of dark patterns” as a common practice limiting consumer control over their own data.³ The Commission notes that “trade regulation rules reflecting these current realities may be needed” to both protect consumers from the harms of unwanted data retention and “foster a greater sense of predictability for companies and consumers and minimize the uncertainty that case-by-case enforcement may engender.”⁴

As Policy Integrity laid out in a recent report, the Commission should consider regulating the use of immortal accounts.⁵ “Immortal accounts” refers to a phenomenon by which entities obstruct the process of deleting a consumer account or do not provide any account-deletion option at all.⁶ In some cases, immortal accounts result when entities deceive a user into believing an account was entirely deleted, when in reality the data from that account was maintained.⁷ The Commission has recognized that entities use immortal accounts and “confusing cancellation policies” as a type of “manipulative design practices” known as “dark patterns” that “get consumers to part with their money or data.”⁸ **This letter offers justification**

¹ This document does not purport to present New York University School of Law’s views, if any.

² Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273, 51,273 (Aug. 22, 2022) [hereinafter Notice].

³ *Id.* at 51,274, 51,287.

⁴ *Id.* at 51,276.

⁵ LAURA A. FIGUEROA ET AL., REGULATING IMMORTAL ACCOUNTS, INST. FOR POL’Y INTEGRITY (2022) (enclosed).

⁶ *Id.* at i.

⁷ *Id.*

⁸ FED. TRADE COMM’N, BRINGING DARK PATTERNS TO LIGHT 1 (2022), <https://perma.cc/63UJ-85F4>; *id.* at 22 (recognizing that use of “immortal accounts” “mak[es] it hard or impossible to delete an account”).

for regulating the use of immortal accounts and highlights best practices for the cost-benefit analysis for such a regulation.

I. The Commission Should Regulate the Use of Immortal Accounts

Immortal accounts create considerable consumer harm. In the case of negative option subscription services, where consumers are charged fees so long as they do not cancel, immortal accounts threaten monetary harm through unwanted charges. Retention of personally identifiable consumer data through the use of immortal accounts also leaves consumers vulnerable to identity theft and other monetary harms arising from potential data breaches, internal misuse of data, or unwanted secondary uses of information.⁹ Users are also harmed by the loss of control over their personal data, and when an account is difficult to cancel and an individual must engage in onerous steps or resort to outside research to aid in cancelling an account, that individual has suffered a loss of time.¹⁰

An FTC rule that requires reasonable cancellation practices for all market actors and provides clear and specific guidelines for what constitutes an unreasonable account-deletion practice would address the harms of immortal accounts. Some key factors to be considered in a rule banning unreasonable account-deletion practices are: the time, number of steps, and type of steps required to complete the account-deletion process; whether external help such as research through sources outside of the platform is necessary; and the presence of other tactics that undermine the will of the user.

Additionally, and subject to any necessary exceptions, the FTC should prohibit entities from retaining consumer account information that either explicitly or constructively identifies a particular consumer after purportedly deleting the consumer's account. To the extent necessary, the Commission may outline exceptions for which data retention is necessary, such as those proposed by Consumer Reports in its Model State Privacy Act.¹¹ For example, the Commission should not restrict the retention of de-identified or anonymized data, provided that the Commission defines these terms with sufficient rigor.¹²

A rule protecting consumers from the use of immortal accounts would be consistent with FTC precedent and with action on dark patterns by other legislative and enforcement bodies. For one, the FTC has recognized immortal accounts as a deceptive practice through individual enforcement actions.¹³ The FTC also recently released an Enforcement Policy Statement Regarding Negative Option Marketing explaining that negative option sellers must

⁹ See Comments of the Center for Democracy & Technology at 2, *FTC Informational Injury Workshop P175413* (Oct. 27, 2017), <https://perma.cc/ENJ6-MEK8> (discussing risks of data over-collection).

¹⁰ FIGUEROA ET AL, *supra* note 5, at 5–7 (explaining how the use of immortal accounts harms and unduly burdens consumers).

¹¹ CONSUMER REPORTS, MODEL STATE PRIVACY ACT 18–20 (2021), <https://perma.cc/34ZE-JSR7>.

¹² See, e.g., *id.* at 15, 18 (defining “deidentified” and exempting such data from model law). The FTC has stated that data is de-identified when there is a “reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device.” FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 21 (2012), <https://perma.cc/8RDK-WMSQ>.

¹³ See, e.g., FED. TRADE COMM’N, STATEMENT OF COMMISSIONER ROHIT CHOPRA REGARDING DARK PATTERNS IN THE MATTER OF AGE OF LEARNING, INC. (2020), <https://perma.cc/S85N-APD9> (“By making it extremely difficult to cancel recurring subscription fees, ABCmouse engaged in conduct that was not only unethical, but also illegal.”).

“provide a simple, reasonable means for consumers to cancel their contracts.”¹⁴ Other legislative and enforcement bodies, both in the United States and abroad, have also taken action to regulate immortal accounts and other dark patterns.¹⁵

Regulation in this mold falls under the Commission’s authority and would advance the FTC’s mission to protect consumers and competition by preventing anticompetitive, deceptive, and unfair business practices. First, the use of immortal accounts is a deceptive practice because it involves material omissions or misrepresentations that are likely to mislead consumers acting reasonably under the circumstances.¹⁶ Second, the use of immortal accounts is an unfair practice because the practice “causes or is likely to cause substantial injury to consumers” and perpetuates “harm(s) to a large number of people”¹⁷ which are “not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”¹⁸ Third, the use of immortal accounts presents an unfair method of competition because the practice bestows powerful advantages to entities that use it, perpetuating a race to the bottom in terms of privacy protection.¹⁹

The attached report, *Regulating Immortal Accounts*, offers more detail on both the harms from immortal accounts and the legal standards for regulating them.

II. A Robust Cost-Benefit Can Help Support Immortal-Accounts Regulation

In questions 24 through 29 of the Notice, the Commission seeks guidance on how it should balance regulatory costs and benefits.²⁰ In response, this section offers guidance to the Commission on conducting a cost-benefit analysis, with a focus on the suggested regulation on immortal accounts. **A strong cost-benefit analysis can both inform the Commission’s rulemaking and bolster the record in support of any future rule.**

The Commission must assess the “economic effect of [any] rule” regulating unfair or deceptive acts of practices,²¹ and, for unfair practices specifically, must determine that the “substantial injury to consumers which is not reasonably avoidable by consumers themselves” and the injury prevented by regulation is “not outweighed by countervailing benefits to consumers or to competition.”²² These requirements largely mirror the mandates of rational decisionmaking imposed upon all administrative agencies by executive order and the Administrative Procedure Act (APA).²³ Under Executive Order 12,866, executive agencies are

¹⁴ Enforcement Policy Statement Regarding Negative Option Marketing, 86 Fed. Reg. 60,822, 60,826 (Nov. 4, 2021).

¹⁵ FIGUEROA ET AL, *supra* note 5, at 1–4.

¹⁶ Fed. Trade Comm’n v. Stefanchik, 559 F.3d 924, 928 (9th Cir. 2009); *see also* FIGUEROA ET AL, *supra* note 5, at 8–10.

¹⁷ Fed. Trade Comm’n v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 2010) (internal quotation marks omitted).

¹⁸ 15 U.S.C. § 45(n) (first and third quotes); Fed. Trade Comm’n v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 2010) (internal quotation marks omitted) (second quote); *see also* FIGUEROA ET AL, *supra* note 5, at 10–14.

¹⁹ Fed. Trade Comm’n v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 313 (1934) (outlining legal standard); *see also* FIGUEROA ET AL, *supra* note 5, at 14–15.

²⁰ Notice, 87 Fed. Reg. at 51,282.

²¹ 15 U.S.C. § 57a(d)(1)(C).

²² *Id.* § 45(n).

²³ The Federal Trade Commission Act’s evidentiary standards require “the same degree of evidentiary support needed to satisfy the arbitrary and capricious standard” under the Administrative Procedure Act. Consumers Union of U.S., Inc. v. FTC, 801 F.2d 417, 422 (D.C. Cir. 1986).

instructed to conduct an assessment of the costs and benefits of all major regulations and to “adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify the costs.”²⁴ And under the Administrative Procedure Act (APA), agencies typically treat regulatory costs as a “centrally relevant factor when deciding whether to regulate.”²⁵

While a “formal cost-benefit analysis in which each advantage and disadvantage is assigned a monetary value” is not required under either the APA²⁶ or the Federal Trade Commission Act,²⁷ the APA imposes certain obligations on the Commission to reasonably assess and weigh beneficial and adverse regulatory impacts. For one, the agency cannot disregard reasonably foreseeable adverse impacts.²⁸ The Commission should seek to “quantify the certain costs” of the rule to the extent practicable, or else “explain why those costs could not be quantified.”²⁹ Moreover, agencies must reasonably balance regulatory costs and benefits.³⁰ In balancing costs and benefits, the Commission should “look beyond the direct benefits and direct costs of [its] rulemaking and consider any important ancillary benefits and countervailing risks” that may result.³¹

With respect to costs, a potentially substantial cost of regulating the use of immortal accounts will be the “[p]rivate-sector compliance cost” that entities will incur to modify their account-deletion process. Although precise estimates of compliance cost are likely unavailable, the Commission may wish to commission its own study or consult with economists or industry experts on the issue. The Commission should also be receptive to (and critically consider) estimates provided by the regulated community. The Commission should transparently disclose the basis for any estimates.³² Moreover, the Commission should consider the government administrative cost, or the FTC’s enforcement cost, to enforce any regulation on immortal accounts.

²⁴ Exec. Order No. 12,866 §1(b)(6), 58 Fed. Reg. 51,733 (Oct. 4, 1993). Although Executive Order 12,866 does not directly apply to independent agencies like the FTC, *id.* § 3(b), courts have recognized that independent agencies must rationally assess regulatory costs and benefits. See *Bus. Roundtable v. SEC*, 647 F.3d 1144, 1149 (D.C. Cir. 2011) (rejecting rule promulgated by the SEC, another independent agency, due to faulty cost-benefit analysis).

²⁵ *Michigan v. EPA*, 576 U.S. 743, 752-53 (2015).

²⁶ *Id.* at 759 (“We need not and do not hold that the law unambiguously required the Agency, when making this preliminary estimate, to conduct a formal cost-benefit analysis in which each advantage and disadvantage is assigned a monetary value.”).

²⁷ *Am. Fin. Servs. Ass’n v. FTC*, 767 F.2d 957, 986 (D.C. Cir. 1985) (explaining that, under the FTCA, “a highly quantitative benefit/cost analysis may not be appropriate in each and every individual case,” as the statute rather requires the FTC to “summarize its best estimate of” the regulation’s economic impact) (internal quotation marks omitted).

²⁸ *Cf. Nat’l Family Farm Coal. v. United States EPA*, 960 F.3d 1120, 1142 (9th Cir. 2020) (“FIFRA requires the EPA to consider, as part of a cost-benefit analysis, any unreasonable risk to man or the environment, *taking into account the economic, social, and environmental costs* and benefits of the use of any pesticide. . . . The EPA entirely failed to acknowledge risks of economic and social costs.”) (internal quotation marks and citation omitted).

²⁹ *Bus. Roundtable v. SEC*, 647 F.3d 1144, 1149 (D.C. Cir. 2011).

³⁰ *Id.* at 1148-49 (faulting agency for lopsided analysis that “inconsistently and opportunistically frame[s]” regulatory impacts); see also *Ctr. for Biological Diversity v. Nat’l Highway Traffic Safety Admin.*, 538 F.3d 1172, 1198 (9th Cir. 2008) (agency cannot “put a thumb on the scale”).

³¹ Office of Mgmt. & Budget, Circular A-4 on Regulatory Analysis 26 (2003) (hereinafter “Circular A-4”).

³² See *Mayor of Baltimore v. Azar*, 973 F.3d 258, 282 (4th Cir. 2020) (en banc) (vacating regulation as arbitrary and capricious when agency provided “no justification” for compliance-cost estimates and failed to provide any studies supporting those estimates).

An immortal-account regulation might also impose costs by denying entities access to consumer data that could otherwise be used to better target advertisements or develop new product features. However, the cost to this loss would likely be limited so long as entities could continue to be retain de-identified or anonymized data that may inform the entity’s ability to target advertisements or develop new product features. Nonetheless, the Commission should explore whether there may be any costs to entities that lose access to personal data.

In terms of benefits, the Commission can expect a regulation on immortal accounts to produce a decrease in the time consumers waste when they must jump through hoops or engage in outside research to cancel an account. While also difficult to measure with precision, the Commission can make basic assumptions, using available information, about time wasted on attempting to cancel accounts.³³ The Commission can measure time saved “both in terms of hours saved and to the extent feasible, in terms of monetary equivalents” through “a measure of the value of that time.”³⁴ For instance, the Commission can use the average U.S. hourly wage as a proxy for the monetary value of each hour of time saved.

The Commission can also expect a regulation on immortal accounts to produce an increase in data security and consumer autonomy over data. When users can delete their accounts at will, their personal data will no longer be susceptible to identity theft and other harms arising from data breaches, internal misuse of data, or other unwanted secondary uses of information.³⁵ Thus, a quantifiable benefit would result from the decreased probability of data misuse and resulting damages, and from the decrease in stress that users feel regarding the potential for their data to be misused, as consumers value their data and control over that data.³⁶ Notably, one study found that the median participant would “demand \$80 [per month] to allow access to personal data.”³⁷ The Commission could use studies of this kind to estimate autonomy and data-security benefits.

Finally, the Commission should assess and consider the transfer payments likely to result from regulation, even though those transfers are neither costs nor benefits in the strict economic sense. Transfer payments are “monetary payments from one group to another that do not affect total resources” available to society.³⁸ One class of transfers likely to result from a regulation on immortal accounts is a decrease in accounts or subscriptions, thereby transferring money (where subscriptions include regular payments) from the business to the consumer.³⁹ Though neither a cost nor a benefit in the strict sense, this distributional impact can nonetheless help justify a regulation.⁴⁰

³³ See, e.g., FIGUEROA ET AL, *supra* note 5, at 6 (describing results of survey of six web sites finding an average time of under one minute to create an account but over 15 minutes to delete the same account).

³⁴ OMB, Regulatory Impact Analysis: Frequently Asked Questions 11 (Feb. 7, 2011), <https://perma.cc/63RE-SPE4> [hereinafter Regulatory Impact Analysis FAQ].

³⁵ Comments of the Center for Democracy & Technology at 2, *FTC Informational Injury Workshop P175413* (Oct. 27, 2017), <https://perma.cc/ENJ6-MEK8>.

³⁶ Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 15, 2019), <https://perma.cc/WG2L-GWJB>.

³⁷ A. G. Winegar & C. R. Sunstein, *How Much is Data Privacy Worth? A Preliminary Investigation*, 42 J. CONSUMER POL’Y 425, 425 (2019).

³⁸ Regulatory Impact Analysis FAQ, *supra* note 34, at 8.

³⁹ See Circular A-4, *supra* note 31, at 38 (explaining transfers).

⁴⁰ See *id.* at 14.

* * *

Policy Integrity supports regulatory action on dark patterns that harm consumers, including immortal accounts. As detailed in the enclosed report, the FTC has the authority to regulate immortal accounts, and should do so as part of this rulemaking. In addition, the FTC should support such regulation with a cost-benefit analysis conducted in line with best practices.

Sincerely,

Laura A. Figueroa, Legal Fellow
Max Sarinsky, Senior Attorney

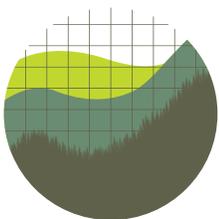
Enclosure:

- 1) LAURA A. FIGUEROA ET AL., REGULATING IMMORTAL ACCOUNTS, INST. FOR POL'Y INTEGRITY (2022)



Regulating Immortal Accounts

How the FTC Can Limit Unwanted Data Retention



Institute for
Policy Integrity

NEW YORK UNIVERSITY SCHOOL OF LAW

May 2022

Laura A. Figueroa

Max Sarinsky

Rayne Ellis

Emma Schwartz

Copyright © 2022 by the Institute for Policy Integrity.
All rights reserved.

Institute for Policy Integrity
New York University School of Law
Wilf Hall, 139 MacDougal Street
New York, New York 10012

Laura A. Figueroa is a Legal Fellow at the Institute for Policy Integrity at New York University School of Law, where Max Sarinsky is a Senior Attorney. Rayne Ellis and Emma Schwartz graduated from New York University School of Law in 2022, and contributed to this report as students in New York University School of Law's Regulatory Policy Clinic. The authors thank Jack Lienke and Richard Revesz for providing valuable guidance and feedback, and Alex Song for his careful review.

This report does not necessarily reflect the views, if any, of New York University School of Law.

Executive Summary

In a widely-anticipated speech in April 2022 before the International Association of Privacy Professionals, Federal Trade Commission Chair Lina Khan described how digital technologies have allowed companies to collect data on consumers at a “hyper-granular level,” enabling a multitude of consumer harms including fraud, identity theft, cyberstalking, and unprecedented systemic power imbalances between companies and consumers.¹ She then expressed her belief that the Commission should “approach data privacy and security protections by considering substantive limits rather than just procedural protections.”²

One important substantive limit that the FTC should pursue is a restriction on the use of immortal accounts, which infringe on consumer privacy and create a host of consumer harms.

“Immortal accounts” refers to a phenomenon by which entities³ obstruct the process for deleting a consumer account or do not provide any account deletion option at all.⁴ Some entities might even trick a user into believing an account was entirely deleted, when in reality the data from that account was maintained.⁵ By making the account deletion process deliberately challenging, if not altogether impossible, the entity dissuades users from deleting in order to continue to retain data, charge subscriptions, or profit from the user’s personal information.⁶

Immortal accounts create considerable consumer harm. In the case of negative option subscription services, where consumers are charged fees so long as they do not cancel, immortal accounts threaten monetary harm through unwanted charges. Retention of personally identifiable consumer data through the use of immortal accounts also leaves consumers vulnerable to identity theft and other monetary harms arising from potential data breaches, internal misuse of data, or unwanted secondary uses of information.⁷ Users are also harmed by the loss of control and autonomy over their personal data, and when an account is difficult to cancel and an individual must engage in onerous steps or resort to outside research to aid in cancelling an account, that individual has suffered a loss of time.⁸

An FTC rule that that requires reasonable cancellation practices for all market actors and provides clear and specific guidelines for what constitutes an unreasonable account deletion practice would address the harms of immortal accounts. Some key factors to be considered in a rule banning unreasonable account deletion practices are:

¹ *In First Major Policy Speech, FTC Chair Lina Khan Highlights Data Privacy and Security Enforcement Priorities*, PAUL WEISS (Apr. 18, 2022), <https://www.paulweiss.com/practices/litigation/data-innovation-privacy-cybersecurity/publications/in-first-major-policy-speech-ftc-chair-lina-khan-highlights-data-privacy-and-security-enforcement-priorities?id=42954>.

² *Id.*

³ This report uses “entity” to refer to any “person, partnership, or corporation” that FTC has authority over pursuant to 15 U.S.C. § 45(b). While the report focuses primarily on Internet-based entities, the issues discussed are also applicable to immortal account practices by other entities.

⁴ As used in this report, the term “account” can be understood as “a formal business arrangement providing for regular dealings or services (such as banking, advertising, or store credit) and involving the establishment and maintenance of an account” or “an arrangement in which a person uses the Internet or email services of a particular company.” *Account*, MERRIAM-WEBSTER ONLINE DICTIONARY (last updated May 8, 2022), <https://www.merriam-webster.com/dictionary/account>.

⁵ Christoph Bosch et al., *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, 4 PROCEEDINGS ON PRIVACY ENHANCING TECH. 237, 251 (2016).

⁶ See generally Colin M. Gray et al., *The Dark (Patterns) Side of UX Design*, in PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYS. 4, 6 (2018) (discussing Roach Motels).

⁷ See Comments of the Center for Democracy & Technology at 2, *FTC Informational Injury Workshop P175413* (Oct. 27, 2017), <https://cdt.org/wp-content/uploads/2017/10/2017-1027-CDT-FTC-Informational-Injury-Comments.pdf> (discussing risks of data over-collection).

⁸ See *infra* Section I for a fuller discussion of harms to consumers from immortal accounts.

the time, number of steps, and type of steps required to complete the account deletion process; whether external help such as research through sources outside of the platform is necessary; and the presence of other tactics that undermine the will of the user.

Additionally, and subject to any necessary exceptions, the FTC should prohibit entities from retaining consumer account information that reasonably identifies a particular consumer after purportedly deleting the consumer’s account. To the extent necessary, the Commission may outline exceptions for which data retention is necessary, such as those proposed by Consumer Reports in their Model State Privacy Act.⁹ For example, the Commission should not restrict the retention of de-identified or anonymized data, provided that the Commission defines these terms with sufficient rigor.¹⁰

A rule protecting consumers from the use of immortal accounts would be consistent with FTC precedent and with action on dark patterns by other legislative and enforcement bodies. For one, the FTC has recognized immortal accounts as a deceptive practice through individual enforcement actions.¹¹ The FTC also recently released an Enforcement Policy Statement Regarding Negative Option Marketing explaining that negative option sellers must “provide a simple, reasonable means for consumers to cancel their contracts.”¹² Other enforcement and legislative bodies, both in the United States and abroad, have also taken action to regulate immortal accounts and other deceptive online design features, known as dark patterns.

Regulation in this mold falls under the FTC’s authority and would advance the FTC’s mission to protect consumers and competition by preventing deceptive, unfair, and anticompetitive business practices. First, the use of immortal accounts is a deceptive practice because it involves material omissions or misrepresentations that are likely to mislead consumers acting reasonably under the circumstances.¹³ Second, the use of immortal accounts is an unfair practice because the practice “causes or is likely to cause substantial injury to consumers”¹⁴ and perpetuates “harm(s) to a large number of people”¹⁵ which are “not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”¹⁶ Third, the use of immortal accounts presents an unfair method of competition because the practice bestows powerful advantages to entities that use them, perpetuating a race to the bottom in terms of privacy protection.¹⁷

⁹ CONSUMER REPORTS, MODEL STATE PRIVACY ACT 18–20 (2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

¹⁰ *See, e.g., id.* at 15, 18 (defining “deidentified” and exempting such data from model law). The FTC has stated that data is de-identified when there is a “reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device.” FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 21 (2012), <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers>.

¹¹ *See, e.g.,* FED. TRADE COMM’N, STATEMENT OF COMMISSIONER ROHIT CHOPRA REGARDING DARK PATTERNS IN THE MATTER OF AGE OF LEARNING, INC. (2020), https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf [hereinafter “Statement Regarding Dark Patterns”] (“By making it extremely difficult to cancel recurring subscription fees, ABCmouse engaged in conduct that was not only unethical, but also illegal.”).

¹² Enforcement Policy Statement Regarding Negative Option Marketing, 86 Fed. Reg. 60,822, 60,826 (Nov. 4, 2021) [hereinafter “Enforcement Policy Statement”].

¹³ Fed. Trade Comm’n v. Stefanchik, 559 F.3d 924, 928 (9th Cir. 2009).

¹⁴ 15 U.S.C. § 45(n).

¹⁵ Fed. Trade Comm’n v. Neovi, Inc., 604 F.3d 1150, 1157 (9th Cir. 2010) (internal quotation marks omitted).

¹⁶ 15 U.S.C. § 45(n).

¹⁷ Fed. Trade Comm’n v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 313 (1934) (outlining legal standard).

Table of Contents

Background: Regulation of Immortal Accounts by the FTC and Other Legislative and Enforcement Bodies	1
I. Immortal Accounts Harm and Unduly Burden Consumers	5
II. Immortal Accounts Fall Squarely Within the FTC’s Authority to Regulate Deceptive, Unfair, and Anticompetitive Trade Practices	8
A. The Use of Immortal Accounts Constitutes a Deceptive Practice Within the Meaning of Section 5 of the FTCA	8
i. Immortal Accounts Involve Misrepresentations, Misleading Omissions, and/or Deceptive Practices	8
ii. The Misleading Omissions and Representations Are Material	9
B. The Use of Immortal Accounts Constitutes an Unfair Practice Within the Meaning of Section 5 of the FTCA	10
i. Immortal Accounts Cause Substantial Injuries to Consumers	11
ii. The Consumer Harms from the Use of Immortal Accounts Are Not Reasonably Avoidable	12
iii. The Substantial Injuries Are Not Offset by Countervailing Benefits	13
iv. Established Public Policy Supports an Unfairness Determination	13
C. Immortal Accounts Constitute an Unfair Method of Competition Within the Meaning of Section 5 of the FTCA	14
Conclusion	15

Background: Regulation of Immortal Accounts by the FTC and Other Legislative and Enforcement Bodies

The FTC has already signaled an interest in addressing the problem of dark patterns in general, and immortal accounts in particular. In 2020, the FTC settled an enforcement action against ABCmouse, an online children’s learning program, which failed to inform users that their memberships would automatically renew and made it difficult for users to cancel their memberships; as a result, users incurred unwanted charges.¹⁸ The FTC alleged that ABCmouse had committed unfair and deceptive trade practices.¹⁹ In a statement discussing the action, then-Commissioner Rohit Chopra affirmed the FTC’s commitment to stamping out online dark patterns that companies use to deceive consumers:

Digital deception should not be a viable American business model. If the Federal Trade Commission aspires to be a credible watchdog of digital markets, the agency must deploy these tools to go after large firms that make millions, or even billions, through tricking and trapping users through dark patterns. We cannot replicate the whack-a-mole strategy that we have pursued on pressing issues like fake reviews, digital disinformation, and data protection. Instead, we need to methodically use all of our tools to shine a light on unlawful digital dark patterns, and we need to contain the spread of this popular, profitable, and problematic business practice.²⁰

“Digital deception should not be a viable American business model. If the Federal Trade Commission aspires to be a credible watchdog of digital markets, the agency must deploy these tools to go after large firms that make millions, or even billions, through tricking and trapping users through dark patterns.”

Former FTC Commissioner
Rohit Chopra

Numerous other FTC enforcement actions further demonstrate the agency’s commitment to protecting consumers against dark patterns such as immortal accounts. The Commission has addressed these practices in both the digital and analog space, particularly through enforcement actions against telemarketers.²¹ In one action in 2006, the FTC alleged that a business’s practices were deceptive under Section 5(a) of the Federal Trade Commission Act (“FTCA”) when the business routinely made it “difficult or impossible for the consumers to cancel” their accounts.²² In another action in

¹⁸ See Complaint at 3, Fed. Trade Comm’n v. Age of Learning, Inc., No. 2:20-cv-07996 (C.D. Cal. Sept. 1, 2020) (outlining allegations); Stipulated Order for Permanent Injunction and Monetary Judgment, Fed. Trade Comm’n v. Age of Learning, Inc., No. 2:20-cv-07996 (C.D. Cal. Sept. 8, 2020) (outlining terms of settlement, including \$10 million judgment and injunction of certain practices).

¹⁹ Complaint at 20–23, *Age of Learning, Inc.*, No. 2:20-cv-07996.

²⁰ Statement Regarding Dark Patterns, *supra* note 11, at 3.

²¹ See, e.g., First Amended Complaint at 14, Fed. Trade Comm’n v. Universal Premium Servs., Inc., No. CV06-0849 (C.D. Cal. May 9, 2006), <https://www.ftc.gov/sites/default/files/documents/cases/2006/05/060509famndcmplt0523153.pdf>; First Amended Complaint at 12–14, Fed. Trade Comm’n v. Remote Response Corp., No. 1:06-cv-20168-CMA (S.D. Fla. June 5, 2006), <https://www.ftc.gov/sites/default/files/documents/cases/2006/06/060606remoterresponsefirstamndcmplt.pdf> (charging misrepresentation of cancellation policy as a deceptive practice and denial or ignoring of cancellation requests through telephone line as an unfair practice).

²² First Amended Complaint at 11, *Universal Premium Servs.*, No. CV06-0849. These practices included providing an incorrect phone number for cancellations, telling consumers that the order was “not ‘in the system yet,’” telling consumers that the request was still “processing,” and other misleading and dilatory tactics. *Id.* The court granted summary judgment in favor of the FTC on this issue. Fed. Trade Comm’n v. Universal Premium Servs., No. CV06-0849, 2007 WL 9728965, at *4 (C.D. Cal. Feb. 21, 2007).

Entities often use deceptive design choices, known as “dark patterns,” to inhibit consumers from deleting their accounts. Dark patterns may take the form of difficult-to-locate links and menus online, deliberately confusing language, or an unreasonable amount of steps to conclude a cancellation request, among other practices.³⁰ The use of immortal accounts is an example of a dark pattern.

2007, the FTC obtained a settlement with Sony,²³ which had made it almost impossible to uninstall software from consumers’ computers that was needed to access certain content.²⁴ The FTC had charged this practice as unfair or deceptive under Section 5 of the FTCA.²⁵

More recently, in April 2021, the FTC hosted a workshop titled “Bringing Dark Patterns to Light,” at which researchers, legal experts, consumer advocates, and industry specialists discussed the ways in which “user interfaces can have the effect, intentionally or unintentionally, of obscuring, subverting, or impairing consumer autonomy, decision-making, or choice.”²⁶ Panelists discussed various types of dark patterns, how they affect consumers, and how they should be combatted.²⁷ One panelist highlighted immortal

accounts as an example of dark patterns that erode users’ control over their own data.²⁸ In his closing remarks for the workshop, Daniel Kaufman, acting director of the Bureau of Consumer Protection for the FTC, said that the Commission would continue with aggressive enforcement of dark patterns and would continue to consider “all options,” including potential new regulations in this area.²⁹

These statements were followed by new FTC enforcement guidance for negative option marketing published in November 2021.³¹ The guidance focuses on services that take a “consumer’s silence or failure to take affirmative action to reject a good or service or to cancel the agreement as acceptance or continuing acceptance of the offer.”³² While the guidance specifically requires negative option sellers to provide a simple mechanism to stop recurring charges under the Restore Online Shoppers’ Confidence Act, it also clarifies that under Section 5 of the FTCA, “marketers must not erect unreasonable barriers to cancellation or impede the effective operation of promised cancellation procedures, and must honor cancellation requests that comply with such procedures.”³³ Apart from this new guidance, the FTC also signaled in late 2021 that it is considering initiating rulemaking to “limit privacy abuses.”³⁴

Beyond FTC enforcement actions and policy statements, other enforcement and legislative bodies, both in the United States and abroad, have taken action to regulate dark patterns broadly and immortal accounts specifically. The Consumer Financial Protection Bureau recently sued the credit reporting bureau TransUnion for using an “array of dark patterns to trick people into recurring payments” and “not only fail[ing] to offer a simple mechanism for cancellation, [but] []

²³ Decision and Order, Sony BMG Music Entertainment, Docket No. C-4195 (June 28, 2007), <https://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019do070629.pdf>.

²⁴ Complaint at 2–3, Sony BMG Music Entertainment Docket No. C-4195 (June 28, 2007), <https://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019cmp070629.pdf>.

²⁵ *Id.* at 5.

²⁶ See *Bringing Dark Patterns to Light: An FTC Workshop*, FED. TRADE COMM’N (Apr. 29, 2021) <https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop>.

²⁷ *Id.*

²⁸ *Id.*, Transcript at 9–11 (Apr. 29, 2021) (statement of Johanna T. Gunawan), https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf.

²⁹ *Id.*, Transcript at 84 (statement of Daniel Kaufman).

³⁰ Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 48–50 (2021).

³¹ Enforcement Policy Statement, 86 Fed. Reg. 60,822.

³² *Id.* at 60,822.

³³ *Id.* at 60,823–24.

³⁴ *Trade Regulation Rule on Commercial Surveillance*, RIN 3084-AB69, OFF. INFO. & REG. AFFAIRS (2021), <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69>.

actively ma[king] it arduous for consumers to cancel through clever uses of font and color on its website.”³⁵ The District of Columbia also sued Grubhub and Google this year for allegedly using dark patterns in their services.³⁶ The separate complaints allege that Grubhub charged hidden fees for food delivery³⁷ and that Google “makes extensive use of dark patterns, including repeated nudging, misleading pressure tactics, and evasive and deceptive descriptions of location features and settings, to cause users to provide more and more location data (inadvertently or out of frustration).”³⁸

State legislatures have also taken aim at dark patterns. For example, starting in 2023 the California Consumer Privacy Act (“CCPA”) will explicitly define “dark pattern” as “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation” and render any user consent obtained through the use of a dark patterns ineffective.³⁹ Current CCPA regulations already prohibit “method[s] that [are] designed with the purpose or [have] the substantial effect of subverting or impairing a consumer’s choice to opt-out” of the sale of personal information.⁴⁰ The CCPA also provides consumers the right to request the deletion of personal information and obligates businesses to fulfill such requests.⁴¹ The Colorado Privacy Act, which goes into effect in 2023, uses the same definition for dark patterns as the latest CCPA amendment, similarly prohibits their use in obtaining consent, and also provides consumers the right to delete personal data.⁴² Likewise, Virginia’s Consumer Data Protection Act, which also takes effect next year, includes a consumer’s right “[t]o delete personal data provided by or obtained about the consumer.”⁴³

Enacted laws in California, Colorado, and Virginia – the latter two of which take effect in 2023 – provide consumers the right to delete personal data.

Meanwhile, regulators in Europe are empowered to regulate companies in accordance with the General Data Protection Regulation (“GDPR”), which includes the “right to be forgotten” under Article 17.⁴⁴ This regulation gives individuals the right to have their data erased for a number of reasons, including if the individual retracts consent or if his or her “personal data [is] no longer necessary in relation to the purposes for which [it was] collected or otherwise processed.”⁴⁵ In enforcing the various provisions of the GDPR, regulators have focused on the use of dark patterns and imposed penalties on entities that used dark patterns to erode consumer autonomy and data privacy. In 2019, for instance, the CNIL (the French data protection authority) fined Google 50 million euros for lack of transparency, inadequate information,

³⁵ CFPB Charges TransUnion and Senior Executive John Danaher with Violating Law Enforcement Order, Consumer Fin. Prot. Bureau (Apr. 12, 2022), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-charges-transunion-and-senior-executive-john-danaher-with-violating-law-enforcement-order/>; see Complaint, Consumer Fin. Prot. Bureau v. TransUnion, No. 1:22-cv-01880 (N.D. Ill. Apr. 12, 2022), https://files.consumerfinance.gov/f/documents/cfpb_transunion_complaint_2022-04.pdf.

³⁶ Ben Brody, *The FTC is Going After Dark Patterns. That’s Bad News for Amazon Prime.*, PROTOCOL (Apr. 25, 2022), <https://www.protocol.com/policy/dark-patterns-subscriptions-ftc-amazon>.

³⁷ Complaint at 3, 26, District of Columbia v. Grubhub Holdings, Inc., No. 2022 CA 001199 B (D.C. Super. Ct. Mar. 21, 2022), <https://perma.cc/XJ7F-Z96X>.

³⁸ Complaint at 24, District of Columbia v. Google LLC, No. 2022 CA 000330 B (D.C. Super. Ct. Jan. 24, 2022), <https://perma.cc/4YQ3-RX24>.

³⁹ Cal. Civ. Code § 1798.140(1) (effective Jan. 1, 2023); *id.* § 1798.140(h) (effective Jan. 1, 2023) (“[A]greement obtained through use of dark patterns does not constitute consent.”)

⁴⁰ Cal. Code Regs. tit. 11, § 999.315(h). Among other illustrative examples, this regulation provides that a business’s “process for submitting a request to opt-out shall not require more steps than that business’s process for a consumer to opt-in to the sale of personal information.” *Id.* § 999.315(h)(1).

⁴¹ Cal. Civ. Code § 1798.105(a), (c).

⁴² Colo. Rev. Stat. §§ 6-1-1303(5)(c), 6-1-1303(9), 6-1-1306(1)(d) (all effective July 1, 2023).

⁴³ Va. Code Ann. § 59.1-577(A)(3) (effective Jan. 1, 2023).

⁴⁴ Commission Regulation 2016/679 art. 17, 2016 J.O. (119), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.

⁴⁵ *Id.*

and lack of valid consent in its ad personalization tool.⁴⁶ The French regulator found that Google had imposed too many hurdles for users to properly set their privacy preferences:

Essential information, such as the data processing purposes, the data storage periods or the categories of personal data used for the ads personalization, are excessively disseminated across several documents, with buttons and links on which it is required to click to access complementary information. The relevant information is accessible after several steps only, implying sometimes up to 5 or 6 actions.⁴⁷

Immortal accounts specifically have also been the subject of enforcement actions by South Korea’s Fair Trade Commission, which recently fined Netflix, Google, and other subscription service businesses for making it difficult for consumers to cancel their memberships.⁴⁸ As these examples illustrate, regulators around the world are taking action to protect consumers against dark patterns. FTC regulation of immortal accounts would follow in this mold.

While there is not yet any federal law aimed specifically at dark patterns or immortal accounts,⁴⁹ there are several proposed bills that address these topics. For example, the Deceptive Experiences To Online Users Reduction Act (“DETOUR Act”), would make it unlawful for larger online operators “to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data.”⁵⁰ Similarly, the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (“SAFE DATA Act”), would establish various requirements relating to the collection of consumer data, data transparency, and security.⁵¹ The bill recognizes users’ right to delete or de-identify their data, and requires covered entities to comply with users’ reasonable requests to do so.⁵² As these so-far unsuccessful attempts at legislation illustrate, there is a demand for regulation of data privacy that has not yet been fulfilled.

⁴⁶ *The CNIL’s Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, EURO. DATA PROT. BD. (Jan 21, 2019), https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.

⁴⁷ *Id.*

⁴⁸ Jin-Ho Jeung & Tae-Hee Lee, *FTC Identifies, Prohibits, Streaming-Service ‘Dark Patterns’*, KOREA JOONGANG DAILY (Feb. 14, 2022), <https://koreajoongangdaily.joins.com/2022/02/14/business/industry/netflix-google-kt/20220214180532859.html>.

⁴⁹ As the Commission recognized in its Enforcement Policy Statement Regarding Negative Option Marketing, certain federal legislation—such as the Restore Online Shoppers’ Confidence Act, the Electronic Fund Transfer Act, and the Unordered Merchandise Statute—“address various aspects of negative option marketing” and thus provide authority to regulate certain uses of dark patterns. Enforcement Policy Statement, 86 Fed. Reg. at 60,823.

⁵⁰ S. 1084, 116th Congress, § 3(a)(1)(A) (2019).

⁵¹ S. 4626, 116th Congress (2019–2020).

⁵² *Id.* § 103(a)(1)(C).

I. The Use of Immortal Accounts Harms and Unduly Burdens Consumers

Immortal accounts cause a number of significant harms to consumers. As then-Commissioner Chopra outlined in his statement regarding *ABCmouse*, immortal accounts often require consumers to spend considerable time jumping over burdensome hurdles in order to delete their accounts.⁵³ In some cases, if the consumer is unsuccessful in deleting that account, he or she will be subject to additional charges as a result of continuing fees. Many consumers who confront immortal accounts may also worry about the safety and use of their personal information, and could forgo using products or services that they were interested in due to privacy concerns.⁵⁴ In this way, immortal accounts waste consumer time, cost consumers money, infringe on consumer dignity and autonomy, and erode consumer trust.

To make account cancellation difficult or impossible, many entities use dark patterns “to deceive, steer, or manipulate users into behavior that is profitable for an online service, but often harmful to users or contrary to their intent.”⁵⁵ Dark patterns are used for many different and often related objectives, such as promoting account registration and permissive data sharing. Much of the existing research in this area explores the harmful effects of dark patterns as a unit. This is likely due to the fact that websites frequently deploy these tactics in concert with one another; thereby making it difficult for researchers to isolate the harm from a single tactic. Nonetheless, existing research clearly indicates that the array of tactics used to create immortal accounts harms consumer autonomy, trust, and time.

Dark patterns are “strikingly effective in getting consumers to do what they would not do when confronted with more neutral user interfaces.”⁵⁶ One study—which was co-authored by University of Chicago law professor Lior Jacob Strahilevitz and published in Harvard’s *Journal of Legal Analysis*—found that relatively mild dark patterns more than doubled the percentage of consumers who signed up for a dubious identity theft protection service, while aggressive patterns, like “Roach Motels” that make it easy for users to sign up for the service but very difficult to decline it, nearly quadrupled the percentage of consumers signing up.⁵⁷ The authors also provided evidence that “less educated Americans are significantly more vulnerable to dark patterns than their more educated counterparts,” particularly with respect to more subtle dark patterns.⁵⁸

According to this same study, “hidden information (smaller print in a less visually prominent location), obstruction (making users jump through unnecessary hoops to reject a service), trick questions (intentionally confusing prompts), and social proof (efforts to generate a bandwagon effect)” are the most effective dark pattern strategies.⁵⁹ The use of immortal accounts may deploy all or some of the above dark pattern strategies in order to keep account holders from successfully deleting their account.⁶⁰

⁵³ Statement Regarding Dark Patterns, *supra* note 11, at 2.

⁵⁴ See Andrew Perrin, *Half of Americans Have Decided Not to Use a Product or Service Because of Privacy Concerns*, PEW RSCH. CTR. (Apr. 14, 2020), <https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/>.

⁵⁵ Statement Regarding Dark Patterns, *supra* note 11, at 1.

⁵⁶ Luguri & Strahilevitz, *supra* note 30, at 46.

⁵⁷ *Id.*; *id.* at 62 (explaining that Roach Motels were used in the “aggressive” condition).

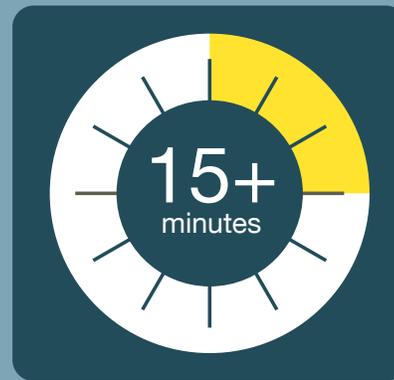
⁵⁸ *Id.* at 47.

⁵⁹ *Id.*

⁶⁰ See generally Bosch et al., *supra* note 5, at 250 (explaining how service providers “unnecessarily complicat[e] the account deletion experience” through the use of immortal accounts).



Average Time to Create an Account
44 Seconds



Average Time to Delete an Account
15+ minutes

Based on a Consumer Reports survey of six popular websites: Google, Walgreens, Instagram, Groupon, Pizza Hut, and Sirius XM.⁶¹ Walgreens allowed consumers to delete some of their data but did not allow consumers to delete their usernames or email addresses. SiriusXM did not allow consumers to delete their location data or their accounts. Instagram and Groupon imposed a delay period prior to deleting the account—thirty days for Instagram, two for Groupon—that are not included in the average account-deletion time. Only one of the six companies surveyed—Google—did not require significantly extra time to delete an account than to create one.

Another study from a team of researchers at Princeton University attempted to quantify the pervasiveness of dark pattern techniques by surveying a large sample (around 11,000 websites) of e-commerce platforms.⁶² The authors identified 1,818 instances of dark patterns on shopping websites, which appeared on 1,254 of the sites (around 11% of those surveyed).⁶³ These dark patterns included immortal accounts, referred to as accounts that are “hard to cancel” in the study, in addition to other types of misdirection.⁶⁴ The authors emphasized that their numbers represent a “lower bound” of the total number of dark patterns on these websites due to methodological limitations.⁶⁵

These pervasive dark patterns can create significant pecuniary harms for consumers. For instance, these same Princeton University researchers found that more often than not, shopping websites did not disclose to users that the process for canceling a subscription or membership is far more complicated than the process for signing up for the subscription or membership.⁶⁶ This is consistent with the FTC’s finding that “[o]ver the years, unfair or deceptive negative option practices have remained a persistent source of consumer harm, often saddling shoppers with recurring payments for products and services they did not intend to purchase or did not want to continue to purchase.”⁶⁷ Apart from direct charges, consumer time and effort is spent in trying to cancel an account, and consumers who are unable to delete their data from a particular platform face the risks associated with a potential data breach. The potential for personal data to be implicated

⁶¹ See Thomas Germain, *Saying Goodbye: Tips for Closing Hard-to-Delete Online Accounts*, Consumer Reports (Aug. 9, 2021), <https://www.consumerreports.org/digital-security/tips-for-closing-hard-to-delete-online-accounts-a6499479986/>. The authors of this report calculated averages using the data from this article.

⁶² Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 *PROC. ACM HUMAN-COMPUT. INTERACT.* 1, 2 (2019).

⁶³ *Id.*

⁶⁴ *Id.* at 12, 21–22.

⁶⁵ *Id.* at 2.

⁶⁶ *Id.* at 21.

⁶⁷ Enforcement Policy Statement, 86 Fed. Reg. at 60,823.

in a data breach can be far-ranging. For example, a 2019 Capital One data breach included personal information from credit card applications dating back to 2005.⁶⁸

Immortal accounts also result in further harms to free will and privacy.⁶⁹ Clearly, a consumer who tries to cancel an account and finds her path obstructed would directly experience a loss of free will. Beyond that, some dark patterns and other forms of online manipulation are effective because they make one's actions *appear* like an exercise of free will, thereby eroding a user's "decisional privacy," or internal decision-making process.⁷⁰ For immortal accounts, this may apply where a consumer believes she has exercised her free will by deleting an account and all of its data, when in fact the entity has retained the consumer's data.

Moreover, so long as immortal account practices allow entities to retain data against a consumer's preferences, that consumer's privacy is diminished. Online entities gather massive amounts of data from their users, and some entities, including internet service providers, retain data for years.⁷¹ The FTC has previously recognized the substantial harm to consumers from the collection and sharing of such data when it pursued enforcement action against Vizio for tracking consumers' viewing activity.⁷² The FTC has also signaled its interest in protecting users' decisional privacy, noting that remedial action was warranted against Facebook in the Cambridge Analytica case because "Facebook undermined consumers' choices."⁷³

Finally, academics have increasingly underscored the harms to dignity and autonomy potentially resulting from dark patterns, including immortal accounts. In the context of data breaches, one paper evaluated liberty, privacy, and dignity as values in American law that derive from the concept of autonomy.⁷⁴ The author argued that a loss of control over personally identifiable information, such as that caused by a data breach, creates a "loss of negative freedom [that] manifests in feelings of anxiety, vulnerability, and distress," even when the information has not been used to commit identity theft.⁷⁵ Ultimately, the article argues that the FTC, with its authority to redress consumer harm that it is widely felt, should regulate dark patterns based on the harm to one's dignity resulting from the appropriation of personal information.⁷⁶

⁶⁸ Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, N.Y. TIMES (July 29, 2019), <https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html>.

⁶⁹ Gregory Day & Abbey Stemler, *Are Dark Patterns Anticompetitive?*, 72 ALA. L. REV. 1, 4 (2020).

⁷⁰ *Id.*

⁷¹ FED. TRADE COMM'N, A LOOK AT WHAT ISPS KNOW ABOUT YOU: EXAMINING THE PRIVACY PRACTICES OF SIX MAJOR INTERNET SERVICE PROVIDERS 31–33 (2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

⁷² Complaint, Fed. Trade Comm'n v. Vizio, Inc., No. 2:17-cv-00758 (D.N.J., Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf. This lawsuit resulted in a \$2.2 million settlement. Press Release, *VIZIO to Pay \$2.2 Million to FTC, State of New Jersey to Settle Charges it Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, FED. TRADE COMM'N (Feb. 6, 2017), <https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million>.

⁷³ Press Release, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions> (quoting then-FTC Chairman Joe Simons).

⁷⁴ George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 WAKE FOREST L. REV. 1, 6–7 (2016).

⁷⁵ *Id.* at 56.

⁷⁶ *Id.* at 44–56.

II. Immortal Accounts Fall Squarely Within the FTC’s Authority to Regulate Deceptive, Unfair, and Anticompetitive Trade Practices

Under the FTCA, the FTC is the primary government agency entrusted with preventing deceptive and unfair trade practices and, along with the Justice Department, unfair methods of competition.⁷⁷ The FTC envisions a “vibrant economy characterized by vigorous competition and consumer access to accurate information.”⁷⁸ To achieve that vision, the Commission should take action to regulate immortal accounts. It has three distinct sources for doing so: under Section 5 of the FTCA, immortal accounts are deceptive, unfair to consumers, and an unfair method of competition.⁷⁹

A. The Use of Immortal Accounts Constitutes a Deceptive Practice Within the Meaning of Section 5 of the FTCA

To justify rulemaking under Section 5(a), the FTC must make three findings: “(1) there is a representation, omission, or practice that,” (2) “is likely to mislead consumers acting reasonably under the circumstances,” and (3) “the representation, omission, or practice is material.”⁸⁰ As detailed below, immortal accounts satisfy each of these elements. This section tackles the first two prongs together, and then explains how immortal accounts satisfy the standard’s third prong.

i. *Immortal Accounts Involve Misrepresentations, Misleading Omissions, and/or Deceptive Practices*

The immortal account practices employed by entities to obstruct account deletion meet the first two elements required to invoke the FTC’s authority under Section 5(a). A practice will be considered likely to mislead if the “net impression” created by the representation or omission is likely to mislead the consumer.⁸¹ This means that the Commission may regulate if a significant minority of reasonable consumers are likely to perceive the representation or omission as misleading.⁸² Further, the Commission considers a practice in its totality when determining how reasonable consumers are likely to respond.⁸³ The FTC does not need to show that the entity intended for the practice to deceive; rather, the Commission must only show that the “overall net impression” of the communication is misleading.⁸⁴ Immortal accounts, in their totality, are likely to mislead consumers acting reasonably.

⁷⁷ 15 U.S.C. § 45(a)(2) (“The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.”).

⁷⁸ *About the FTC*, FED. TRADE COMM’N, <https://www.ftc.gov/about-ftc> (last visited May 17, 2022).

⁷⁹ See 15 U.S.C. § 45(a).

⁸⁰ Fed. Trade Comm’n v. Stefanchik, 559 F.3d 924, 928 (9th Cir. 2009); see also FED. TRADE COMM’N, FTC POLICY STATEMENT ON DECEPTION (1983) (appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984)), <http://ftc.gov/bcp/policystmt/ad-decept.htm> [hereinafter “Deception Policy Statement”].

⁸¹ Fed. Trade Comm’n v. Cyberspace.com LLC, 453 F.3d 1196, 1200 (9th Cir. 2006).

⁸² Fanning v. Federal Trade Comm’n, 821 F.3d 164, 170 (1st Cir. 2016).

⁸³ Deception Policy Statement, *supra* note 80, at 5.

⁸⁴ Fed. Trade Comm’n v. E.M.A. Nationwide, Inc., 767 F.3d 611, 631 (6th Cir. 2014).

Consumers have a reasonable expectation that they will be able to cancel an account they have created.⁸⁵ When a consumer encounters dark pattern practices such as visually inconspicuous text, difficult-to-locate menus and settings, confusing prompts, and other practices that meaningfully obstruct account deletion, the consumer’s reasonable expectations are frustrated. Much like prior FTC enforcement actions recognized that unreasonable barriers to canceling an account during a free trial period are a deceptive practice,⁸⁶ unreasonable barriers to canceling any account, whether paid or not, constitutes a practice likely to mislead consumers acting reasonably.

This reasonable expectation applies at the time of account creation—and thus cannot simply be solved by informing consumers that their account cannot be closed after that account has already been created. For example, a study of consumer expectations found that 48% of respondents believed Amazon Echo users could delete voice data whenever they chose and another 21% believed such data was automatically deleted.⁸⁷ This study found similar attitudes towards Facebook facial recognition technology—44% believed users could delete data and 21% believed data deleted automatically.⁸⁸ Given the hypothetical framing of the study’s survey questions, a consumer’s expectation that she will be able to delete her account data is likely present at the time of account creation.

Immortal accounts that retain user data after account deletion may, in particular, operate on the basis of misrepresentations or misleading omissions. The FTC defines a misrepresentation as “an express or implied statement contrary to fact” and a misleading omission as the non-disclosure of “qualifying information necessary to prevent a practice, claim, representation, or reasonable expectation or belief from being misleading.”⁸⁹ Therefore, because consumers reasonably expect to be able to delete their personally-identifiable account data,⁹⁰ an entity that fails to clearly disclose that account information will be retained beyond account deletion commits a misleading omission. Relatedly, an entity that represents to a consumer at the time of account cancellation—either expressly or by implication—that it has deleted the consumer’s account information, when in fact it has retained that information, commits a misrepresentation.

ii. *The Misleading Omissions and Representations Are Material*

The deceptive practices, misrepresentations and misleading omissions regarding account deletion and retained information are material and thus actionable under the FTCA. Materiality is established when the information presented or omitted “is important to consumers, and hence, likely to affect their choice of, or conduct regarding, a product.”⁹¹ The Commission considers “claims or omissions material if they significantly involve health, safety, or other areas with which the reasonable consumer would be concerned,” including information that “concerns the . . . cost[] of the product or service.”⁹² Additionally, materiality can be established by a reliable survey of consumers or credible testimony.⁹³

⁸⁵ *Cf.* 15 U.S.C. § 8401(8) (recognizing “consumers’ expectations that they would have an opportunity to accept or reject” membership following completion of trial period).

⁸⁶ *See, e.g.*, First Amended Complaint, Fed. Trade Comm’n v. Universal Premium Services, No. CV06-0849, at 13–14 (C.D. Cal. 2006), <https://www.ftc.gov/sites/default/files/documents/cases/2006/05/060509famndcmplt0523153.pdf>.

⁸⁷ Lior Jacob Strahilevitz & Jamie Luguri, *Consumertarian Default Rules*, 82 *LAW & CONTEMP. PROBS.* 139, 150 (2019).

⁸⁸ *Id.* at 151. 34% of respondents also believed users could delete location data from Google maps, but the paper did not specify what percentage of respondents believed this process was automatic. *Id.* at 152. In all three scenarios, the majority of respondents normatively believed the companies should not be able to retain these data sets in the first place. *Id.* at 150–52.

⁸⁹ Deception Policy Statement, *supra* note 80, at 7.

⁹⁰ *See supra* notes 87–89 and accompanying text.

⁹¹ *Cyberspace.com LLC*, 453 F.3d at 1201.

⁹² Deception Policy Statement, *supra* note 80, at 5.

⁹³ *Id.*

A misrepresentation or omission regarding the consumer’s ability to cancel her account or control her personal data meets this standard. For one, insofar as difficult account-deletion practices cause consumers to incur additional recurring charges, those additional fees clearly meet the standard for materiality. Indeed, one recent study found that cost is “the most influential decision driver, with nearly half of the respondents [in the survey] considering it as one of the top three factors for selecting a product or service.”⁹⁴ The FTC has recognized product price as an example of a material term,⁹⁵ and the agency has successfully pursued enforcement actions when price was misrepresented.⁹⁶ Deceptive practices that make account deletion unreasonably difficult or impossible increase the cost to the consumer and thus satisfy the materiality prong.

Even where consumer cost is not involved, deceptive practices that deprive consumers of autonomy over their personal data and information are nonetheless material. Americans believe their personal information is valuable and care how it is used by others.⁹⁷ Surveys have shown that consumers are concerned with the protection of their personal information and feel as if they have no control over who can access it.⁹⁸ According to a study from the Pew Research Center, more than 80% of those surveyed said that the potential risks they face because of data collection by companies outweigh the benefits.⁹⁹ Additionally, this study found that 79% of Americans are concerned about the way that their data is being used by companies.¹⁰⁰ Moreover, 79% of Americans say they are not too or at all confident that companies will admit mistakes and take responsibility if they misuse or compromise personal information and 69% report this same lack of confidence that businesses will use their personal information in ways that they will be comfortable with.¹⁰¹

In short, immortal account practices satisfy all three prongs of the test to constitute a deceptive trade practice. Because immortal accounts involve material representations and omissions that mislead reasonable consumers, the FTC should issue a rule regulating this practice under its deceptive-practices authority.

B. The Use of Immortal Accounts Constitutes an Unfair Practice Within the Meaning of Section 5 of the FTCA

The FTC also has the authority to regulate immortal accounts as an unfair act or practice under Section 5 of the FTCA.¹⁰²

Under the FTCA, a practice is unfair if it (1) “causes or is likely to cause substantial injury to consumers,” (2) “which is not reasonably avoidable by consumers themselves,” and is (3) “not outweighed by countervailing benefits to consumers or to competition.”¹⁰³ In determining whether an act or practice is unfair, the Commission may also consider established

⁹⁴ Indika Jayasinghe, *Consumer Decision Making Criteria and the Importance of Price*, MEDIUM (Oct. 24, 2016), <https://medium.com/stax-insights/consumer-decision-making-criteria-and-the-importance-of-price-1783d5589a8e>.

⁹⁵ Deception Policy Statement, *supra* note 80, at 5.

⁹⁶ *See, e.g., Resort Car Rental Sys., Inc. v. Fed. Trade Comm’n*, 518 F.2d 962, 964 (9th Cir. 1975).

⁹⁷ *See* Angela G. Winegar & Cass R. Sunstein, *How Much Is Data Privacy Worth? A Preliminary Investigation*, 42 J. CONSUMER POL’Y 425 (2019).

⁹⁸ Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

¹⁰² 15 U.S.C. § 45(a)(2).

¹⁰³ 15 U.S.C. § 45(n).

public policies such as those set forth by statute, common law, industry practice, or otherwise.¹⁰⁴ Finally, any analysis should be guided by the primary purpose of the Commission’s unfairness authority, which “continues to be to protect consumer sovereignty by attacking practices that impede consumers’ ability to make informed choices.”¹⁰⁵

Because immortal accounts meet all three prongs of the unfairness test, they accordingly constitute an unfair practice under Section 5(a) of the FTCA.

i. Immortal Accounts Cause Substantial Injuries to Consumers

Immortal accounts meet the first prong of the unfairness test, as potential monetary costs, search costs, and the cost of loss of control over personal data substantially injure consumers. There are several types of injury that may support this prong of the FTC’s unfairness authority. First, the FTC’s 1980 Policy Statement on Unfairness states that often, but not always, substantial injury comes in the form of monetary harm.¹⁰⁶ The facts of *ABCmouse* establish that immortal accounts can exact monetary injury on users when subscriptions that are impossible or difficult to cancel incur automatic charges.¹⁰⁷ Relatedly, because immortal accounts leave users’ personal data in the hands of another entity, injury can be tied to susceptibility to identity theft and other monetary harms arising from data breaches, internal misuse of data, or unwanted secondary uses of information.¹⁰⁸

There are also numerous non-monetary harms posed by immortal accounts. For one, reviewing courts have recognized the investment of time as a harm for users.¹⁰⁹ Where an account is difficult to cancel and a user must engage in onerous steps or resort to outside research to aid in cancelling an account, that user has suffered a loss of time. Another type of injury is the violation of one’s right to control one’s own personal data, which the Executive Office of the President recognized as essential in 2012 in its Privacy Bill of Rights.¹¹⁰ As previously mentioned, studies show that users value their personal data,¹¹¹ and their inability to permanently delete an account to prevent an entity’s use of their personal data against their wishes imposes an injury on those users. Similarly, the concerns of general surveillance and a loss of autonomy in commercial interactions are injuries that were highlighted as pernicious by the Department of Commerce’s National Institute of Standards and Technology and could also be applicable in the immortal accounts context.¹¹²

When users are unable to delete their accounts, e-commerce platforms maintain control over their personally-identifiable data, and thus have continuing access to personal information that users would prefer they not have; it is thus both the lack of control and the lack of privacy that harms the user. The FTC has demonstrated interest in protecting users’

¹⁰⁴ *Id.*; FED. TRADE COMM’N, FTC POLICY STATEMENT ON UNFAIRNESS (Dec. 17, 1980) (appended to *International Harvester Co.*, 104 F.T.C. 949, 1070 (1984)), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness> [hereinafter “Unfairness Policy Statement”].

¹⁰⁵ J. Howard Beales, *The FTC’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FED. TRADE COMM’N (May 30, 2003), <https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection>.

¹⁰⁶ Unfairness Policy Statement, *supra* note 104.

¹⁰⁷ See *Age of Learning, Inc.*, No. 2:20-cv-07996.

¹⁰⁸ Comments of the Center for Democracy & Technology, *supra* note 7, at 2.

¹⁰⁹ See, e.g., *Fed. Trade Comm’n v. Amazon.com, Inc.*, No. C14-1038-JCC, 2016 U.S. Dist. LEXIS 55569, at *12–13 (W.D. Wash. Apr. 26, 2016); *Fed. Trade Comm’n v. Neovi, Inc.*, 604 F.3d 1150, 1158 (9th Cir. 2010).

¹¹⁰ THE EXECUTIVE OFFICE OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf> [hereinafter “Privacy Bill of Rights”].

¹¹¹ See Auxier et al., *supra* note 98; Winegar & Sunstein, *supra* note 97.

¹¹² SEAN BROOKS ET AL., AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS 10 (Jan. 2017), <http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>.

control over their personal information, and recognized that a lack of control presents a legitimate harm to users.¹¹³ Additionally, the FTC stated in an enforcement action against Vizio that “collection and sharing of sensitive data without consumers’ consent has caused or is likely to cause substantial injury to consumers.”¹¹⁴ As this finding demonstrates, the practice of retaining data against a consumer’s wishes by making account deletion unreasonably difficult or impossible also causes substantial consumer injury.

Importantly, under Section 5(a) injury can be substantial by doing “small harm to a large number of people.”¹¹⁵ The use of immortal accounts meets the test for substantial injury under this standard, demonstrated by the extent to which experts have documented the pervasiveness of immortal accounts. In one study (previously discussed in Section I) that surveyed approximately 11,000 e-commerce platforms, the authors identified 1,818 instances of dark patterns—including immortal accounts—on 1,254 of the sites assessed (around 11%).¹¹⁶ Shopping websites that were more popular according to Amazon Alexa rankings were more likely to feature dark patterns.¹¹⁷ The authors emphasized that their numbers represented a lower bound on the total number of dark patterns on these websites due to limitations in their methodology.¹¹⁸ Thus, consumers who interact with a broad base of e-commerce platforms are likely to encounter immortal accounts, further evincing the prevalence of consumer injury.

ii. *The Consumer Harms from the Use of Immortal Accounts Are Not Reasonably Avoidable*

Immortal accounts meet the second prong of the unfairness test, as consumers cannot reasonably avoid the harm associated with this dark pattern. A practice is not reasonably avoidable if a consumer does not have a free and informed choice.¹¹⁹ In contrast, injury is reasonably avoidable if consumers “have reason to anticipate the impending harm and the means to avoid it, or if consumers are aware of, and are reasonably capable of pursuing, potential avenues toward mitigating the injury after the fact.”¹²⁰

Immortal accounts cannot be reasonably avoided because consumers are typically not provided with advance notice regarding the difficulty (or impossibility) of deleting their account and account data. Even when a consumer generally expects that account deletion will be more difficult than account creation, in the case of immortal accounts, she may underestimate the amount of time and effort required for deletion.¹²¹ Furthermore, while some studies have compiled lists of entities that use immortal accounts, a consumer may not reasonably use these to avoid harm because such lists may be difficult for consumers to locate, hardly cover the total range of entities, and may not be regularly updated to reflect the current practices of any particular entity.¹²² A consumer who does not realize she is signing up for an account that will be difficult or impossible to cancel cannot reasonably avoid the harm from the immortal account before signing up for an account.

¹¹³ See Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm’n v. Frostwire LLC, 2011 WL 9282853 (S.D. Fla. 2011) (alleging unfair and deceptive practices when an app eroded users’ control over the privacy settings of their files, which could be shared with strangers by default).

¹¹⁴ Complaint at 9, *Vizio*, *supra* note 72.

¹¹⁵ *Neovi, Inc.*, 604 F.3d at 1157 (internal quotation marks and citations omitted).

¹¹⁶ Mathur et al., *supra* note 62, at 2.

¹¹⁷ *Id.*

¹¹⁸ *Id.* at 6.

¹¹⁹ *Neovi, Inc.*, 604 F.3d at 1158.

¹²⁰ *Davis v. HSBC Bank*, 691 F.3d 1152, 1168–69 (9th Cir. 2012) (internal quotation marks omitted).

¹²¹ See, e.g., LILI LÁNG & PAULA DANA PUDANE, DECEPTIVE INTERFACES: A CASE STUDY ON AMAZON’S ACCOUNT DELETION NAVIGATION AND ITS EFFECTS ON USER EXPERIENCE 15 (2019), <https://www.diva-portal.org/smash/get/diva2:1315156/FULLTEXT01.pdf>.

¹²² See, e.g., JUSTDELETE.ME, <https://backgroundchecks.org/justdeleteme/> (last visited Apr. 26, 2022); Thomas Germain, *Saying Goodbye: Tips for Closing Hard-to-Delete Online Accounts*, CONSUMER REPORTS (Aug. 9, 2021), <https://www.consumerreports.org/digital-security/tips-for-closing-hard-to-delete-online-accounts-a6499479986/>.

Moreover, while the use of immortal accounts often enables users to cancel their account after expending considerable time and effort, even in that case the time that the consumer spends to cancel her account cannot be reasonably avoided. For example, in *FTC v. Amazon.com*, Amazon claimed that consumers could reasonably avoid an injury from in-app purchases by seeking a refund. The U.S. District Court for the Western District of Washington rejected this claim, finding that the time that consumers spent seeking the refund constituted an injury in and of itself.¹²³ Likewise, the time that consumers spend seeking to cancel an account constitutes an unavoidable injury when the entity has intentionally made the cancellation process difficult and time-consuming through the use of immortal accounts.

iii. The Substantial Injuries Are Not Offset by Countervailing Benefits

To the consumer, immortal accounts have limited countervailing benefits that offset the injuries they cause. In considering offsetting benefits, the FTC looks to the “the costs of imposing a remedy” and “any benefits that consumers enjoy as a result of the practice, such as the avoided costs of more stringent authorization procedures and the value of consumer convenience.”¹²⁴ In the case of immortal accounts, there is no immediate countervailing benefit to a consumer subscribing to a service they no longer desire. By definition, immortal accounts prevent or obstruct users from achieving their desired end. Furthermore, immortal accounts waste consumers’ time and energy by forcing them to navigate onerous obstacles to account deletion.

Broadly, the oversharing of data could benefit the consumer in a few ways: the collection of data fuels an ad-supported internet model, where consumers do not need to pay a fee to use services and may be targeted by ads for relevant products because websites sell consumer data to third parties; certain services, like Google Maps, are made possible by data collection; and, users may be able to use personal data to prevent fraud and verify identities.¹²⁵ However, it is crucial to distinguish between regulating an entity’s use of dark patterns, such as immortal accounts, and regulating data collection in its entirety. Entities need not rely on immortal accounts to use or sell data, as they have access to the data from all of the active accounts to which users consent. Moreover, this report recommends that the FTC issue a rule that extends only to data that reasonably identifies a particular consumer. That is, entities could continue to use data that has been de-identified or anonymized, and those entities and their customers would continue to derive benefit from the use of such de-identified data. Accordingly, the consumer benefits described above would exist in the absence of immortal accounts.

Notably, consumers themselves recognize that just some of the harms from immortal accounts outweigh the potential benefits. An overwhelming majority of individuals—more than 80%—concluded that the potential risks they face from data collection outweigh the benefits, as reported in a study from the Pew Research Center.¹²⁶

iv. Established Public Policy Supports an Unfairness Determination

The FTC should consider established public policies as evidence to be considered with all other evidence, and those public policies largely support the regulation of immortal accounts. In looking at sources of public policy, the Commission can first look to the CCPA, which establishes a right for consumers to have their data deleted and generally enshrines user consent and autonomy in interactions with e-commerce platforms.¹²⁷ Similarly, the Colorado Privacy Act

¹²³ *Amazon.com*, 2016 U.S. Dist. LEXIS 55569 at *21.

¹²⁴ Beales, *supra* note 105.

¹²⁵ FED TRADE COMM’N., FTC INFORMATIONAL INJURY WORKSHOP: BE AND BCP STAFF PERSPECTIVE 3 (2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

¹²⁶ See *supra* notes 98–101 and accompanying text.

¹²⁷ Cal. Civ. Code § 1798.105.

and Virginia’s Consumer Data Protection Act include a consumer’s right to delete personal data.¹²⁸ The GDPR, with its emphasis on privacy protections and consumer control over data, shows that these values are gaining a strong foothold not only domestically, but also internationally. Furthermore, previous administrations have signaled their interest in championing consumer control over data, as evidenced by President Obama’s Privacy Bill of Rights.¹²⁹ Thus, this growing recognition of the importance of consumer privacy and autonomy should be taken into account in determining the severity of the harms imposed on consumers.

C. The Use of Immortal Accounts Constitutes an Unfair Method of Competition Within the Meaning of Section 5 of the FTCA

The FTC can also regulate immortal accounts under its authority to proscribe unfair methods of competition. This authority is not limited to violations of other antitrust laws, but also encompasses a broader range of anticompetitive conduct.¹³⁰ The Supreme Court has held that the Commission can consider “public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws.”¹³¹

To determine whether a method of competition is unfair, courts analyze whether the method “casts upon one’s competitors the burden of the loss of business unless they will descend to a practice which they are under a powerful moral compulsion not to adopt, even though it is not criminal,” and “involve[s] the kind of unfairness at which the statute was aimed.”¹³² In the analysis, it is unnecessary to show specific losses to any one company in order to establish a practice as an unfair method of competition.¹³³ Instead, it is sufficient to show that the practice in question unfairly burdens competition for a not insignificant volume of commerce.¹³⁴

Considering our ad-supported internet model, which makes the overcollection of data extremely valuable for online businesses, refraining from practices that increase the amount of data collected, such as the use of immortal accounts, is likely to harm an individual marketplace actor. Commentators have explained that there is currently “an imperfect market where companies do not compete based on privacy given their aligned interest to acquire as much personal information of consumers as possible. This leads to a race to the bottom in terms of privacy protection.”¹³⁵ This hypothesis is strengthened by studies that show that shopping websites that are more popular are also more likely to feature dark patterns.¹³⁶ Such a finding signals that even popular and successful e-commerce platforms resort to the use of dark patterns, including immortal accounts, to compete with their peers in profiting from the unwanted use of consumer data.

¹²⁸ Colo. Rev. Stat. § 6-1-1306(1)(d); Va. Code Ann. § 59.1-577(A)(3).

¹²⁹ Privacy Bill of Rights, *supra* note 110.

¹³⁰ FED. TRADE COMM’N, STATEMENT OF CHAIR LINA M. KHAN JOINED BY COMMISSIONER ROHIT CHOPRA AND COMMISSIONER REBECCA KELLY SLAUGHTER ON THE WITHDRAWAL OF THE STATEMENT OF ENFORCEMENT PRINCIPLES REGARDING “UNFAIR METHODS OF COMPETITION” UNDER SECTION 5 OF THE FTC ACT 2–4 (2021), https://www.ftc.gov/system/files/documents/public_statements/1591498/final_statement_of_chair_khan_joined_by_rc_and_rks_on_section_5_0.pdf; *see also* Commissioner J. Thomas Rosch, Remarks at Federal Trade Commission Workshop on Section 5 of the FTC Act as a Competition Statute, Transcript at 137 (Oct. 17, 2008) (transcript available at <http://www.ftc.gov/bc/workshops/section5/transcript.pdf>) (“[*Sperry & Hutchinson*], in my judgment, is alive and well, notwithstanding the trilogy of appellate cases decided in the early ‘80s, that rejected the Commission’s decisions challenging conduct as unfair methods of competition under Section 5.”); Commissioner Jon Leibowitz, Remarks at Federal Trade Commission Workshop on Section 5 of the FTC Act as a Competition Statute, Transcript at 208 (Oct. 17, 2008) (transcript available at <http://www.ftc.gov/bc/workshops/section5/transcript.pdf>) (discussing Supreme Court precedents and concluding “that the FTC Act goes well beyond the metes and bounds of the Sherman Act”).

¹³¹ Fed. Trade Comm’n v. *Sperry & Hutchinson Co.*, 405 U.S. 233, 244 (1972).

¹³² Fed. Trade Comm’n v. *R.F. Keppel & Bro., Inc.*, 291 U.S. 304, 313 (1934).

¹³³ Fed. Trade Comm’n v. *Raladam Co.*, 316 U.S. 149, 152 (1942).

¹³⁴ Fed. Trade Comm’n v. *Texaco, Inc.*, 393 U.S. 223, 230 (1968).

¹³⁵ Christine Lyon & Lokke Moerel, *Why Placing a Price Tag on Personal Data May Harm Consumer Privacy*, IAPP (July 21, 2020), <https://iapp.org/news/a/why-placing-a-price-tag-on-personal-data-may-harm-consumer-privacy/>.

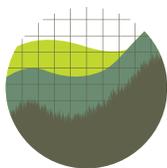
¹³⁶ Mathur et al., *supra* note 62, at 2.

Companies that do not resort to dark pattern tactics stand to suffer a disadvantage when compared to their competitors that do use them, given the overall efficacy of these techniques from a data-collection perspective. As discussed above, dark patterns—such as immortal accounts—are extremely effective at extracting data from consumers, due to their ability to exploit human psychological systems.¹³⁷ Thus, a platform that refrains from using immortal accounts misses out on a highly powerful data-collection tool that bestows advantages (for example, monetary profit in both recurring fees and selling data to third parties) to those peer platforms that do use them.

Conclusion

The FTC has signaled its willingness to strengthen privacy regulation, especially with regards to dark patterns. Regulation of immortal accounts, which create considerable consumer harms, should be a priority within an enhanced privacy regulatory framework. An FTC rule that focuses on clear guidelines for reasonable account deletion practices would fall squarely within the FTC’s authority and support its mission to protect consumers from deceptive, unfair, and anticompetitive practices.

¹³⁷ See *supra* Section I for discussion of the efficacy of dark patterns.



Institute *for*
Policy Integrity

NEW YORK UNIVERSITY SCHOOL OF LAW

Institute for Policy Integrity
New York University School of Law
Wilf Hall, 139 MacDougal Street, New York, New York 10012
policyintegrity.org