Regulating Immortal Accounts

How the FTC Can Limit Unwanted Data Retention

May 2022
Laura A. Figueroa
Max Sarinsky
Rayne Ellis
Emma Schwartz
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. She then expressed her belief that the Commission should “approach data privacy and security protections by considering substantive limits rather than just procedural protections.”

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 entities obstruct the process for deleting a consumer account or do not provide any account deletion option at all. Some entities might even trick a user into believing an account was entirely deleted, when in reality the data from that account was maintained. 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.

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. 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.

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:

---

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).
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. 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.

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. 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.” 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. 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” which are “not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” 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.

---

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

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

I. Immortal Accounts Harm and Unduly Burden Consumers

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

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

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

      ii. The Misleading Omissions and Representations Are Material

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

      i. Immortal Accounts Cause Substantial Injuries to Consumers

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

      iii. The Substantial Injuries Are Not Offset by Countervailing Benefits

      iv. Established Public Policy Supports an Unfairness Determination

   C. Immortal Accounts Constitute an Unfair Method of Competition Within the Meaning of Section 5 of the FTCA

Conclusion
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. The FTC alleged that ABCmouse had committed unfair and deceptive trade practices. 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.

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. 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.

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

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.” Panelists discussed various types of dark patterns, how they affect consumers, and how they should be combated. One panelist highlighted immortal accounts as an example of dark patterns that erode users’ control over their own data. 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.

These statements were followed by new FTC enforcement guidance for negative option marketing published in November 2021. 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.” 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 FTC Act, “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.” Apart from this new guidance, the FTC also signaled in late 2021 that it is considering initiating rulemaking to “limit privacy abuses.”

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]”

---

25 Id. at 5.
27 Id.
29 Id., Transcript at 84 (statement of Daniel Kaufman).
32 Id. at 60,822.
33 Id. at 60,823–24.
actively making it arduous for consumers to cancel through clever uses of font and color on its website.” The District of Columbia also sued Grubhub and Google this year for allegedly using dark patterns in their services. The separate complaints allege that Grubhub charged hidden fees for food delivery 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).”

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. 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. The CCPA also provides consumers the right to request the deletion of personal information and obligates businesses to fulfill such requests. 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. 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.”

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. 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.” 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,
and lack of valid consent in its ad personalization tool. 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.

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. 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, there are several proposed bills that address these topics. For example, the Deceptive Experiences To Online Users Reduction Act (“DE-TOUR 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.” 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. 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. As these so-far unsuccessful attempts at legislation illustrate, there is a demand for regulation of data privacy that has not yet been fulfilled.

47 Id.
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.
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. 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. 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.” 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.” 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. 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.

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. 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.

---

53 Statement Regarding Dark Patterns, supra note 11, at 2.
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).
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. 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). 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. The authors emphasized that their numbers represent a “lower bound” of the total number of dark patterns on these websites due to methodological limitations.

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. 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.” 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

63 Id.
64 Id. at 12, 21–22.
65 Id. at 2.
66 Id. at 21.
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


70 Id.


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.\textsuperscript{77} The FTC envisions a “vibrant economy characterized by vigorous competition and consumer access to accurate information.”\textsuperscript{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.\textsuperscript{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.”\textsuperscript{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.\textsuperscript{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.\textsuperscript{82} Further, the Commission considers a practice in its totality when determining how reasonable consumers are likely to respond.\textsuperscript{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.\textsuperscript{84} Immortal accounts, in their totality, are likely to mislead consumers acting reasonably.

\textsuperscript{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.”).


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

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

\textsuperscript{83} Deception Policy Statement, supra note 80, at 5.

\textsuperscript{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. 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, 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. This study found similar attitudes towards Facebook facial recognition technology—44% believed users could delete data and 21% believed data deleted automatically. 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.” Therefore, because consumers reasonably expect to be able to delete their personally-identifiable account data, 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.” 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.” Additionally, materiality can be established by a reliable survey of consumers or credible testimony.

---

85 C.f. 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).
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.” The FTC has recognized product price as an example of a material term, and the agency has successfully pursued enforcement actions when price was misrepresented. 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. 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. 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. Additionally, this study found that 79% of Americans are concerned about the way that their data is being used by companies. 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.

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.

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.” In determining whether an act or practice is unfair, the Commission may also consider established

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).
99 Id.
100 Id.
101 Id.
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’

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.
111 See Auxier et al., supra note 98; Winegar & Sunstein, supra note 97.
control over their personal information, and recognized that a lack of control presents a legitimate harm to users. 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.” 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.” 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%). Shopping websites that were more popular according to Amazon Alexa rankings were more likely to feature dark patterns. 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. 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. 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.”

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. 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. 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).

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.


\(^{126}\) See *supra* notes 98–101 and accompanying text.

and Virginia’s Consumer Data Protection Act include a consumer’s right to delete personal data.\textsuperscript{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.\textsuperscript{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.

\section*{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.\textsuperscript{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.”\textsuperscript{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.”\textsuperscript{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.\textsuperscript{133} Instead, it is sufficient to show that the practice in question unfairly burdens competition for a not insignificant volume of commerce.\textsuperscript{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.”\textsuperscript{135} This hypothesis is strengthened by studies that show that shopping websites that are more popular are also more likely to feature dark patterns,\textsuperscript{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.

\begin{thebibliography}{99}
\bibitem{note129} Privacy Bill of Rights, \textit{supra} note 110.
\bibitem{note130} \textit{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), \url{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}; \textit{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 \url{http://www.ftc.gov/bc/workshops/section5/transcript.pdf}) (“\textit{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 \url{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”).
\bibitem{note131} Fed. Trade Comm’n v. Sperry & Hutchinson Co., 405 U.S. 233, 244 (1972).
\bibitem{note136} Mathur et al., \textit{supra} note 62, at 2.
\end{thebibliography}
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. 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 signalled 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.

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