

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF SOUTH CAROLINA  
COLUMBIA DIVISION

NETCHOICE, LLC,

*Plaintiff,*

v.

ALAN WILSON, in his official capacity as  
South Carolina Attorney General,

*Defendant,*

and

HENRY DARGAN MCMASTER, in his  
official capacity as Governor of the  
State of South Carolina,

*Intervenor-Defendant.*

Civil Action No.: 3:26-cv-543-sal

**RESPONSE TO  
MOTION FOR  
PRELIMINARY INJUNCTION**

Henry Dargan McMaster, in his official capacity as Governor of the State of South Carolina, and Alan Wilson, in his official capacity as South Carolina Attorney General, submit this response in opposition to NetChoice, LLC's Motion for Preliminary Injunction (ECF No. 22).

## TABLE OF CONTENTS

INTRODUCTION .....	1
STATEMENT OF THE CASE .....	2
A.    The South Carolina Social Media Regulation Act .....	2
B.    Procedural history .....	4
LEGAL STANDARD.....	4
ARGUMENT .....	5
I.    NetChoice is not likely to prevail on the merits.....	5
A.    NetChoice cannot show a substantial likelihood that it has standing.....	5
1.    NetChoice lacks associational standing .....	5
2.    NetChoice cannot assert the interests of its members’ users.....	8
B.    NetChoice is unlikely to prevail on its First Amendment claims .....	9
1.    NetChoice’s First Amendment claims fail based on the First Amendment’s original public meaning .....	9
2.    NetChoice’s First Amendment claims fail under means-end scrutiny .....	10
i.    Duty of “reasonable care” (§ 39-80-20(A)) .....	11
ii.   Personalization regulations (§§ 39-80-30(B), 39-80-40(F)) .....	16
iii.  Default requirements (§ 39-80-30(A), (C)).....	19
iv.  Reporting requirements (§§ 39-80-60(E), 39-80-70) .....	21
v.    Alleged censorship.....	21
C.    NetChoice is unlikely to prevail on its vagueness claims .....	22
1.    “Reasonable care” for “minors” .....	23
2.    “Harm” .....	25
3.    “Design features” .....	28
4.    “Expressed preferences” .....	30

5. “Dark patterns” ..... 31

6. “Personal data” ..... 33

D. NetChoice is unlikely to prevail on its preemption claims ..... 33

1. Section 230 does not preempt the Act ..... 33

2. COPPA does not preempt the Act..... 38

E. NetChoice is unlikely to prevail on its Commerce Clause claim ..... 40

F. NetChoice is unlikely to prevail on its due process claim ..... 42

II. The other factors do not support granting a preliminary injunction ..... 43

A. NetChoice will not suffer irreparable harm ..... 43

B. The remaining factors cut against an injunction..... 44

III. NetChoice seeks relief the Court cannot grant..... 45

CONCLUSION ..... 45

## INTRODUCTION

The internet has become the “modern public square.” *Packingham v. North Carolina*, 582 U.S. 98, 107 (2017). But this square is more dangerous for children than the traditional one. So governments have been working for decades to protect children from these new threats.

The South Carolina Social Media Regulation Act marks the latest such effort. As the Governor noted in signing it into law, the Act “provide[s] parents with critical tools to protect their children from the harmful effects of excessive social media use and their children’s privacy online.” Governor’s Signing Statement (Feb. 5, 2026). The Act—which the General Assembly passed unanimously—creates common-sense, straightforward rules for covered online services that will help parents protect their children. Who could be against that?

Giant Internet companies. That’s who. Through their trade association, NetChoice, they challenged this Act. That alone is a problem, as NetChoice lacks associational standing. NetChoice brings claims that typically require individualized consideration (that is, things that aren’t facial claims), but associational standing typically doesn’t work for as-applied claims.

But even if NetChoice could get over its standing problems, it has not shown that it’s likely to prevail on the merits. Some problems pervade NetChoice’s arguments. For instance, its generalized arguments fall far short of what *Moody v. NetChoice, LLC*, 603 U.S. 707 (2024), requires for facial challenges—a theme throughout its motion. And NetChoice repeatedly fails to develop arguments about specific members that are necessary for as-applied challenges. Speaking of not developing arguments, NetChoice objects to many parts of the Act, but it frequently doesn’t fully work out why it says those parts are problematic. It just throws out a hypothetical or two and then cites a case. And on the subject of citations, NetChoice points to a lot of cases it has litigated across the country, but it doesn’t cite many of the more recent decisions that cut against it.

On top of these problems, NetChoice’s merits arguments are unpersuasive. The First Amendment isn’t often implicated by the Act, which generally regulates conduct, not speech. But even if traditional means-end scrutiny applied, NetChoice’s tailoring analysis undersells the Act’s impact and overstates any burdens. Its scattershot vagueness claims turn largely on misreading the Act, while ignoring critical parts of jurisprudence. Its preemption claims identify nothing in the Act that would be an obstacle to the purposes of section 230 or COPPA. Its Commerce Clause claim would impose a per se rule to bar States from any sort of internet regulation, but the Supreme Court has rejected that logic because of our interconnected economy. And its due process claim just asks the Court to pause (or better yet, enjoin) the Act’s effectiveness until NetChoice’s members (or the whole world—NetChoice has asserted a facial challenge) say they can comply.

NetChoice’s shortcomings don’t stop with the merits. It has not shown any irreparable harm, and no one is facing any enforcement action right now. The public interest and equities favor the State too. South Carolina is trying to protect children, and NetChoice has admitted that “South Carolina has a compelling interest in protecting minors.” ECF No. 22-1, at 30.<sup>1</sup>

Ultimately, the Act regulates diverse platforms and features, and NetChoice doesn’t develop the factual record or legal arguments to justify the sweeping relief it seeks. The Court should therefore deny the motion.

## **BACKGROUND**

### **A. The South Carolina Social Media Regulation Act**

The Act does multiple things to protect children online. First, it requires a covered online service to “exercise reasonable care” regarding both a minor’s personal data and the “design and operation” of its site to avoid specific harms like compulsive usage, identity theft, and depression.

---

<sup>1</sup> All page cites are to the ECF-generated page numbers at the top of each page.

S.C. Code Ann. § 39-80-20(A). As part of that design, a user must have “easily accessible and easy-to-use tools” for things like disabling certain design features, limiting the time that can be spent on the site, limiting the value of financial purchases on the site, restricting who can view a minor’s account, and restricting access to a user’s location. *Id.* § 39-80-30(A). These tools must be the default settings if the covered online service knows the account belongs to a minor. *Id.* § 39-80-30(C). Along with these features, a covered online service must allow a user to opt out of personalized recommendation systems. *Id.* § 39-80-30(B). And a covered online service may not direct certain ads (like drugs, tobacco, gambling, and alcohol) at minors or use dark patterns (an interface that manipulates the user’s autonomy and subverts his independent decisionmaking). *Id.* § 39-80-60(B)–(C).

The Act also protects children’s personal data. A covered online service may “only collect, use, or share the minimum amount of a minor’s personal data necessary to provide” the service with which the child “has knowingly engaged.” *Id.* § 39-80-40(A). This data “may not be used for reasons other than those for which it was collected.” *Id.* And the covered online service may keep the data only “as long as necessary” to provide the service. *Id.* § 39-80-40(B). Plus, it generally may not, by default, collect a minor’s geolocation. *Id.* § 39-80-40(D).

Other protections exist too. For instance, a covered online service must provide users with “accessible and easy-to-use tools to prevent notifications and push alerts” at certain times. *Id.* § 39-80-40(E). This includes offering the option to turn off alerts for a minor’s account at night and during the school day. *Id.*

Parents likewise must have “accessible and easy-to-use tools” that help “protect and support minors.” *Id.* § 39-80-50(A). Parents must have the ability to change and control the child’s privacy and account settings and limit the child’s purchasing on the site. *Id.* § 39-80-50(B). Parents

must also be given a tool to monitor and limit the total time that a child spends on a site, including restricting the child's access at certain hours. *Id.* § 39-80-50(C).

Finally, the Act includes various reporting requirements. One type of reporting is for parents, minors, and schools to have a way to report harms to minors from using a covered online service. *Id.* § 39-80-60(A). Another type of reporting requirement is for covered online services, which must annually issue a public report from an independent third-party auditor detailing various aspects of its compliance with the Act. *Id.* § 39-80-70(A).

## **B. Procedural history**

NetChoice urged the Governor to veto the Act. The Governor declined that entreaty and signed the Act into law on February 5, 2026.

A few days later, NetChoice sued, challenging the Act's constitutionality. NetChoice attacks multiple provisions in the Act. It asserts ten claims under myriad theories, including the First Amendment, the Fourteenth Amendment, the Commerce Clause, and section 230. ECF No. 1. On this motion, NetChoice seeks a preliminary injunction on five theories: the First Amendment, vagueness, the Commerce Clause, preemption, and due process. ECF No. 22.

## **LEGAL STANDARD**

A preliminary injunction “is an extraordinary and drastic remedy” and “is never awarded as of right.” *Munaf v. Geren*, 553 U.S. 674, 689–90 (2008) (internal quotation mark omitted). A plaintiff must show four elements to obtain it: (1) likelihood of success on the merits, (2) irreparable harm, (3) the balance of the hardships tips in his favor, and (4) an injunction is in the public interest. *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008).

## ARGUMENT

### **I. NetChoice is not likely to prevail on the merits.**

#### **A. NetChoice cannot show a substantial likelihood that it has standing.**

“Standing is a threshold jurisdictional question,” *Pye v. United States*, 269 F.3d 459, 466 (4th Cir. 2001), yet NetChoice brushes it aside in a single footnote, ECF No. 22-1, at 27 n.4. But context is key here. This isn’t a motion to dismiss, where the defendants have the burden to prove that a plaintiff has not alleged plausible facts about standing. Instead, this is a motion for a preliminary injunction, so NetChoice bears the burden to show “a substantial likelihood that [it] ha[s] standing.” *Delmarva Fisheries Ass’n v. Atl. States Marine Fisheries Comm’n*, 127 F.4th 509, 514 (4th Cir. 2025). If a plaintiff can’t make that showing, it cannot obtain a preliminary injunction. *See Am. Fed’n of Tchrs. v. Bessent*, 152 F.4th 162, 174 (4th Cir. 2025).

#### **1. NetChoice lacks associational standing.**

i. Associational standing is “in tension” with Article III’s traditional standing requirements. *Ass’n of Am. Physicians & Surgeons v. FDA*, 13 F.4th 531, 540 (6th Cir. 2021). Thus, for many years, courts have treated associational standing claims with considerable skepticism. *See, e.g., Cal. Bankers Ass’n v. Shultz*, 416 U.S. 21, 44 (1974). That skepticism continues today. *See, e.g., FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 399 (2024) (Thomas, J., concurring).

This skepticism is warranted. One, associational standing skirts the “constitutional minimum” of an injury-in-fact. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). Two, it creates remedy problems because it gives relief to a group that “has not suffered [an] injury.” *Ass’n of Am. Physicians & Surgeons*, 13 F.4th at 540. And three, it allows a plaintiff to essentially “bring a class action without satisfying any of the ordinary requirements” of Rule 23. *All. for Hippocratic Med.*, 602 U.S. at 402 (Thomas, J., concurring).

ii. Given these concerns, courts should closely scrutinize claims of associational standing. To establish associational standing, NetChoice must show three things: (1) the organization's members would otherwise have standing to sue in their own right; (2) the interests the organization seeks to protect are germane to the organization's purpose; and (3) neither the claim asserted nor the relief request requires the participation of individual members of the organization in the lawsuit. *Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.*, 600 U.S. 181, 199 (2023).

NetChoice's shortcoming with associational standing is most apparent with respect to the third prong. NetChoice's challenge is twofold. First, it seeks a preliminary injunction on a variety of theories, including First Amendment claims, vagueness claims, preemption claims, a Dormant Commerce Clause claim, and a due process claim. These types of constitutional claims traditionally require some degree of individualized inquiry to assess their merits. *See, e.g., Ayotte v. Planned Parenthood of N. New Eng.*, 546 U.S. 320, 329 (2006) (a "statute may be invalid as applied to one state of facts and yet valid as applied to another"). Second, NetChoice asserts both facial and as-applied claims on behalf of its members. But courts have generally been reluctant to find that associations have standing to bring as-applied constitutional challenges. *See Ass'n for Accessible Meds. v. Bonta*, 766 F. Supp. 3d 1020, 1028 (E.D. Cal. 2025).

When confronted with another sweeping NetChoice lawsuit, the Ninth Circuit recently held that "it was not an abuse of discretion to find that NetChoice lacked associational standing on behalf of its members" on a claim about minors' access to personalized recommendation algorithms. *NetChoice, LLC v. Bonta* ("CA9 Bonta IP"), 152 F.4th 1002, 1014 (9th Cir. 2025). The Ninth Circuit emphasized the "fact intensive" nature of NetChoice's First Amendment claims, noting that the analysis would vary from "platform to platform." *Id.* An individualized analysis

was required because each NetChoice member had a “unique design” for its platforms and algorithms. *Id.* Some designs, which implement “human editorial directions,” might be entitled to some First Amendment protections, but other designs, which merely respond to user interactions, might not be. *Id.* These same individualized considerations apply to NetChoice’s challenge here.

True, NetChoice cites a handful of cases that support its claim of associational standing, but those decisions cannot withstand scrutiny. For starters, cases that offer a conclusory analysis on the third prong of associational standing don’t tell this Court much. *See NetChoice v. Jones*, No. 1:25-CV-2067 (PTG/LRV), 2026 WL 561099, at \*5 (E.D. Va. Feb. 27, 2026); *NetChoice, LLC v. Reyes*, 748 F. Supp. 3d 1105, 1119 (D. Utah 2024); *NetChoice, LLC v. Griffin*, No. 5:23-CV-05105, 2023 WL 5660155, at \*10 n.6 (W.D. Ark. Aug. 31, 2023).

This lack of rigor is even more troubling on closer review. Neither the Eastern District of Virginia nor the District of Utah discussed *Moody*’s impact on what type of standing analysis is required for a First Amendment challenge. The Ninth Circuit correctly recognized that *Moody* plays an important role here: “The First Amendment analysis is fact intensive and will surely vary from platform to platform,” so “the merits of ‘the claim asserted’ and the ‘relief requested’ requires the participation of individual NetChoice members.” *CA9 Bonta II*, 152 F.4th at 1014 (cleaned up). “[A]ssociational standing” is therefore “inappropriate.” *Id.*

Plus, many of the cases NetChoice cites dealt with laws that are materially different from the Act. For instance, several cases dealt with laws that sought to ban minors from having certain online accounts absent parental consent. *See, e.g., NetChoice, LLC v. Fitch*, 787 F. Supp. 3d 262, 269 (S.D. Miss. 2025). South Carolina’s act does no such thing. These laws thus present different constitutional questions, which, in turn, raise different concerns around associational standing.

## 2. NetChoice cannot assert the interests of its members' users.

NetChoice also conclusorily claims that it “has standing to assert the rights of its members’ users.” ECF No. 22-1, at 27 n.4. Courts generally view such arguments with disfavor. *See Maryland v. U.S. Dep’t of Agric.*, 151 F.4th 197, 212 (4th Cir. 2025).

This disfavor should be heightened here because NetChoice takes the extraordinary step of “stacking” standing exceptions when it invokes the rights of its members’ users. NetChoice doesn’t explain anything about these users. NetChoice doesn’t even identify any of its members’ users. It just claims that it can assert these unidentified people’s rights. But whose? NetChoice could even be trying to assert the Court’s rights here, depending on what, if any, social media sites the Court uses. So too with members of the South Carolina General Assembly, which enacted the Act that NetChoice now challenges.

Even if stacking were allowed, NetChoice lacks third-party standing for two reasons. One, to have third-party standing, NetChoice must still demonstrate its own Article III injury. *See Kowalski v. Tesmer*, 543 U.S. 125, 129 (2004). As discussed, NetChoice has failed to establish associational standing, and it has not even attempted to invoke its own organizational standing.

And two, NetChoice cannot satisfy the prudential limitations that come with third-party standing. Those requirements are (1) that “the party asserting the right has a ‘close’ relationship with the person who possesses the right”; and (2) that there “is a ‘hindrance’ to the possessor’s ability to protect his own interests.” *Id.* at 130 (quoting *Powers v. Ohio*, 499 U.S. 400, 411 (1991)).

On the first limitation, unlike vendors bringing claims on behalf of their customers, NetChoice itself has no direct relationship with its members’ users. *Cf. Md. Shall Issue, Inc. v. Hogan*, 971 F.3d 199, 216 (4th Cir. 2020) (“[A] vendor has third-party standing to pursue claims on behalf of its customers.”). Put another way, Google, Pinterest, Snap, and other NetChoice

members aren't asserting claims on their customers' behalf. There's another link in the chain—a link that undermines the logic of letting the vendor sue on behalf of its customer. *Virginia v. American Booksellers Ass'n* doesn't compel a different result because bookstores (unlike Google, Pinterest, or Snap here) were plaintiffs in the case. *See* 484 U.S. 383, 388 n.3 (1988).

Turning to the second limitation, there is nothing to suggest that any of NetChoice's members' users—who number in the millions—are hindered from bringing these claims. Presumably at least one of those users, if he thought the Act harmed him somehow, could challenge it. NetChoice never tries to explain why a user couldn't bring a case. Nor does NetChoice assure the Court that there is no possible conflict of interest between it and the users. *See June Med. Servs. L.L.C. v. Russo*, 591 U.S. 299, 402 (2020) (Alito, J., dissenting) (no third-party standing when “there is a potential conflict of interest between the plaintiff and the third party”). After all, users may like the Act because it protects minors.

**B. NetChoice is unlikely to prevail on its First Amendment claims.**

**1. NetChoice's First Amendment claims fail based on the First Amendment's original public meaning.**

Courts historically interpreted constitutional rights by examining “the history of the times in the midst of which the provision was adopted.” *Reynolds v. United States*, 98 U.S. (8 Otto) 145, 162 (1878). In other words, the scope of rights is determined by the text's original public meaning, not ad hoc judicial balancing. That changed in the past century. Following footnote 4 in *United States v. Carolene Products Co.*, 304 U.S. 144, 152 n.4 (1938), courts began employing a means-end scrutiny in cases involving constitutional rights, *see, e.g., Skinner v. Oklahoma ex rel. Williamson*, 316 U.S. 535, 541 (1942) (“strict scrutiny” for sterilization law).

In recent years, the Supreme Court has wisely moved away from such tests. It “decline[d] to adopt” a means-end scrutiny for the Second Amendment, looking instead to text, history, and

tradition for historical analogues. *N.Y. State Rifle & Pistol Ass’n v. Bruen*, 597 U.S. 1, 117 (2022). And it relied on “original meaning and history” to guide Establishment Clause decisions. *Kennedy v. Bremerton Sch. Dist.*, 597 U.S. 507, 536 (2022). So it should be with the Free Speech Clause.

Under this proper framework, NetChoice’s claims fail. That’s because “‘the freedom of speech,’ as originally understood, does not include a right to speak to minors (or a right of minors to access speech) without going through the minors’ parents or guardians.” *Brown v. Ent. Merchants Ass’n*, 564 U.S. 786, 821 (2011) (Thomas, J., dissenting).<sup>2</sup> In *Brown*, Justice Thomas traced parental authority over children through the New England Puritans, the Revolution, and the early nineteenth century. *Id.* at 823–34. The “founding generation . . . believed parents to have complete authority over their minor children and expected parents to direct the development of those children.” *Id.* at 834. So “the founding generation would not have understood ‘the freedom of speech’ to include a right to speak to children without going through their parents.” *Id.* at 835. The Act therefore does not violate the First Amendment—no balancing required.

## 2. NetChoice’s First Amendment claims fail under means-end scrutiny.

NetChoice’s claims still fail under means-end scrutiny. Though NetChoice claims to bring facial and as-applied First Amendment challenges, *see* ECF No. 1, at 33 (Count I), 41 (Count III), 44 (Count IV), 54 (Count VI), it does not distinguish between these challenges in its motion and argues these claims as facial challenges (given the lack of individualized discussion).

Some First Amendment background is useful at the outset. The Ninth Circuit explained this framework in NetChoice’s recent challenge to a California law. First, a court must “determine

---

<sup>2</sup> Justice Thomas dissented in *Brown*, but that’s no issue. The petitioner there didn’t make an originalist argument. It argued that violent video games were like obscene materials that fell outside the First Amendment. *See* Pet.’s Br., No. 08-1448 (U.S. July 12, 2010). So while Justice Thomas addressed the originalist argument, the Court didn’t have to reject it to rule as it did.

whether the regulation implicates protected expression” to trigger the First Amendment’s protection. *NetChoice, LLC v. Bonta* (“*CA9 Bonta III*”), \_\_\_ F.4th \_\_\_, No. 25-2366, 2026 WL 694471, at \*6 (9th Cir. Mar. 12, 2026). Second, a court must determine whether a law “is content based or content neutral.” *Id.* And third, a court must apply the appropriate level of scrutiny. *Id.*

When a plaintiff brings a facial challenge as NetChoice does, there is more. To prevail on that challenge, a plaintiff must show that “a substantial number of the law’s applications are unconstitutional, judged in relation to the statute’s plainly legitimate sweep.” *Moody*, 603 U.S. at 723 (internal alteration omitted). A court must therefore determine the law’s scope (the denominator) and then decide which applications violate the First Amendment (the numerator) to determine whether a law survives the facial challenge. *CA9 Bonta III*, 2026 WL 694471, at \*6.

All NetChoice’s First Amendment theories have problems on both fronts. On the steps, the first one is a problem for NetChoice. The Act generally regulates platform features that shape user experience—not expressive activity—so the Act isn’t subject to any stringent First Amendment review. And on the type of claims, NetChoice offers no evidence for either the numerator and denominator to prevail on a facial challenge.

**i. Duty of “reasonable care” (§ 39-80-20(A))**

A covered online service must “exercise reasonable care in the use of a minor’s personal data and the design and operation” of its service “to prevent” certain “harm to minors.” S.C. Code Ann. § 39-80-20(A). Such harms include “compulsive usage,” “anxiety,” “depression,” and “highly offensive intrusions on the minor’s reasonable privacy expectations.” *Id.*

**a.** NetChoice challenges this subsection of the Act as a “proxy” for speech restrictions that triggers the First Amendment. *See* ECF No. 22-1, at 29. NetChoice is incorrect. Section 39-80-20(A) regulates how a covered online service uses a minor’s data and how it designs and operates

its site to avoid harming minors. The “use” of data doesn’t regulate speech but conduct, and NetChoice never explains how that part of section 39-80-20(A) restricts speech.

That leaves the “design and operation” of a site. That does not automatically qualify for sweeping First Amendment protection. Take the “operation.” If that is driven chiefly by artificial intelligence rather than people, there may be no expressive activity. That *computer v. human* issue “might have constitutional significance.” *Moody*, 603 U.S. at 746 (Barrett, J., concurring).

And the “design” covers more than just how a covered online service “prioritizes the dissemination of one type of content over another.” *M.P. by & through Pinckney v. Meta Platforms Inc.*, 127 F.4th 516, 525 (4th Cir. 2025) (quoted at ECF No. 22-1, at 29).<sup>3</sup> Ultimately, there’s a difference in “content moderation” (which might implicate speech) and “engagement maximization” (which does not). *See Moody*, 603 U.S. at 736 n.5. Many covered design features—including infinite scroll, autoplay, and notifications—are not expressive. *See Edelson Decl.* ¶ 14. And even if there were some “incidental burdens on speech” with this part of the Act, that does not automatically mean that the law triggers heightened First Amendment scrutiny. *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 567 (2011). Government can regulate “economic activity” while incidentally burdening speech. *Id.* Otherwise, virtually every economic regulation would be unconstitutional.

**b.** Even if the Act implicated the First Amendment, NetChoice’s challenge to section 39-80-20(A) still fails for two reasons. *First*, there’s the lack of evidence. When it comes to a facial challenge, NetChoice just proffers hypotheticals about news reports, ballet videos, and violent video games. *See ECF No. 22-1*, at 29–30. NetChoice cannot succeed on a facial challenge by

---

<sup>3</sup> *Pinckney* is an awkward authority for NetChoice. That was a section 230 case. *See* 127 F.4th at 521. There’s an inherent tension in insisting that the design of your website is expressive activity but what your website says isn’t your speech. NetChoice can’t have it both ways.

speculating “about ‘hypothetical’ or ‘imaginary’ cases,” *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 450 (2008).

Plus, NetChoice never tries to explain when or how the Act regulates its members’ speech (or other services’ speech) compared to other applications. In other words, NetChoice fails to try to show the numerator and denominator for the plainly-legitimate-sweep analysis. *See CA9 Bonta III*, 2026 WL 694471, at \*6. No doubt, “dealing with a broad swath of varied platforms and functions in a facial challenge” is “a daunting, if not impossible, task.” *Moody*, 603 U.S. at 745 (Barrett, J., concurring). But that’s the “cost” of a facial challenge. *Id.* at 723 (majority opinion). Without evidence and argument on this front, NetChoice’s facial challenge fails.

NetChoice fares no better when it comes to arguments about its members for an as-applied challenge. Such a claim requires “sufficiently concrete circumstances” so that a court “can . . . resolve[]” whether the law violates a plaintiff’s rights on those facts. *Richmond Med. Ctr. For Women v. Herring*, 570 F.3d 165, 169 (4th Cir. 2009) (en banc). NetChoice’s argument lacks those required specifics. It invokes hypotheticals about posts from yoga studios, ECF No. 22-2, at ¶ 29 (Baird); “certain” (unnamed) books, ECF No. 22-5, at ¶ 13 (Roin); combat, weapons, dieting, and human reproduction, ECF No. 22-6, at ¶ 75 (Weber); the Civil War and LGBT movement, ECF 22-4, at ¶ 84 (Paolucci); or paragraphs from declarations that don’t provide even hypotheticals, *see* ECF No. 22-3, at ¶¶ 44–46 (Cleland). But no specifics about members’ users. Without “particular facts” about the law applied to the plaintiff, that plaintiff cannot win an as-applied challenge. *United States v. Hasson*, 26 F.4th 610, 616 (4th Cir. 2022).

*Second*, NetChoice’s analysis of the tailoring is flawed. *See* ECF No. 22-1, at 30–32. The State’s interest is easy: NetChoice does “no[t] dispute that South Carolina has a compelling interest in protecting minors.” *Id.* at 30.

So NetChoice’s claim turns on tailoring. While NetChoice insists the law must be narrowly tailored because the Act must survive strict scrutiny, the Act need only satisfy intermediate scrutiny because it is content neutral. Section 39-80-20(A) does not regulate anything based on what a site says, so it’s not content-based on its face. It only regulates how a covered online service’s use of data, design, or operation might harm a minor. It’s the impact of the use, design, or operation on the minor that matters. This section can therefore “be justified without reference to the content of the regulated speech,” and South Carolina didn’t adopt it “because of disagreement with the message the speech [if there is any] conveys.” *Reed v. Town of Gilbert*, 576 U.S. 155, 164 (2015) (cleaned up).

Nothing NetChoice says on the tailoring question is compelling (no matter the level of tailoring required). NetChoice (understandably) doesn’t really challenge that covered design features harm minors. Research on “infinite scroll” features, for instance, shows that they make it “difficult to disengage from” a site and lead to habitual usage. Edelson Decl. ¶¶ 19–22. Same with autoplay features. *Id.* ¶¶ 24–26. The addictive nature is true whether the design feature is expressive or not. As one example, gamification (which might be nonexpressive in some contexts) “works by turning participation itself into a goal to pursue, preserve, and avoid losing.” *Id.* ¶ 30.

Instead, NetChoice claims the Act is overinclusive because it “governs many websites that offer significant informational value and pose little risk of harm, such as language apps, online calculators, and dictionary apps.” ECF No. 22-1, at 31. What harm is reasonably foreseeable from a calculator or dictionary? This sky-is-falling argument ignores the statutory requirement that a covered online service take “*reasonable care*.” S.C. Code Ann. § 39-80-20(A) (emphasis added). There’s no sensitive-person veto for what “*some user(s) in some contexts*” might find problematic. ECF No. 22-1, at 31. Plus, NetChoice treats section 39-80-20(A) as focused solely on what a minor

sees online. That misreads the Act. Section 39-80-20(A) focuses on harms to minors. It covers, for instance, anything that would cause “compulsive usage.” *Id.* § 39-80-20(A)(1). So this isn’t really about “averting [anyone’s] eyes.” *NetChoice v. Griffin*, No. 5:25-CV-5140, 2025 WL 3634088, at \*8 (W.D. Ark. Dec. 15, 2025). And in any event, “reasonable care” is already something that NetChoice’s members should be exercising because of the codes of ethics that govern them (not to mention state tort law). *See* Edelson Decl. ¶¶ 52–57.

NetChoice next argues that section 39-80-20(A) is underinclusive because section 39-80-20(C) still allows a minor to search for any content she wants. ECF No. 22-1, at 31–32. That does not make section 39-80-20(A) underinclusive. Rather, it shows that section 39-80-20(A) does not target speech but aims to prevent harm. Nor does NetChoice’s invocation of the “physical world” move the needle. *Id.* at 32. The internet causes unique harms that require different remedies from the harms that happen on the playground. Jonathan Haidt, *The Anxious Generation* 11 (2024) (describing the “four foundational harms” from minors’ time online: “sleep deprivation, social deprivation, attention fragmentation, and addiction”).

None of NetChoice’s proposed alternatives to the Act is credible. *See* ECF No. 22-1, at 32. One, NetChoice says its members are already incentivized to filter content or block material. *See id.* (“as many already do”). Two, NetChoice waxes poetic about all the tools that parents already have to monitor children online. *See id.* at 20–22 (citing dozens of paragraphs in the declarations about existing tools). And three, NetChoice says criminal laws that could protect children.

Those aren’t viable options, so requiring “reasonable care” is necessary. Neither one nor two is working, given the ongoing harms to children. Or consider protecting minors’ privacy. People generally do not fully understand what privacy they are giving up on social media sites. McCoy Decl. ¶¶ 12–13. And companies are misrepresenting what they are doing with users’

information. *Id.* ¶¶ 15–16. This is all particularly harmful to minors, who are, for example, having child predators recommended as “friends” or connections at a shockingly high rate. *Id.* ¶ 14.

**ii. Personalization regulations (§§ 39-80-30(B), 39-80-40(F))**

Social media sites often use automated systems to rank or promote content for each user, based on an automated processing of a user’s personal data. In other words, these sites try to put on each user’s screen content that the user is likely to find interesting and keep him on the site.

The Act prohibits covered online services from making this automated personalized recommendation system the default for any minor’s account. S.C. Code Ann. § 39-80-30(B). Any user must have the option to turn off such a system. *Id.* And covered online services cannot profile any user that the service knows to be a minor unless the minor has “knowingly requested” to use an aspect of the online service that requires profiling. *Id.* § 39-80-40(F).

**a.** NetChoice attacks these sections as a burden on its speech, *see* ECF No. 22-1, at 33–34, leaning heavily on the *Moody* majority’s assertion that “social-media platforms are in the business, when curating their feeds, of combining ‘multifarious voices’ to create a distinctive expressive offering.” 603 U.S. at 738. Game over, says NetChoice, for the express-activity question.

Not quite. Once again, maximizing user engagement does not necessarily implicate speech because curating a feed to show a user what she wants does not make any editorial decision about content. *See Moody*, 603 U.S. at 736 n.5.

Plus, Justice Barrett (who joined the *Moody* majority) observed that differences between human and algorithmic feed curation “might have constitutional significance.” *Id.* at 746 (Barrett, J., concurring). “[T]he analysis is bound to be fact intensive,” Justice Barrett explained, “and it will surely vary from function to function and platform to platform.” *Id.* at 747. The Ninth Circuit recognized the same thing in rejecting NetChoice’s argument. *See CA9 Bonta II*, 152 F.4th at 1021.

None of the declarations that NetChoice cites begin to provide sufficient evidence for that fact-intensive review or explain the role that people—rather than computers—play in this process. *See* ECF No. 22-1, at 33 (citing ECF No. 22-2, at ¶¶ 30–31 (Baird); ECF No. 22-3, at ¶¶ 40–42 (Cleland); ECF No. 22-5, at ¶ 15 (Roin); ECF No. 22-6, at ¶ 39 (Weber)).

Another way to confirm that the Act doesn’t implicate expressive activity on this front is that NetChoice points to the “infinite scroll” rules as proof that the Act “target[s]” speech. ECF No. 22-1, at 34. But infinite scroll technology has been patented. *See* Edelson Decl. ¶ 18. That’s telling because copyright—not patent law—protects expression. *Design Basics, LLC v. Signature Constr., Inc.*, 994 F.3d 879, 889 (7th Cir. 2021).

**b.** NetChoice also offers no evidence of how the Act impacts anyone *other than* NetChoice’s members. That’s fatal to its facial challenge, which considers *all* a law’s potential applications. *See Moody*, 603 U.S. at 723–24. As the Ninth Circuit recently observed in ruling against NetChoice’s facial challenge to a California law, a plaintiff bringing a facial challenge must “develop a record that would allow the court to determine the law’s full set of applications, cataloging what activities, by what actors the law regulates.” *CA9 Bonta III*, 2026 WL 694471, at \*10 (cleaned up). NetChoice can’t leave to the Court to “speculate whether a law unduly burdens expression without a developed record that explains not only how NetChoice’s platforms work, but also how a wide range of third-party services operate” because that “information is necessary to characterize the denominator of a law’s applications.” *Id.* (cleaned up).

NetChoice’s problem doesn’t stop with its lack of evidence. More fundamentally, it’s not certain that NetChoice has the law right. The parts of *Moody* that NetChoice relies on are on “nonbinding dicta.” *Moody*, 603 U.S. at 766 (Alito, J., concurring in the judgment). NetChoice, in other words, puts more weight on *Moody* than it can bear by trying to shoehorn its sweeping facial

claims within *Moody*'s scope by avoiding its clear holding on facial challenges. But the *Moody* majority (in a part that wasn't dicta) observed that "[t]he online world is variegated and complex." *Id.* at 725 (majority opinion); *see also id.* at 736 n.5 (recognizing that the Court wasn't deciding certain questions). It is therefore "not hard to see how the answers might differ" depending on the covered online service or even the features of each service. *Id.* at 725. So NetChoice has failed to show that it can prevail on a facial challenge to sections 39-80-30(B) and 39-80-40(F).

This tracks tort cases against social media sites. Those claims were allowed to proceed over those sites' First Amendment objections because the plaintiffs sought relief for "non-expressive and intentional design choices to foster compulsive use in their minor users." *In re Soc. Media Adolescent Addiction/Pers. Inj. Prods. Liab. Litig.*, 754 F. Supp. 3d 946, 978 (N.D. Cal. 2024).

c. But even if NetChoice were correct that sections 39-80-30(B) and 39-80-40(F) fall within the First Amendment's ambit and were allowed to litigate this claim as a facial challenge, its tailoring analysis is flawed. The intermediate scrutiny standard NetChoice attempts to apply says a law "need not be the least speech-restrictive means of advancing the Government's interests." *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 662 (1994). The law simply must "not burden substantially more speech than is necessary to further the government's legitimate interests." *Id.* (internal quotation mark omitted).

NetChoice ignores the State's interest in protecting children. "[R]esearch suggests that social media are having a devastating effect on many young people, leading to depression, isolation, bullying, and intense pressure to endorse the trend or cause of the day." *Moody*, 603 U.S. at 768 (Alito, J., concurring in the judgment). As the *Moody* majority put it, "today's social media pose dangers not seen earlier: No one ever feared the effects of newspaper opinion pages on adolescents' mental health." *Id.* at 733 (majority opinion); Edelson Decl. ¶¶ 19, 20, 24, 25, 29, 30,

31, 33, 37, 41, 42, 48, 49. Another leading researcher found that a “phone-based childhood” causes “four foundational harms: sleep deprivation, social deprivation, attention fragmentation, and addiction.” Haidt, *supra*, at 11. These follow from many minors being online “almost constantly.” *Id.* at 119. And the best way to remedy those harms is to make being online less addictive. Social media’s purported benefits cannot compel a different result.

**iii. Default requirements (§ 39-80-30(A), (C))**

The Act requires covered online services provide users “easily accessible and easy-to-use tools” for things like limiting the time a user spends online, the money a user may spend on the site, and who can search for a user’s account. S.C. Code Ann. § 39-80-30(A). These limits must be the default setting for anyone the covered online service knows is a minor. *Id.* § 39-80-30(C).

NetChoice says these are content-based restrictions that fail any level of scrutiny. ECF No. 22-1, at 35–36. Once again, NetChoice is mistaken: Default requirements do not implicate expressive activity. At its core, NetChoice treats sections 39-80-30(A) and (C) as a blanket prohibition on what a covered online service may say. That’s not the case. These provisions require two things. One, tools to disable certain features must be easy to find. Put differently, online services may not obscure how to turn off various features. That does not limit the services’ expressive activity. Having to have these features accessible does not, in other words, turn on “the topic discussed or the idea or message expressed.” *Reed*, 576 U.S. at 163. Instead, they are merely regulations of “economic activity or, more generally, . . . nonexpressive conduct” that do not trigger the First Amendment. *Sorrell*, 564 U.S. at 567. Again, among the features that NetChoice points to is “autoplay” of videos, ECF No. 22-1, at 35, but that’s another feature that’s been patented, Edelson Decl. ¶ 23. So it can’t be expressive. *Design Basics, LLC*, 994 F.3d at 889. Same with notification design features, which are also patented. Edelson Decl. ¶ 36.

And two, for minors, the default must be that certain features are turned off. Those features can be turned back on. There's nothing wrong with changing the default rule for minors because "a child—like someone in a captive audience—is not possessed of that full capacity for individual choice which is the presupposition of First Amendment guarantees." *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 214 n.11 (1975). Knowing the harm that social media sites can cause minors, South Carolina has taken a modest, reasonable step of requiring minors to choose to turn on certain features for these sites, rather than forcing minors to turn them off. The State has therefore not "bar[red] . . . dissemination" of anything to minors. *Id.* at 213. It's simply required an opt-in system, rather than an opt-out one. An opt-in scheme can trigger only intermediate scrutiny and such opt-in schemes can pass constitutional muster based on the privacy interests involved. *See, e.g., Trans Union Corp. v. F.T.C.*, 267 F.3d 1138, 1143 (D.C. Cir. 2001) (upholding opt-in scheme in the Fair Credit Reporting Act for sale of customer information).

But if some of these settings (such as "quantification of engagement," or more colloquially, "likes," and appearance-altering filters) might be expressive, the tailoring analysis cuts against an injunction. Users are drawn to access social media sites more frequently to see how many "likes" a post has and to modify their behavior to get more "likes." Edelson Decl. ¶¶ 33–35. Appearance-altering filters cause body-image issues from seeing versions of people that are "not naturally achievable." *Id.* ¶¶ 48–50. This is no different in purpose than the other covered design features. Notifications are intended to draw users back onto a site. *Id.* ¶¶ 38–39. In-game purchases are designed to push minors to spend more money through "the same reinforcement principle that underlies slot machines and other forms of gambling." *Id.* ¶ 43. The Act, in other words, directly targets the cause of the harms it seeks to remedy.

**iv. Reporting requirements (§§ 39-80-60(E), 39-80-70)**

NetChoice next challenges the Act’s reporting requirement as violating the “right to refrain from speaking.” *See* ECF No. 22-1, at 36–37. NetChoice doesn’t really build out the argument. Instead, it cites a couple cases in a single paragraph and says the result should be the same here.

But the Court shouldn’t blindly follow what the Ninth Circuit said because the state laws are different. That court described the challenged laws in other States as requiring companies to “opin[e] on whether and how certain controversial categories of content should be moderated.” *X Corp. v. Bonta*, 116 F.4th 888, 901 (9th Cir. 2024) (discussing California’s law). South Carolina’s law simply requires information to be reported under section 39-80-70 and provided to users under section 39-80-60(E). This information doesn’t require NetChoice’s members to opine on anything. Instead, they must simply describe how they are complying with the Act.

Under NetChoice’s view, any number of regulatory reporting or disclosure requirements already on the books would trigger (and presumably fail) strict scrutiny. South Carolina requires physicians to submit reports about patients with tuberculosis. S.C. Code Ann. § 44-31-10. Another mandates that lobbyists submit a semi-annual report to the State Ethics Commission. *Id.* § 2-17-30(A)(1). And to be sure, the federal government has plenty of its own reporting requirements.

**v. Alleged censorship**

As a final argument, NetChoice claims the Act “[c]ombine[s]” to require its members to be “censors for the State.” ECF No. 22-1, at 37. The Court need not dwell on this claim because NetChoice doesn’t develop it at all. In a couple of sentences with a couple of case cites and sweeping references to declarations, NetChoice breezily claims that its members are censors. That’s not enough. *Cf. Grayson O Co. v. Agadir Int’l LLC*, 856 F.3d 307, 316 (4th Cir. 2017) (“A party waives an argument by failing to present it in its opening brief or by failing to develop its

argument—even if its brief takes a passing shot at the issue.” (cleaned up)).

But even if NetChoice had tried to develop this argument, it would have failed. This is just a mash-up of its other arguments. Those arguments fail on their own, and they fail together.

**C. NetChoice is unlikely to prevail on its vagueness claims.**

NetChoice claims to bring both facial and as-applied challenges, ECF 1, at 46, but its motion makes no effort to show how the “law is . . . vague as applied to” NetChoice and its members specifically, *Expressions Hair Design v. Schneiderman*, 581 U.S. 37, 49 (2017); *see, e.g.*, ECF 22-1, at 42 (discussing only “covered online services” generally). So really, NetChoice is seeking a preliminary injunction on a facial vagueness claim.

And that claim is “hard to win.” *Moody*, 603 U.S. at 723. In a non-First Amendment case, as long as the law has a “plainly legitimate sweep,” “a plaintiff cannot succeed on a facial challenge.” *Id.* To be sure, NetChoice’s vagueness claim is a non-First Amendment claim. “Vagueness doctrine is an outgrowth not of the First Amendment, but of the Due Process Clause.” *United States v. Williams*, 553 U.S. 285, 304 (2008).

NetChoice fairly points out “statute[s] capable of reaching expression sheltered by the First Amendment” receive heightened review under the “[vagueness] doctrine.” ECF 22-1, at 38 (alteration in original) (quoting *Ctr. for Individual Freedom, Inc. v. Tennant*, 706 F.3d 270, 280 (4th Cir. 2013)). But “perfect clarity and precise guidance have never been required even of regulations that restrict expressive activity.” *Ward v. Rock Against Racism*, 491 U.S. 781, 794 (1989)). Courts still routinely reject vagueness challenge despite this “heightened standard.” *Holder v. Humanitarian L. Project*, 561 U.S. 1, 21 (2010) (collecting cases).

NetChoice claims that “[a]ll the Act’s challenged speech restrictions are invalid” because they are “subjective and abstract.” ECF No. 22-1, at 38 (emphasis added). But NetChoice only

identifies a handful of specific provisions that supposedly meet that description. Because the ultimate inquiry on a vagueness challenge is whether the “[w]ords . . . are vague,” *United States v. Cardiff*, 344 U.S. 174, 176 (1952), NetChoice’s argument must be limited to the six specific provisions it references. “It is not the Court’s role to analyze and consider every word, phrase, or provision in all of the . . . statute[] upon the Defendants’ suggestion or conclusory argument that some portion of some statute may be so vague as to deem it unconstitutional.” *United States v. Carlson*, Crim. No. 12-305(DSD/LIB), 2013 WL 5125434, at \*11 (D. Minn. Sept. 12, 2013).

### 1. “Reasonable care” for “minors”

i. NetChoice argues that asking covered services to exercise “reasonable care” to avoid harming “minors” is problematic because it cannot tell whether that duty applies to minors “generally or minors in different age ranges.” ECF 22-1, at 38. As a threshold problem, exercising “reasonable care” is something that NetChoice’s members should understand and be doing already. It’s part of their codes of ethics. *See* Edelson Decl. ¶¶ 52–57.

In any event, that objection misstates how statutes regulating harms to minors operate. The Act does not require providers to calibrate their conduct to every conceivable child from infancy through age 17. Instead, it directs services to exercise reasonable care to prevent “harm to minors,” S.C. Code Ann. § 39-80-20(A)—plural—which refers to harms affecting minors as a class rather than the most sensitive or youngest imaginable child. *See CA9 Bonta III*, 2026 WL 694471, at \*16 (contrasting use of the singular “child,” which suggests liability based on “a single child’s response”). That framing reflects a familiar and administrable approach. The statute contemplates the narrow category of conduct that would reasonably be understood to harm minors across age groups, including older adolescents, not edge-case reactions at the margins.

Courts interpreting comparable “harmful to minors” statutes have long rejected the notion

that such provisions must be evaluated from the perspective of the youngest possible child or the most sensitive audience member. Instead, they ask whether material would impact a “legitimate minority of normal, older adolescents.” *Virginia v. Am. Booksellers Ass’n*, 372 S.E.2d 618, 621, 624 (Va. 1988); *see also Am. Booksellers Ass’n v. Webb*, 919 F.2d 1493, 1504–05, 1513 (11th Cir. 1990). The same principle applies here. Although the Act defines “minor” as any consumer under 18, it sensibly operates with reference to minors as a group—including older adolescents—rather than requiring covered services to tailor their conduct to the youngest conceivable child.

Beyond any legal doctrines, research already connects covered design features with specific harms. Infinite scroll, autoplay, and gamification, for instance, promote compulsive usage, Edelson Dec. ¶¶ 22, 26, 31, while in-game purchases cause financial harm, *id.* ¶ 44, and appearance-altering filters cause psychological issues, *id.* ¶ 51. Based on this research, there’s a core meaning to what reasonable care looks like.

**ii.** NetChoice’s related claim—that liability turns on the varying “sensitivities” of individual minors—fares no better. ECF 22-1, at 39. As an initial matter, that argument is untethered from the Act’s text. NetChoice broadly gestures to “assess[ing] . . . risk” to minors in the abstract, but fails to engage with the specific, defined harms the Act regulates. *See id.* at 38–39. But vagueness analysis turns on the statute’s terms, not abstract descriptions of what a law might cover. *See Cardiff*, 344 U.S. at 176.

Looking at that language, the Act does not impose liability based on amorphous or purely subjective reactions. Rather, it identifies concrete harms, defined by reference to objective criteria and examples. *See* S.C. Code Ann. § 39-80-20(A). By ignoring those definitions, NetChoice’s “sensitivities” argument attacks a statute that does not exist.

**iii.** Another issue for NetChoice here is its invocation of cases involving criminal statutes.

Both the Arkansas law in *Griffin*, 2025 WL 3634088, at \*12, and the Colorado law in *Counterman v. Colorado*, 600 U.S. 66, 70 (2023), subjected people to criminal penalties. South Carolina’s Act does not, *see* S.C. Code Ann. § 39-80-80, and courts have “expressed greater tolerance of enactments with civil rather than criminal penalties because the consequences of imprecision are qualitatively less severe,” *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498–99 (1982).

## 2. “Harm”

i. NetChoice says “the Act’s references to various ‘harms’” that covered services should take reasonable care to prevent are too subjective. ECF 22-1, at 39. Despite this sweeping claim that each statutory harm is vague, NetChoice only identifies a few examples. *See id.* at 39–40.

The limited harms NetChoice does identify—compulsive usage, severe psychological and emotional harms—are not facially vague. “Compulsive usage” “means the persistent and repetitive use of a covered online service that substantially limits one or more of a user’s major life activities including, but not limited to, sleeping, eating, learning, reading, concentrating, communicating, or working.” S.C. Code Ann. § 39-80-10(1). It’s a defined term—and the subject of much research. *See* Edelson Decl. ¶¶ 19, 20, 24, 25, 29, 30, 31, 33, 37 (citing studies).

NetChoice’s objection here is nothing more than line-drawing questions asking how much use is “persistent,” when life activities are “substantially limit[ed],” and when ordinary behavior becomes “compulsive.” ECF 22-1, at 39–40 (five sentence argument of five questions). But margin probing isn’t a vagueness argument. Any statute raises “a close question” “in marginal situations.” *Doe v. Cooper*, 842 F.3d 833, 842 (4th Cir. 2016). But “[t]hat some smidgen of ambiguity remains is no reason to find a statute unconstitutionally vague.” *Recht v. Morrissey*, 32 F.4th 398, 415 (4th Cir. 2022). Whether a law has a plainly legitimate sweep—not whether its margins are always

clear—is what matters in a facial vagueness challenge. NetChoice’s attack on the outer bounds of these terms effectively concedes that it has a knowable “core.” *Cooper*, 842 F.3d at 842.

NetChoice’s challenge to the harms of “severe psychological harm” and “severe emotional distress” also falls flat. This objection poses a single hypothetical about discomfort from reading Anne Frank’s diary and says that “covered services have no way to know whether this discomfort” would fall under the statutory language. ECF 22-1, at 40. But “speculation about possible vagueness in hypothetical situations not before the Court will not support a facial attack.” *Hill v. Colorado*, 530 U.S. 703, 733 (2000).

Beyond the sole-hypothetical problem, NetChoice doesn’t even pretend to do any analysis on whether the law has a plainly legitimate sweep. It doesn’t discuss what the law covers and what is understandable compared to what is not. That’s another fatal shortcoming.

ii. Beyond its inability to mount a proper facial vagueness challenge, the little substance NetChoice does offer is unavailing. These terms provide notice in the core of cases. “Compulsive usage” is defined using ordinary, widely used language: “persistent,” “repetitive,” and conduct that “substantially limits . . . major life activities.” S.C. Code Ann. § 39-80-10(1). “[R]un-of-the-mill statutory phrases” like these do not create vagueness problems. *Recht*, 32 F.4th at 415. Terms such as “persistent” and “repetitive” appear dozens of times each in the South Carolina Code and hundreds of times in the U.S. Code. And “substantially limits” reflects a familiar degree-based standard courts have long upheld. *See, e.g., United States v. Miselis*, 972 F.3d 518, 545 (4th Cir. 2020) (recognizing “serious” and “substantial” as “perfectly constitutional” qualitative standards). The statute further clarifies its scope by listing concrete examples of “major life activities,” S.C. Code Ann. § 39-80-10(1)—sleeping, eating, learning, reading, concentrating, communicating, or working—which provide an obvious basis for analogy, as courts routinely do when applying

statutory terms. *Cap. Associated Indus., Inc. v. Stein*, 922 F.3d 198, 210–11 (4th Cir. 2019).

“Severe psychological harm” and “emotional distress” do not pose “inescapable” vagueness problems either. ECF 22-1, at 40. These terms are easily understood by people of common intelligence. For one, “severe psychological harm” is further tailored by the referenced examples of “anxiety, depression, self-harm [and] suicidal ideations.” S.C. Code Ann. § 39-80-20(A)(2). And “severe” isn’t only a matter of degree commonly condoned in statutory drafting, *Nash v. United States*, 229 U.S. 373, 377 (1913) (“the law is full of instances where a man’s fate depends on his estimating rightly . . . some matter of degree”), it’s a go-to evaluative criterion. The Diagnostic and Statistical Manual of Mental Disorders, standard in psychology, references “severe” over 1,000 times. American Psychiatric Association, *Diagnostic and Statistical Manual of Mental Disorders* (5th ed. text rev. 2022). Indeed, “severe depression” and “severe anxiety” are recognized and distinct conditions. *See id.* at 82, 156. And again, there’s research on this harm. Edelson Decl. ¶ 48.

“Emotional distress,” likewise legion in the psychological world, is also “easily understood” in the law. *United States v. Conlan*, 786 F.3d 380, 386 (5th Cir. 2015). For example, it’s “[a] familiar term from tort law,” where people—NetChoice members included—are asked to behave reasonably to avoid infliction of “emotional distress.” *United States v. Uhlenbrock*, 125 F.4th 217, 224 (5th Cir. 2024) (rejecting a vagueness challenge to “substantial emotional distress”); *United States v. Osinger*, 753 F.3d 939, 945 (9th Cir. 2014) (same). In other words, the General Assembly didn’t pull these terms from thin air. It used standard terms in life and law.

That’s enough to reject NetChoice’s argument on this front. But if somehow any remaining vagueness exists in the specific harms that NetChoice challenges, it is fully “remedied” by the “reasonable care” limitation. *Munn v. City of Ocean Springs*, 763 F.3d 437, 441 (5th Cir. 2014).

### 3. “Design features”

i. NetChoice also attacks the Act’s requirement to disable unnecessary, covered design features. This requires covered online services to provide users easy access to opt out of “design features including, but not limited to, all covered design features, that are not necessary to provide the covered online service.” S.C. Code Ann. § 39-80-30(A)(1). The thrust of NetChoice’s vagueness argument is that “design feature,” as opposed to “covered design feature,” isn’t defined—meaning this provision could extend to boundless website features from font size to search bars. ECF 22-1, at 40. But that argument isolates the phrase “design features” from the statutory context in an effort to inject vagueness into a law where it isn’t.

Section 39-80-30(A)(1), like the rest of the Act, is concerned with engagement-maximizing product mechanics that drive compulsive use and result in significant harm. That’s why “covered design feature,” which *is* defined, encompasses services that “encourage or increase” a minor’s time online, including features like infinite scroll, auto-playing videos, gamification and the like. S.C. Code Ann. § 39-80-10(3). The Act repeatedly returns to that defined category. Covered services must exercise reasonable care in the design and operation of their services “including, but not limited to, covered design features.” *Id.* § 39-80-20(A). And annual reports must describe these features. *Id.* § 39-80-70(A)(6). This consistent emphasis demonstrates that the statute’s regulatory target is not arbitrary interface elements like font size, but the specifically defined class of engagement-driving features. *See Grayned*, 408 U.S. at 112 (the “purpose” of a statute can furnish the “particular context” in which “fair notice” can be evaluated for other terms).

So when 39-80-30(A)(1) opens with the technically broader “design features,” expressly inclusive of “all covered design features,” that does not create a new free-floating regulatory category. *See Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 162 (2012) (“includ[ing]”

is “illustrative, not exhaustive”). The most natural reading of this section is that “design features” captures the defined category of “covered design features” and functionally similar engagement-driving mechanisms that may not have been listed. After all, “covered design features” includes the same non-limited language in its definition. S.C. Code Ann. § 39-80-10(3).

**ii.** That brings up another underdeveloped argument NetChoice makes: It can’t tell when a feature is “necessary.” ECF 22-1, at 40. But the Act’s use of “necessary” reflects a functional, service-specific inquiry. Section 39-80-30(A)(1) asks whether a feature is “necessary to provide the covered online service,” which directs the analysis to the service’s core operation as delivered to users. A feature is “necessary” if it is integral to providing the service in a usable form; it is unnecessary if the service can operate coherently without it. That distinction maps directly onto the statute’s definition of “[c]overed design feature[s],” which identifies engagement-maximizing mechanics such as infinite scroll, autoplay, and engagement counters, S.C. Code Ann. § 39-80-10(3), which are not often required to deliver the service’s core functionality. “Necessary” is thus a “comprehensible normative standard.” *Cooper*, 842 F.3d at 842.

NetChoice can press this standard by saying certain covered design features like “notifications and push alerts” might be integral to providing a particular service. S.C. Code Ann. § 39-80-10(3)(e). Maybe that’s a tough case with some service. But the Act can’t be “void for vagueness [merely] because it is unclear in *some* of its applications to the conduct of . . . other hypothetical parties.” *Vill. of Hoffman Ests.*, 455 U.S. at 495. That’s the price of a facial challenge.

**iii.** What “disabling” unnecessary design features looks like under the Act is not vague either. ECF 22, at 40. Section 39-80-30(A)(1) requires services to “disable design features . . . by allowing users to opt out of the use of all such design features.” So while “disable” can be different things in context, this context makes clear what “disable” means here: “allow[] users to opt out.”

*See Williams*, 553 U.S. at 306 (“narrowing context” can eliminate vagueness). And opting out is a clear standard on its face. What it looks like in a particular circumstance is an as-applied problem.

iv. NetChoice last attacks the defined term “covered design feature” itself, saying it could “apparently refer[] to any design or content judgment a user might like.” ECF 22-1, at 40–41. That’s wrong. The statute defines “covered design feature” as features that “encourage or increase a minor’s frequency, time spent, or activity” on a covered online service and then provides a list of examples—such as infinite scroll, autoplay, and engagement counters—that illustrate that category. S.C. Code Ann. § 39-80-10(3). As the Supreme Court has explained, terms like “including” introduce illustrative examples, not an unbounded expansion of the category. *See Christopher*, 567 U.S. at 162. And under ordinary interpretive principles, general language is read in light of the examples that accompany it. *See Williams*, 553 U.S. at 294. That’s why a “statutory definition [that] provides a lengthy but unexhaustive list of what does and doesn’t” fall within its ambit gives “a person of ordinary intelligence . . . fair notice of what” the statute prohibits. *Cap. Associated Indus.*, 922 F.3d at 210–11. So far from meaning “any design . . . a user might like,” ECF 22-1, at 41, the term “covered design features” is narrowed by seven enumerated examples to encompass those features and related ones only.

#### 4. “Expressed preferences”

NetChoice’s claim that the Act provides “no guidance” as to what constitutes a user’s “expressed preferences” is incorrect. ECF 22-1, at 41. The Act defines that term as “a freely given, considered, specific, and unambiguous indication of a user’s preferences.” S.C. Code Ann. § 39-80-10(6)(a). It then goes further, expressly identifying what does *not* qualify, including inferences drawn from time spent on a service or routine user interactions like comments or reshares. *Id.* § 39-80-10(6)(b). That combination of affirmative definition and negative limitation provides precisely

the kind of guidance vagueness doctrine requires—especially in a facial challenge. *See Holder*, 561 U.S. at 21 (“add[itional] narrowing definitions . . . increase[] the clarity of the statute’s terms”).

These concepts that the statutory definition employs are not novel or indeterminate. They track familiar markers of voluntary, informed consent long recognized across the law. *See, e.g., Williams*, 553 U.S. at 306 (“[C]ourts and juries every day pass upon knowledge, belief and intent—the state of men’s minds—having before them no more than evidence of their words and conduct, from which, in ordinary human experience, mental condition may be inferred.”). NetChoice’s position would render vast swaths of consent-based regulation unconstitutional. At most, applying those standards may require judgment at the margins, but (once again) that is not a constitutional defect. *See Nat’l Dairy Prods. Corp.*, 372 U.S. at 32.

## 5. “Dark patterns”

NetChoice’s challenge to the Act’s prohibition on “dark patterns” is not really a vagueness argument. Other than a passing reference to “no guidance,” NetChoice primarily asserts that the definition could reach a broad range of expressive or persuasive design choices. *See* ECF 22-1, at 41. But that’s a First Amendment objection to the statute’s scope, not a claim that it lacks fair notice. *See Vill. of Hoffman Ests.*, 455 U.S. at 494–98 (treating overbreadth and vagueness distinctly). Its reliance on analogies to novels and operas only confirms the point. Those examples assume—rather than establish—that interface design is expressive, and then fault the statute for reaching too much of that activity. That’s a category error. The Act regulates the functional design of user interfaces, not the communicative content of expression, and NetChoice never defends the premise that “dark patterns” are speech at all. It does not advance that theory in its First Amendment claims, underscoring that the analogy is doing argumentative work unique to its vagueness challenge. And that matters for vagueness analysis: Heightened vagueness scrutiny is

reserved for laws regulating speech, not for ordinary conduct-based or economic regulation. *See Moody*, 603 U.S. at 723. Consistent with that distinction, courts have expressed skepticism that “dark patterns” constitute protected expression. *See, e.g., NetChoice, LLC v. Bonta*, 113 F.4th 1101, 1123 (9th Cir. 2024). If NetChoice seeks the benefit of heightened vagueness scrutiny, it must first establish that “dark patterns” are protected expressive conduct.

In any event, the definition itself is constrained. A “dark pattern” is not any interface design, but one “designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.” S.C. Code Ann. § 39-80-10(5). NetChoice isolates the word “subverting” while ignoring the limiting language that surrounds it. ECF 22-1, at 41. But read as a whole—and unlike the expressive analogies NetChoice invokes—the statute does not reach any design that merely influences user behavior. Instead, it targets interfaces deliberately structured to undermine a user’s decisionmaking, which confines the provision to calculated, outcome-oriented design choices, not ordinary efforts to engage users writ-large. Those features also supply the kind of narrowing context and scienter-like limitation that mitigate vagueness concerns. *See Vill. of Hoffman Ests.*, 455 U.S. at 498–99. At most, NetChoice suggests that companies may struggle to identify the exact point at which a design “cross[es] the line.” ECF 22-1, at 41. But (again) marginal cases do not render a statute facially vague. *See Cooper*, 842 F.3d at 842. And NetChoice’s quick citations to the declarations attached to its motion—which provide little substantive evidence or guidance on “dark patterns”—do not make their hypotheticals any less marginal. *See, e.g.,* ECF No. 22-3, at ¶ 61 (Cleland) (conclusorily saying that “‘dark patterns’ provides no guidance on when an interface crosses a line”) (cited at ECF No. 22-1, at 41). All of this makes “dark patterns” in the Act distinguishable from the California term was preliminarily enjoined. *See CA9 Bonta III*, 2026 WL 694471, at \*16 (problems included harms not defined,

“child” in singular, and lack of statutory guidance).

## **6. “Personal data”**

NetChoice says that if “personal data” means “any data that ‘alone or in combination with other information’ is linkable to a user,” then all data is “personal” because “*all* data is ‘linkable’ to a user via ‘other information.’” ECF 22-1, at 41. But NetChoice selectively quotes “linkable” and omits the definition’s narrowing context. “Personal data” does not include “other information” that is merely “linkable” to unique identifiers. It includes information that “is linked or reasonably linkable” to unique identifiers. S.C. Code Ann. § 39-80-10(11)(a). The full text supplies statutory bounds NetChoice overlooks and ends the vagueness argument where it begins.

### **D. NetChoice is unlikely to prevail on its preemption claims.**

Federal law controls over conflicting state law, U.S. Const. art. VI, cl. 2, and preemption comes in three forms: conflict, express, and field, *Murphy v. NCAA*, 584 U.S. 453, 477 (2018).

NetChoice bears the burden of proving preemption, *J.O.C. Farms, L.L.C. v. Fireman’s Fund Ins. Co.*, 737 F. App’x 652, 654 (4th Cir. 2018), and it must do so with a presumption *against* preemption because Congress has legislated in an area of “traditional state authority,” *GenBioPro, Inc. v. Raynes*, 144 F.4th 258, 271 (4th Cir. 2025). Thus, Congress’s intent to preempt States in these areas must be “clear and manifest.” *Id.*

### **1. Section 230 does not preempt the Act.**

Section 230 of the Communications Decency Act prohibits a “provider or user of an interactive computer service” from being “treated as the publisher or speaker of any information provided by another information content provider.” 47 U.S.C. § 230(c)(1). It permits enforcement of “any State law that is consistent with [section 230]” and prohibits bringing a cause of action or imposing liability that is “inconsistent” with that section. *Id.* § 230(e)(3).

Despite section 230’s “narrow focus,” “[s]ocial-media platforms have increasingly used § 230 as a get-out-of-jail free card.” *Doe Through Roe v. Snap, Inc.*, 144 S. Ct. 2493, 2493–94 (2024) (Thomas, J., dissenting from denial of certiorari, joined by Gorsuch, J.). Ironically, “[m]any platforms claim that users’ content is their own First Amendment speech,” but “[w]hen it comes time for platforms to be held accountable for their websites, . . . they argue the opposite.” *Id.* at 2494. These platforms—and NetChoice on behalf of a group of them—can’t have it both ways.

“When a federal law contains an express preemption clause, [courts] focus on the plain wording of the clause, which necessarily contains the best evidence of Congress’ preemptive intent.” *Chamber of Com. of U.S. v. Whiting*, 563 U.S. 582, 594 (2011) (internal quotation mark omitted). Here, section 230’s plain wording does not express an intent to preempt the Act because it bars only “inconsistent” State regulation—not *all* state regulation. 47 U.S.C. § 230(e)(3).

Thus, the analysis hinges on the definition of “inconsistent.” The Fourth Circuit has explained that the word “inconsistent” should be given “its ordinary dictionary meaning: ‘lacking consistency: incompatible, incongruous, inharmonious, so related that both or all cannot be true.’” *Goldfarb v. Mayor & City Council of Balt.*, 791 F.3d 500, 509–10 (4th Cir. 2015) (cleaned up). “[I]nconsistent” provisions must be “fundamentally at odds” and “direct[ly in] conflict.” *Id.* at 510.

That makes this a question of conflict preemption, *Metrophones Telecomm., Inc. v. Glob. Crossing Telecomm., Inc.*, 423 F.3d 1056, 1073 (9th Cir. 2005), and “[t]here are two types of conflict preemption,” *GenBioPro, Inc.*, 144 F.4th at 275. The type that NetChoice invokes is when state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress,” often called obstacle preemption. *Id.* (internal quotation marks omitted).

i. Because NetChoice relies on obstacle preemption, ECF No. 22-1, at 42, it must show that the Act is an “obstacle” to section 230’s “purposes and objectives.” *GenBioPro, Inc.*, 144 F.4th at

275. NetChoice cannot do so.

What are section 230's purposes and objectives? Go back to its origins. In "a 1995 New York state court case," "an interactive computer service" was subjected to publisher liability for "defamatory statements" posted on its bulletin boards. *Pinckney*, 127 F.4th at 523. Congress saw this as a "threat[ to] 'the vibrant and competitive free market that [existed] for the Internet and other interactive computer services.'" *Id.* (second alteration in original) (quoting 47 U.S.C. § 230(b)(2)). So Congress enacted section 230 to reverse the "imposition of tort liability on service providers for the communications of others." *Id.* at 524 (cleaned up).

At the same time, Congress also sought "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services." 47 U.S.C. § 230(b)(3). And Congress specifically aimed to "empower parents to restrict their children's access to objectionable or inappropriate online material." *Id.* § 230(b)(4).

The Act fits those purposes and objectives like a glove. *First*, the Act seeks to give parents control over what information their children receive and to empower parents to restrict access to objectionable online material. *See, e.g.*, S.C. Code Ann. § 39-80-50(A) (requiring covered online services to "provide parents with accessible and easy-to-use tools to help parents protect and support minors" online). It also equips schools to be partners in that process. *See, e.g., id.* § 39-80-60(A) (requiring a reporting mechanism for schools, parents, and minors).

*Second*, the Act does not hamper the competitive free market. It does not prevent anyone from accessing the internet or even a social media site. It simply requires service providers to set age-appropriate defaults for minors, which can be modified.

*Third*, the Act does not interfere with section 230's immunity. In fact, the Act explicitly

avoids conflict with section 230. *See* S.C. Code Ann. § 39-80-20(B). NetChoice acknowledges this in a single footnote. *See* ECF No. 22-1, at 44 n.8. And it tries to inject confusion into the Act’s meaning by claiming that “Section 230 does not allow liability for some harms but not others.” *Id.* But that’s exactly what section 230’s “narrow focus” does. *Snap, Inc.*, 144 S. Ct. at 2493 (Thomas, J., dissenting from the denial of certiorari, joined by Gorsuch, J.). For instance, section 230 contains specific carveouts for liability under both civil and criminal laws relating to sex trafficking. 47 U.S.C. § 230(e)(5). That alone is sufficient to puncture NetChoice’s fiction that “Section 230 does not allow liability for some harms but not others.” ECF No. 22-1, at 44 n.8; *see also NetChoice, LLC v. Reyes*, No. 2:23-CV-00911-RJS-CMR, 2024 WL 3510919, at \*9 (D. Utah July 22, 2024) (“NetChoice’s preemption argument stretches Section 230 immunity beyond what the plain text of the law supports.”).

Plus, section 230’s immunity is narrow in other ways. It “does not directly regulate the activities of interactive computer service providers” but “is addressed only to the bringing of a cause of action.” *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 334 (4th Cir. 1997). The Act, on the other hand, directly regulates the activities of interactive computer service providers. The Act regulates something that section 230 does not, so section 230 cannot preempt the Act.

As more proof that NetChoice’s preemption argument falls flat, read *Pinckney* (which NetChoice cites frequently) closely. Absent from the majority opinion in that case is the word “preemption.” Or “preempted.” Or “preempt.” In fact, Judge Rushing’s concurrence in part uses a variant of “preempt” only once. *Pinckney*, 127 F.4th at 529. And that concurrence argued that section 230 does *not* bar claims relating to a social media site recommending a group, person, or event because such recommendations are the site’s “own speech, not that of a third party.” *Id.* at 531. *Pinckney* therefore doesn’t do much for NetChoice.

ii. To bolster its preemption argument, NetChoice first looks to the Act's requirement that a covered online service exercise reasonable care, but it tries to paint that requirement as applying to "publishing third-party speech." ECF No. 22-1, at 44. The Act's text refutes that claim. The Act requires covered online services to "exercise reasonable care *in the use of a minor's personal data* and the *design and operation of the covered online service* including, but not limited to, *covered design features*." S.C. Code Ann. § 39-80-20(A) (emphasis added). The use of a minor's personal data has nothing to do with "publishing third-party speech." And section 230 says nothing about the use of a minor's data.

The Act's regulation of the design and operation of covered online services fares no worse. The Act defines "covered design features" and lists examples of covered design features, such as those that automatically load and display content. S.C. Code Ann. § 39-80-10(3). Requiring reasonable care in how websites are designed is not the same as assigning liability for published third-party speech. Section 230, of course, says nothing about website design.

NetChoice also lists various disablement tools and defaults the Act mandates and then makes the conclusory statement that those provisions relate to "aspects of websites' 'design and architecture' that are 'inextricably intertwined with [a website's] role as a publisher of third-party content.'" ECF No. 22-1, at 45. But NetChoice doesn't even try to explain *how* that is the case for the websites that NetChoice purports to represent. Such conclusory arguments are no basis for enjoining a validly enacted state law.

Lastly, NetChoice argues that the Act's restrictions on targeted advertising to minors violate section 230. *Id.* at 45–46. It claims that section 230 prohibits liability against "interactive service[] provider[s]" for third-party advertising and then blanketly states that the Act imposes liability "on third-party advertising." *Id.* (internal quotation mark removed). Not so. Under the Act,

covered online services “may not *facilitate* targeted advertising to minors,” S.C. Code Ann. § 39-80-40(C), and may not “*facilitat[e]* ads directed to minors for products prohibited for minors . . . to users the covered online services know are minors.” *Id.* § 39-80-60(B) (emphasis added). In other words, the Act does not impose liability “on third-party advertising.” It merely regulates service providers’ conduct by prohibiting them from *facilitating* targeted advertising to minors. Section 230 does not come into play.

## 2. COPPA does not preempt the Act.

The Children’s Online Privacy Protection Act (COPPA) sets minimum requirements for businesses that offer online services directed toward children under 13. Those requirements include obtaining parental consent before collecting, using, or disclosing children’s personal information; providing notice of their privacy policies; and giving parents the ability to review and change their children’s personal information collected by the operator. 15 U.S.C. §§ 6501–6506.

As with section 230, NetChoice argues that COPPA preempts the Act. *See* ECF No. 22-1, at 46. COPPA’s express preemption provision for state laws “inconsistent” with its provisions, 15 U.S.C. § 6502(d), also calls for an obstacle-preemption analysis, *see Jones*, 73 F.4th at 642.

And as with section 230, NetChoice is wrong because the Act poses no obstacle. COPPA’s “originally stated goals” are “to minimize the collection of personal information from children and create a safer, more secure online experience for them, even as online technologies, and children’s uses of such technologies, evolve.” 78 Fed. Reg. 3972-01, 3972 (Jan. 17, 2013). COPPA did not seek to shut out the States. In fact, COPPA specifically contemplates state attorneys general bringing civil actions as *parens patriae*. 15 U.S.C. § 6504(a)(1).

The Act’s objectives, if anything, complement COPPA’s purposes. The Act defines “parent” to have “the same meaning as defined in” COPPA. S.C. Code Ann. § 39-80-10(10). It

also defines “[r]easonably likely to be accessed by a minor” to include online services that are “directed to children as defined by” COPPA. *Id.* § 39-80-10(17)(a)(ii).

And yet the Act is not simply a copy of COPPA as applied to 13–17-year-olds. South Carolina sought to innovate and protect minors in new ways, but which are still consistent with COPPA’s objectives. For example, the Act restricts addictive features. *See, e.g., id.* §§ 39-80-30(A); 39-80-40(E). It also restricts personalized recommendation systems. *See, e.g., id.* §§ 39-80-30(B); 39-80-40(F); 39-80-60(D)).

COPPA’s express-preemption clause only bars “inconsistent” liability for “an activity or action described in this chapter,” which includes “collecting personal information from a child” under 13 years old. 15 U.S.C. § 6502(a)(1), (d). But the Act never imposes liability for “collecting personal information from a child” in a way “incompatible” with COPPA’s treatment of such actions. None of the challenged provisions—sections 39-80-20 through -40 and 39-80-60—are “incompatible” or “direct[ly in] conflict” with COPPA. *Goldfarb*, 791 F.3d at 510. NetChoice never even tries to explain how they could be.

Instead, NetChoice claims that the Act is “inconsistent” with COPPA because the Act imposes rules on minors unregulated by COPPA (13–17-year-olds) and because it “imposes several substantive requirements that COPPA does not.” ECF No. 1, ¶¶ 251–52. Of course, a law that covers collecting personal information from a child under 13 cannot be fundamentally at odds with a statute “regulat[ing] . . . minors aged 13 to 17.” ECF No. 1, ¶¶ 249, 251.

At most, NetChoice protests that the Act adds requirements on organizations that might also be separately subject to COPPA. *Id.* at ¶ 252. NetChoice not only ignores the Fourth Circuit’s definition of “inconsistent,” but also “read[s] the word ‘inconsistent’ out of COPPA’s preemption provision.” *Jones*, 73 F.4th at 642. Congress knew how to bar state requirements if it wanted to. It

has done so many times. *See, e.g.*, 15 U.S.C. §§ 780(i)(1), (2)(B); 7 U.S.C. § 136v(b). Here, it didn't do that. It barred only *inconsistent* state regulation.

This understanding is consistent with how other courts have read COPPA. For example, this Court has suggested that there would be no preemption issue if South Carolina regulated “conduct beyond that regulated by COPPA.” *Manigault-Johnson v. Google, LLC*, No. 2:18-cv-1032-BHH, 2019 WL 3006646, at \*6 (D.S.C. Mar. 31, 2019). That tracks with the Congressional Research Service's observation that COPPA “set a federal floor rather than a federal ceiling.” Chris D. Linebaugh, Cong. Rsch. Serv., R48667, Preemption and Privacy Law 6 (2025).

**E. NetChoice is unlikely to prevail on its Commerce Clause claim.**

NetChoice's Commerce Clause claim rests on the Dormant Commerce Clause. *See* ECF No. 22-1, at 50–53. Under that doctrine, “the Commerce Clause not only vests Congress with the power to regulate interstate trade; the Clause also contains a further, negative command” that forbids state regulations that impermissibly burden out-of-state industry and business. *Nat'l Pork Producers Council v. Ross*, 598 U.S. 356, 368 (2023) (cleaned up).

The Act doesn't facially discriminate against interstate commerce, so NetChoice “begin[s] in a tough spot.” *Id.* at 370. It can prevail only if the Act unduly burdens such commerce. *See Pike v. Bruce Church*, 397 U.S. 137, 142 (1970). *Pike* is a “deferential” two-part test. *Colon Health Ctrs. of Am., LLC v. Hazel*, 733 F.3d 535, 545 (4th Cir. 2013). A court first “looks at the legitimacy of the state's interest,” and then “weighs the burden on interstate commerce in light of the local benefit derived from the statute.” *PSINet, Inc. v. Chapman*, 362 F.3d 227, 240 (4th Cir. 2004).

NetChoice does not challenge the State's interest. Indeed, it already conceded that “South Carolina has a compelling interest in protecting minors.” ECF No. 22-1, at 30. And for good reason. “It is evident beyond the need for elaboration that a State's interest in safeguarding the

physical and psychological well-being of a minor is compelling.” *New York v. Ferber*, 458 U.S. 747, 756–57 (1982) (cleaned up). So this claim turns on the second part of the *Pike* balancing test.

On that front, NetChoice leans heavily on the idea that any state internet regulation will automatically unduly burden interstate commerce. But the Court has rejected this per se extraterritorial argument, saying it “falters out of the gate.” *Nat’l Pork Producers*, 598 U.S. at 371. [I]n “our interconnected national marketplace, many (maybe most) state laws have the ‘practical effect of controlling’ extraterritorial behavior,” *id.* at 374, so it’s no surprise that courts have rejected such arguments when it comes to the internet, *see, e.g., Quik Payday, Inc. v. Stock*, 549 F.3d 1302, 1312 (10th Cir. 2008); *SPGGC, LLC v. Blumenthal*, 505 F.3d 183, 195 (2d Cir. 2007).

*PSINet* is not to the contrary. For one, South Carolina’s Act is not a “blanket regulation of Internet material.” 362 F.3d at 240. The Act regulates how covered online services relate to users in South Carolina. For another, reading *PSINet* as a per se rule both overreads that holding and ignores more recent Supreme Court cases like *National Pork Producers*. Virtually everything that NetChoice says about the internet was also true of the pork producers in that case. And for a third, geographical identification and filtering technologies help businesses operating in multiple jurisdictions comply with the law in a way that was impossible in 2004. *See* Jack Goldsmith & Eugene Volokh, *State Regulation of Online Behavior: The Dormant Commerce Clause and Geolocation*, 101 Tex. L. Rev. 1083, 1107 (2023); McCoy Decl. ¶ 10.

Unable to rely on a per se rule, NetChoice turns to a hypothetical about someone’s aunt in California. ECF No. 22-1, at 51. That’s not enough. *Pike* still hews to the “antidiscrimination rule that lies at the core of [the Court’s] dormant Commerce Clause jurisprudence.” *Nat’l Pork Producers*, 598 U.S. at 377. *Pike* simply “serves as an important reminder that a law’s practical effects may also disclose the presence of a discriminatory purpose.” *Id.* If anything, NetChoice’s

hypothetical shows that the Act has no discriminatory motive. It doesn't treat out-of-state covered online services any differently than in-state ones. *See NetChoice, LLC v. Bonta*, 770 F. Supp. 3d 1164, 1214 (N.D. Cal. 2025) (rejecting Dormant Commerce Clause claim on preliminary injunction motion), *aff'd in part, vacated in part, CA9 Bonta III*.

**F. NetChoice is unlikely to prevail on its due process claim.**

NetChoice's procedural due process claim is merely an attempt to pause the Act so that its members (and the rest of the world) can take at least a year to comply with it. *See* ECF No. 22-1, at 53. This claim fails for at least three reasons.

*First*, courts have long rejected procedural due process challenges to legislative action. *See, e.g., Bi-Metallic Inv. Co. v. State Bd. of Equalization*, 239 U.S. 441, 445 (1915). In fact, courts have rejected the idea that procedural due process somehow requires a tolling period for new statutes. *See, e.g., Torres v. INS*, 144 F.3d 472, 475 (7th Cir. 1998).

The few cases NetChoice cites on this front change nothing. Start with its lead authority, *Pacific Telephone & Telegraph Co. v. City of Seattle*, 291 U.S. 300 (1934). That case was a vagueness challenge, which was ultimately dismissed on ripeness. *See id.* at 301, 304. Any suggestion that due process requires a reasonable "opportunity to comply" was dicta without meaningful discussion. Or consider *Planned Parenthood Great Northwest v. Cameron*, 599 F. Supp. 3d 497 (W.D. Ky. 2022). The analysis there largely focused on a purported violation of *substantive* due process about abortion pre-*Dobbs*. *Id.* at 507. Hardly an on-point authority.

*Second*, NetChoice provides little detail about how long compliance would supposedly take. Once again, it cites some paragraphs of the declarations without much (if any) discussion. Nor does NetChoice explain the specific challenges facing its members. Generalized assertions cannot be enough to enjoin the entire Act for a year or more—particularly when NetChoice has

agreed that “South Carolina has a compelling interest in protecting minors.” ECF No. 22-1, at 30. Plus, “[c]ompliance with the Act isn’t some Herculean engineering feat” but would be “straightforward” based on existing technology. McCoy Decl. ¶ 10.

*Third*, any due process argument ignores the lack of an enforcement action against anyone. See *Thomas v. City of New York*, 143 F.3d 31, 35 (2d Cir. 1998).

## **II. The other factors do not support granting a preliminary injunction.**

NetChoice argues that because it is likely to succeed on its claims, the remaining “preliminary injunction factors tip in its favor.” See ECF No. 22-1, at 53. Aside from assuming the merits, that gets the law wrong. The four-factor test for a preliminary injunction “is supposed to set a high bar” because a preliminary injunction represents drastic relief. *Am. Fed’n of Tchrs.*, 152 F.4th at 169. The bar is high in part because a movant must carry its burden of persuasion by a “clear showing.” *Id.* And it is high in part because of its “asymmetry”: “[E]very factor” must be met before a court may grant a preliminary injunction. *Id.*

### **A. NetChoice will not suffer irreparable harm.**

To show irreparable harm, NetChoice points to its alleged First Amendment injuries and compliance costs associated with the Act. See ECF No. 22-1, at 53–54. But courts have repeatedly said that compliance costs are generally insufficient to establish irreparable harm at this stage. In fact, one district court rejected NetChoice’s precise argument, explaining that “unrecoverable compliance costs may represent a harm—perhaps even a substantial one—but that does not mean that such harm is irreparable for purposes of the preliminary-injunction analysis.” *NetChoice v. Skrmetti*, No. 3:24-CV-01191, 2025 WL 1710228, at \*14 (M.D. Tenn. June 18, 2025).

Turning to its purported First Amendment injury, although it may be true that the loss of First Amendment freedoms might constitute irreparable injury, NetChoice still retains the burden

of proving the constitutional violation. And as explained, NetChoice has failed to meet this burden.

Further undermining any claim of irreparable harm is that the Attorney General has not “instituted or even threatened” an enforcement action against any of NetChoice’s members. *Id.* at

\*11. NetChoice’s members therefore do not face a “certain and immediate” threat. *Id.*

**B. The remaining factors cut against an injunction.**

Although the last two requirements merge when the government is the party opposing the injunction, *Nken v. Holder*, 556 U.S. 418, 435 (2009), NetChoice retains the burden to “clear[ly] show[.]” that both factors are met, *Am. Fed’n of Tchrs.*, 152 F.4th at 169. It has not done so.

NetChoice generally points to the importance of “access” to the internet and avoiding its “balkanization.” ECF No. 22-1, at 54. It also points to its own potential choice to “turn off the lights for minors in South Carolina” rather than comply with the Act. *Id.* at 55. These arguments are unconvincing. For one, NetChoice has not clearly shown how the Act would unduly limit internet access or contribute to its balkanization. For another, NetChoice’s own business decisions should not play into this Court’s analysis. *Cf. Pennsylvania v. New Jersey*, 426 U.S. 660, 664 (1976) (a litigant may not “complain about damage inflicted by its own hand”).

Making matters worse, these arguments minimize the “irreparable harm on the State” from not being able “to enforce its duly enacted” law. *Abbott v. Perez*, 585 U.S. 579, 602 n.17 (2018). And they outright ignore the State’s interest in protecting minors online “even when the laws have operated in the sensitive area of constitutionally protected rights.” *Ferber*, 458 U.S. at 757.

But it’s not just the harm to the State. It’s also the harm to minors. Being addicted to social media sites is harmful, and predators lurk online. *See Haidt, supra*, at 11; Edelson Decl. ¶¶ 19–22, 24–26; McCoy Decl. ¶ 14. The Court shouldn’t make young South Carolinians suffer while giant internet companies litigate their ability to maximize the time these young people spend online.

### III. NetChoice seeks relief the Court cannot grant.

NetChoice demands that the Court enjoin the Act “on its face.” ECF No. 22-1, at 55. This is a request to enjoin Defendants from enforcing the law against anyone: a universal injunction.

But the Court cannot grant such relief. “A universal injunction can be justified only as an exercise of equitable authority, yet Congress has granted federal courts no such power.” *Trump v. CASA, Inc.*, 606 U.S. 831, 841 (2025). Courts can’t issue injunctions that “are broader than necessary to provide complete relief to each plaintiff with standing to sue.” *Id.* at 861.

NetChoice doesn’t engage with this issue at all. Instead, it simply says: *facial challenge!* ECF No. 22-1, at 55–56. That’s not enough. The Fourth Circuit has recognized that *CASA* changes how courts think about injunctive relief on facial challenges. *United States v. Lierman*, 151 F.4th 530, 543 (4th Cir. 2025). Courts must “tailor equitable relief ‘to each plaintiff.’” *Id.* (quoting *CASA*, 606 U.S. at 861). That’s true even when the plaintiff is an “association[] with many members” and when it may be “hard to tell how far an injunction can sweep to give [that] Plaintiff[] ‘complete relief.’” *Id.* (quoting *CASA*, 606 U.S. at 853).

So however the Court might grant injunctive relief to give complete relief to NetChoice’s members, that relief cannot extend to nonparties except in “incidental” ways. *CASA*, 606 U.S. at 852. Enjoining any enforcement of the Act doesn’t incidentally benefit nonparties. It gives them complete relief, no different from what NetChoice’s members get.

### CONCLUSION

The Court should deny the Motion for Preliminary Injunction.<sup>4</sup>

---

<sup>4</sup> The Governor and Attorney General request that the Court stay any injunction pending appeal under Federal Rule of Civil Procedure 62 and Federal Rule of Appellate Procedure 8(a)(1).

Respectfully submitted,

s/Thomas T. Hydrick

Thomas T. Hydrick (Fed. Bar. No. 13322)

*Solicitor General*

Joseph D. Spate (Fed. Bar. No. 13100)

*Deputy Solicitor General*

OFFICE OF THE

SOUTH CAROLINA ATTORNEY GENERAL

1000 Assembly St.

Columbia, South Carolina 29201

(803) 734-4127

thomashydrick@scag.gov

josephspate@scag.gov

*Counsel for Attorney General Wilson*

s/Wm. Grayson Lambert

Wm. Grayson Lambert (Fed. Bar No. 11761)

*Chief Legal Counsel*

Erica W. Shedd (Fed. Bar No. 13206)

*Deputy Legal Counsel*

Tyra S. McBride (Fed. Bar No. 13324)

*Deputy Legal Counsel*

Cameron R. Cox (Fed. Bar No. 14698)

*Deputy Legal Counsel*

OFFICE OF THE GOVERNOR

South Carolina State House

1100 Gervais Street

Columbia, South Carolina 29201

(803) 734-2100

glambert@governor.sc.gov

eshedd@governor.sc.gov

tmcbride@governor.sc.gov

ccox@governor.sc.gov

*Counsel for Governor McMaster*

April 6, 2026

Columbia, South Carolina

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF SOUTH CAROLINA  
COLUMBIA DIVISION**

NETCHOICE, LLC,

*Plaintiff,*

v.

ALAN WILSON, in his official capacity as  
South Carolina Attorney General,

*Defendant,*

and

HENRY DARGAN McMASTER, in his  
official capacity as Governor of the  
State of South Carolina,

*Intervenor-Defendant.*

Civil Action No.: 3:26-cv-543-sal

**DECLARATION OF  
LAURA EDELSON, PH.D.**

I, Laura Edelson, Ph.D., declare and state as follows:

1. I submit this declaration in support of Defendants’ Opposition to Plaintiff’s Motion for Preliminary Injunction.

**BACKGROUND AND QUALIFICATIONS**

2. I am an Assistant Professor of Computer Science at Northeastern University. My research focuses on large online networks, including the algorithmic systems used by social media platforms, user safety systems and algorithms, and user-facing transparency systems and tools.

3. I received a Ph.D. in Computer Science from New York University in 2022 and a B.S. in Computer Science from Pace University in 2008. My curriculum vitae, which sets forth my experience and credentials more fully, is attached as Exhibit A.

4. My research and professional work have focused on how large online platforms are designed and operated, including how they rank, recommend, and present content to users; how they measure and moderate user activity; and how platform design choices affect user experience, transparency, and safety. Before joining Northeastern University, I served as Chief Technologist of the Antitrust Division of the United States Department of Justice.

5. My recent work includes scholarship directly relevant to the issues in this case. In 2025, I co-authored “A Comparative Survey of Algorithmic Feed Recommendation System Designs,” published in *ACM Transactions on Recommender Systems*, which surveys how major social media platforms design and operate algorithmic feed systems.<sup>1</sup>

6. I have also authored and co-authored work concerning platform governance, transparency, and moderation systems, including “Measurement and Metrics for Content Moderation: The Multidimensional Metrics of Engagement and Content Removal on Facebook” which develops a framework for measuring the efficacy of content moderation and applies that framework to measure the impact on user experience of content removal on Facebook.<sup>2</sup> To conduct this survey and related systems and algorithm audits, I relied heavily on source code analysis in cases where platforms made the code for their services publicly inspectable and patent analysis in cases where they did not.

7. I have also co-authored research on youth safety features on social media platforms, including the report “Teen Accounts, Broken Promises: How Instagram is Failing to Protect

---

<sup>1</sup> Edelson, L., Haugen, F., & McCoy, D. (2025). A Comparative Survey Of Algorithmic Feed Recommendation System Designs. *ACM Transactions on Recommender Systems*.

<sup>2</sup> Edelson, L., Kovba, B., Yershova, H., Botelho, A., McCoy, D., & Lauinger, T. (2025). Measurement and Metrics for Content Moderation: The Multi-Dimensional Dynamics of Engagement and Content Removal on Facebook. *Journal of Online Trust and Safety*, 2(5).

Minors,” which evaluates whether Instagram’s publicly described youth-safety features operate as represented in practice.

8. Prior to my academic career, I worked as a software engineer at multiple companies, ending my industry career at Palantir. During this time, I became well acquainted with general industry practices of software engineering, and professional ethics within this domain.

9. My opinions in this declaration are based on my education, training, research, professional experience, and review of the materials identified in this declaration, including the South Carolina Age-Appropriate Code Design Act (“Act”), a number of patents describing the design features at issue, and other technical materials discussed below.

10. I am being compensated in this matter at an hourly rate of \$400 per hour. My compensation is not contingent on the outcome of this case.

#### **SUMMARY OF OPINIONS**

11. The covered design features identified in the Act do not describe a single, uniform type of technology. They instead refer to materially different kinds of product features, including interface mechanics, monetization mechanics, displayed informational features, and features that alter visual content. Understanding how the Act operates in practice requires attention to the concrete technical facts of how a particular feature is actually implemented on a particular service.

12. The most technically accurate way to evaluate the covered design features is to read each one narrowly, using patents or other authoritative technical materials to identify what the feature is and how it works. When the features are analyzed in that way, the understanding of fit between a feature and the Act’s enumerated harms can be feature-specific rather than uniform. Some features are most specifically related to compulsive usage, while others are more specifically

related to material financial injury, or psychological harm. The available research support for those relationships also varies by feature.

13. Additionally, the services operated by different NetChoice members are themselves not uniform, and the analysis of which members' services are implicated by the act is most accurately determined by an evaluation of the presence or absence of each covered design feature in that member's service. A full analysis of the services of all NetChoice members is beyond the scope of this declaration, but at minimum some NetChoice members operate services that employ only one covered design feature, while others operate services that employ all of them.

14. The covered design features named in the Act fall into three categories. I perform a full analysis of each feature in the sections below, but to summarize: First, infinite scroll, autoplay, and notifications are non-expressive interface mechanics. They do not create, alter, or present user-generated content. Instead, they control how content is delivered (infinite scroll, autoplay) or how users are prompted to return to the service (notifications). Each of these features is most directly associated with the Act's enumerated harm of compulsive usage. Infinite scroll and autoplay work by removing stopping cues that would otherwise naturally prompt a user to decide whether to continue, while notifications work by providing service-initiated re-entry cues that pull users back into the service from outside.

15. Second, in-game purchases are a monetization feature that involves, in part, commercial creative content in the form of purchase interfaces and virtual currency systems. In-game purchases are most directly associated with material financial injury, particularly where virtual currency obscures real cost or where chance-based mechanics encourage repeated spending. In the form of variable-ratio reward purchase mechanics such as loot boxes, they are additionally associated with compulsive use and at-risk and problem gambling in adolescents.

16. Third, gamification, quantification of engagement, and appearance-altering filters each involve the creation or presentation of new non-commercial content to users, in the form of badges, streak warnings, and leaderboards (gamification), visible numerical counts of user engagement (quantification of engagement), or digitally altered depictions of the user's own face (appearance-altering filters). Among these, gamification is most directly associated with compulsive usage through reinforcement, goal progress, and loss avoidance. Quantification of engagement is associated with compulsive usage through visible social reward feedback. Appearance-altering filters are associated with severe psychological harm and severe emotional distress particularly for adolescents through self-objectification, appearance comparison, and the internalization of digitally generated beauty ideals.

17. In my field, it is ordinary to evaluate foreseeable user risks and to consider alternative designs that reduce or mitigate those risks. That understanding is consistent with established professional norms in computing. For example, the Association for Computing Machinery Code of Ethics and Professional Conduct states that computing professionals should “avoid harm,” explains that avoiding harm begins with careful consideration of the potential impacts of technical decisions on affected people, and separately emphasizes responsibilities to respect privacy and to use personal information only for legitimate ends.<sup>3</sup> In my opinion, the idea that designers and operators of online services should consider foreseeable harms associated with product features and data usage is consistent with established professional practice in computing.

---

<sup>3</sup> ACM, *ACM Code of Ethics and Professional Conduct* (2018), <https://www.acm.org/code-of-ethics>.

## INFINITE SCROLL

18. The most authoritative technical source for infinite scroll is the Facebook patent family filed by Parker, Odio, and Mosseri: US20120011430A1, “Infinite Scrolling” (filed July 9, 2010), and its continuation, US10055507B2 granted August 21, 2018.<sup>4,5</sup> This patent explains that when a user initially loads a social network website with many embedded items, the site might initially render only some of them. Then, as the user navigates the page by scrolling down, the website loads more items. To create the impression of a continuous feed of content, the system uses “place markers” so that the scrollbar reflects where the user is in an ever-growing feed. Fundamentally, infinite scroll changes the user interface so that more items load when the user scrolls either by swiping on a phone screen or using a mouse instead of requiring the user to click a "next page" button, as was the standard web design prior to this patent. The feature does not create new content or alter the presentation or appearance of user-generated content. Alternative designs remain widely used. The historically standard alternative is paginated loading, in which content is delivered in discrete pages with an explicit “next page” or “load more” button. That design has a natural stopping cue between batches of content, without changing the underlying content, the recommendation algorithm, or the user’s ability to access all the same material. Paginated feeds remain common across e-commerce sites, search engines, and many other web applications.

19. The direct research on infinite scroll is limited but points in a consistent direction. Rixen et al. (2023), in a study published in *Proceedings of the ACM on Human-Computer*

---

<sup>4</sup> U.S. Patent Application No. 2012/0011430 A1, *Rendering Structured Documents with Place-Markers* (Parker et al., assigned to Facebook, Inc., filed July 9, 2010; published Jan. 12, 2012), <https://patents.google.com/patent/US20120011430A1/en>.

<sup>5</sup> U.S. Patent No. 10,055,507 B2, *Infinite Scrolling* (Parker et al., assigned to Facebook, Inc., granted Aug. 21, 2018), <https://patents.google.com/patent/US10055507B2/en>.

*Interaction*, investigated how people actually experience infinite scrolling in social media apps.<sup>6</sup> They found that users frequently described infinite scroll as a loop, with their sessions stretched on until something outside the app, like a phone call or a physical need, broke the cycle. Natarajan (2024), in a study of teenagers published in the *International Journal of Communication*, found that teens often try to create their own stopping points to counteract what the author describes as the frictionless design of social media feeds.<sup>7</sup> The literature supports a concern that infinite scroll can create a pattern of what Rixen et al. term “regretful use,” which young users report as difficult to disengage from, leading them to sometimes adopt external or self-imposed mechanisms to stop.

20. The behavioral mechanism at play is straightforward: When people do something repeatedly, whether they continue or stop is influenced by cues in their environment. Wood and Neal (2007), in a widely cited paper in *Psychological Review*, describe how behaviors become habitual through repeated pairing with contextual cues.<sup>8</sup> Once the association is strong enough, encountering the context can trigger the behavior without much conscious deliberation.

21. This literature is relevant to infinite scroll because the nature of the feature is that it removes stopping cues. In a paginated design, the user reaches the bottom of a page and must decide whether to click to the next one, creating a cue for a moment of decision. Infinite scroll eliminates that moment. The same easy action that the user is performing to navigate the page (scrolling) is overloaded, and now additionally retrieves the next batch of content with no pause, eliminating user choice in the matter of whether to load more content or not. Research from other behavioral domains, including eating, smoking, and cannabis use supports the idea that the

---

<sup>6</sup> Rixen, J. O., Meinhardt, L. M., Glöckler, M., Ziegenbein, M. L., Schlothauer, A., Colley, M., ... & Gugenheimer, J. (2023). The loop and reasons to break it: Investigating infinite scrolling behaviour in social media applications and reasons to stop. *Proceedings of the ACM on Human-Computer Interaction*, 7(MHCI), 1-22.

<sup>7</sup> Natarajan, N. (2024). Do they stop? How do they stop? Why do they stop? Whether, how, and why teens insert “frictions” into social media’s infinite scroll. *International Journal of Communication*, 18, 20-20.

<sup>8</sup> Wood, W., & Neal, D. T. (2007). A new look at habits and the habit-goal interface. *Psychological review*, 114(4), 843.

presence or absence of such cues impacts human behavior.<sup>9,10,11</sup> These studies demonstrate the broader point that whether a person continues or stops a repeated behavior is materially affected by whether their environment provides cues to pause.

22. Infinite scroll is most connected to the Act's enumerated harm of compulsive usage, which the Act defines as, "persistent and repetitive use of a covered online service that substantially limits one or more major life activities, including sleeping, eating, learning, reading, concentrating, communicating, or working."<sup>12</sup> The connection is direct: The design keeps the session going by removing the natural cues that would otherwise prompt a user to decide whether to continue, and it turns the same action the user employs to navigate the page into the trigger for the next load of content.

## **AUTOPLAY VIDEOS**

23. The authoritative technical source describing autoplay is Google's US9071867B1 filed by Ray and Lewis, "Delaying automatic playing of a video based on visibility of the video" (filed July 17, 2013).<sup>13</sup> This patent describes a system that monitors how much of a video player is visible on the user's screen. When the video player becomes sufficiently visible, for example because the user has scrolled down to it in a feed, the system automatically begins playing the video. When the video is no longer visible, the system pauses it. In practical terms, this means that

---

<sup>9</sup> McGreen, J., Kemps, E., & Tiggemann, M. (2024). The effectiveness of Go/No-Go and Stop-Signal training in reducing food consumption and choice: A systematic review and meta-analysis. *Appetite*, 195, 107215. <https://doi.org/10.1016/j.appet.2024.107215>

<sup>10</sup> Hughes, J. R., Naud, S., Fingar, J. R., Callas, P. W., & Solomon, L. J. (2015). Do environmental cues prompt attempts to stop smoking? A prospective natural history study. *Drug and Alcohol Dependence*, 154, 146-151. <https://doi.org/10.1016/j.drugalcdep.2015.06.044>

<sup>11</sup> Hughes, J. R., Naud, S., Budney, A. J., Fingar, J. R., & Callas, P. W. (2016). Environmental cues and attempts to change in daily cannabis users: An intensive longitudinal study. *Drug and Alcohol Dependence*, 161, 15-20. <https://doi.org/10.1016/j.drugalcdep.2015.09.033>

<sup>12</sup> S.C. Code Ann. § 39-80-10(1)

<sup>13</sup> U.S. Patent No. 9,071,867 B1, *Delaying Automatic Playing of a Video Based on Visibility of the Video* (Ray & Lewis, assigned to Google Inc., granted June 30, 2015), <https://patents.google.com/patent/US9071867B1/en>.

as a user scrolls through a social media feed or navigates through a set of videos, each video begins playing on its own as it comes into view, without the user pressing a play button. Similar to infinite scroll, autoplay is fundamentally a user interface mechanism that starts and stops video playback in response to the user scrolling, instead of a button click. It is an interface design choice that, like infinite scroll, removes a stopping cue from that interface. Alternate designs are possible and remain widely used across the internet: most simply, video playback can be initiated when the user clicks a “play” button.

24. Schaffner et al. (2025), in an experimental study of 76 U.S. Netflix users published in *Proceedings of the ACM on Human-Computer Interaction*, found that when autoplay was disabled, participants watched on average about 21 fewer minutes per day and their sessions were roughly 17 minutes shorter.<sup>14</sup> A second study by Chen et al. (2024), published in the *International Journal of Human-Computer Studies* with 394 participants, examined different modes of autoplay on a video platform.<sup>15</sup> The authors found that autoplay increased inattentiveness to the content being recommended and heightened participants' perception of being drawn into a “rabbit hole” of continued viewing.

25. Autoplay operates through the same basic mechanism described above for infinite scroll: It removes a stopping cue. Without autoplay, when one video ends, there is a pause, and the user must decide whether to play the next video and press a button to do so. That pause is a moment of decision, a natural point at which the user might choose to stop. Autoplay eliminates that

---

<sup>14</sup> Schaffner, B., Ulloa, Y., Sahni, R., Li, J., Cohen, A. K., Messier, N., Gao, L., & Chetty, M. (2025). An Experimental Study of Netflix Use and the Effects of Autoplay on Watching Behaviors. *Proceedings of the ACM on Human-Computer Interaction*, 9(2), 1-22. DOI 10.1145/3710928 <https://dl.acm.org/doi/abs/10.1145/3710928>

<sup>15</sup> Chen, C., Kang, J., Sajjadi, P., & Sundar, S. S. (2024). Preventing users from going down rabbit holes of extreme video content: A study of the role played by different modes of autoplay. *International Journal of Human-Computer Studies*, 190, 103303. DOI 10.1016/j.ijhcs.2024.103303 <https://www.sciencedirect.com/science/article/pii/S1071581924000879>

moment, so the next video begins on its own, and the user's only options are to keep watching (which requires no action at all) or to actively intervene to stop. The broader behavioral literature on stopping cues, described in the infinite scroll section above, applies here as well. Autoplay removes the natural cue to the user to consider whether they want to continue use by initiating playback of a video from an action the user took to navigate the site. Here again, the cross-domain evidence from McGreen et al. (2024) on response inhibition and from Hughes et al. (2015, 2016) on environmental cues and stopping behavior further supports the general principle that whether a person continues or stops a repeated behavior depends in part on whether they encounter cues to pause.<sup>16, 17, 18</sup>

26. Again, similar to infinite scroll, autoplay is most connected to the Act's enumerated harm of compulsive usage. The connection is supported by direct experimental evidence. The Netflix study shows that when the feature is turned off, people watch less and their sessions are shorter. The mechanism is also straightforward. Autoplay removes the pause between videos that would otherwise give the user a natural moment to decide whether to continue.

## GAMIFICATION

27. The authoritative technical source for gamification is Wu's US9105044B2, "Gamification for online social communities" (filed March 21, 2013), and its related patent family.<sup>19</sup> This patent describes a system designed to increase user participation in an online

---

<sup>16</sup> McGreen, J., Kemps, E., & Tiggemann, M. (2024). The effectiveness of Go/No-Go and Stop-Signal training in reducing food consumption and choice: A systematic review and meta-analysis. *Appetite*, 195, 107215. <https://doi.org/10.1016/j.appet.2024.107215>

<sup>17</sup> Hughes, J. R., Naud, S., Fingar, J. R., Callas, P. W., & Solomon, L. J. (2015). Do environmental cues prompt attempts to stop smoking? A prospective natural history study. *Drug and Alcohol Dependence*, 154, 146-151. <https://doi.org/10.1016/j.drugalcdep.2015.06.044>

<sup>18</sup> Hughes, J. R., Naud, S., Budney, A. J., Fingar, J. R., & Callas, P. W. (2016). Environmental cues and attempts to change in daily cannabis users: An intensive longitudinal study. *Drug and Alcohol Dependence*, 161, 15-20. <https://doi.org/10.1016/j.drugalcdep.2015.09.033>

<sup>19</sup> U.S. Patent No. 9,105,044 B2, *Gamification for Online Social Communities* (Wu, assigned to Lithium Technologies, Inc., granted Aug. 11, 2015), <https://patents.google.com/patent/US9105044B2/en>.

community by adding gameplay-like elements to the experience. The system measures how much a user participates, and then provides feedback through several different interfaces. These include achievement badges awarded when a user's activity crosses certain thresholds, leaderboards that rank users against one another, time-limited missions that ask a targeted group of users to complete specific actions by a deadline, and trophies for sustained high performance, such as remaining on a leaderboard for five consecutive weeks. In practical terms, the system converts ordinary participation into a structured cycle of measurement, progress tracking, feedback, and reward, all designed to encourage users to come back and participate more over time. It does not create, alter, or present user-generated content. However, while some elements of gamification (tracking user participation) are non-expressive, other elements involve creating and presenting new content to users, typically in the form of badges or other design elements that reward users for participation and warning or error messages that incentivize users to participate by threatening the loss of a "streak," or in the form of leaderboards that create an overall presentation of users' ranking, enabling social comparison as a tool to incentivize participation.

28. Alternative designs are possible. Services can provide the same underlying content and social features without attaching streak counters, mission timers, or leaderboards to participation. They additionally could retain incentives for new participation that are not associated with previous participation. Some services already offer versions of their products without these features, or allow users to disable streak notifications. The gamification layer can be removed without altering the content, the social connections, or the core functionality of the service.

29. The empirical literature strongly supports the understanding that gamified reward systems can increase how often and how much people use a service. Garaialde, Cox, and Cowan (2021), in two online studies, found that users selected applications more frequently when rewards

were placed closer to the beginning of the interaction, and that this effect held for both monetary rewards and for gamified, points-based leaderboard rewards.<sup>20</sup> Lindström et al. (2021), in a study published in *Nature Communications*, found that behavior on social media follows the same patterns predicted by reward-learning theory.<sup>21</sup> Their accompanying experiment confirmed that manipulating social rewards caused changes in behavior in the predicted direction.

30. Behaviorally, gamification works through a different mechanism than infinite scroll or autoplay. Instead of extending use by removing stopping cues, gamification works by turning participation itself into a goal to pursue, preserve, and avoid losing. A streak, badge, or mission gives the user something to earn and something to protect, which creates its own reason to return and continue. Three main lines of research help explain this mechanism. First, the reward-learning research described above (Lindström et al., 2021) establishes that social rewards on platforms can shape subsequent behavior in ways consistent with well-established principles of how people learn from rewards. Second, research on goal progress helps explain why partially completed goals are motivating. Nunes and Drèze (2006) found that giving people artificial advancement toward a goal (i.e., pre-stamping a loyalty card) increased their persistence and decreased the time it took them to complete the goal.<sup>22</sup> The key insight is that a goal that feels partly underway is more motivating than one that has not yet begun. Streaks and badge ladders work through similar logic. They make progress visible, which can motivate further repetition to maintain or extend that progress. Third, the research on streaks specifically sharpens the point. Silverman and Barasch (2024), across seven

---

<sup>20</sup> Garaialde, D., Cox, A. L., & Cowan, B. R. (2021). Designing gamified rewards to encourage repeated app selection: Effect of reward placement. *International Journal of Human-Computer Studies*, 153, 102661. DOI: 10.1016/j.ijhcs.2021.102661

<sup>21</sup> Lindström, B., Bellander, M., Schultner, D. T., et al. (2021). A computational reward learning account of social media engagement. *Nature Communications*, 12, 1311. DOI: 10.1038/s41467-020-19607-x.

<sup>22</sup> Nunes, J. C., & Drèze, X. (2006). The Endowed Progress Effect: How Artificial Advancement Increases Effort. *Journal of Consumer Research*, 32(4), 504–512. DOI: 10.1086/500480.

studies, found that when people were shown that they had an intact streak in their behavioral history, they were more likely to continue the behavior than when they were shown a broken streak, even when their actual prior behavior was identical in both conditions.<sup>23</sup> That finding is directly relevant to streak-based design on social media platforms, where maintaining a streak (such as Snapchat’s “Snapstreaks”) can become a motivation independent of the underlying activity.

31. Gamification’s direct connection to the Act’s enumerated harm of compulsive usage is well supported in the literature. The youth-specific evidence most closely connected to the statutory language comes from van Essen and Van Ouytsel (2023), in a study of 2,483 early adolescents published in *Telematics and Informatics Reports*. That study found that engagement in Snapchat streaks was associated with repetitive, problematic smartphone use. It also reported correlations between “streak intensity” and “fear of missing out.” The connection runs through the mechanisms described above: gamification converts ordinary participation into tracked, rewarded goal pursuit, which gives users reasons to return and repeat their activity that are independent of the content itself. A user maintaining a streak or working toward a badge may continue using the service not because of what the service is showing them, or their enjoyment of the service, but because breaking the streak or missing the badge would feel like a loss.

## **QUANTIFICATION OF ENGAGEMENT**

32. Unlike other covered design features, there is no single patent that defines the basic technical construction of quantification of engagement. The clearest description comes from academic literature on social media design. Ljungberg, Stenmark, and Zaffar (2017) describe social buttons generally as single-click actions whose results are rendered into visible

---

<sup>23</sup> Silverman, J., & Barasch, A. (2023). On or Off Track: How (Broken) Streaks Affect Consumer Decisions. *Journal of Consumer Research*, 49(6), 1095–1117. DOI: 10.1093/jcr/ucac029

measurements.<sup>24</sup> The feature works in three steps. First, a user performs a standardized interaction, such as liking, reacting, viewing, or clicking on a piece of content. Second, the platform records that interaction as a discrete event associated with the content item. Third, the platform displays an aggregate numerical value next to the content item, visible to other users. This feature presents new content to users, in the form of the numerical counts displayed. That displayed number is itself an informational statement, distinct from the underlying post.

33. The research on visible engagement metrics has been conducted primarily against measurement of “Likes.” Martinez-Pecino and Garcia-Gavilán (2019), in a study published in *Cyberpsychology, Behavior, and Social Networking*, found that likes affected problematic Instagram use among teenagers, with self-esteem moderating the relationship.<sup>25</sup> Teenagers with lower self-esteem were more susceptible to problematic use patterns associated with like-seeking behavior. A 2025 systematic review by Dores et al., published in *Healthcare*, examined the effects of social feedback through the Like feature on brain activity.<sup>26</sup> The review concluded that positive social feedback through likes activates reward-related neural systems and influences subsequent online interaction. That finding is consistent with the reward-learning account described in the gamification section.

34. The mechanism for quantification of engagement is social reward and social comparison. Unlike gamification, which works primarily through reinforcement and goal progress, visible engagement counts work by providing users with a public, numerical signal of social approval or attention attached to their content or to the content they view. For the user who posts

---

<sup>24</sup> Ljungberg, J., Stenmark, D., & Zaffar, F. O. (2017, July). Like, share and follow: A conceptualisation of social buttons on the web. In *Scandinavian Conference on Information Systems* (pp. 54-66).

<sup>25</sup> Martinez-Pecino, R., & Garcia-Gavilán, M. (2019). Likes and problematic Instagram use: the moderating role of self-esteem. *Cyberpsychology, Behavior, and Social Networking*, 22(6), 412-416.

<sup>26</sup> Dores, A. R., Peixoto, M., Fernandes, C., Marques, A., & Barbosa, F. (2025, January). The effects of social feedback through the “like” feature on brain activity: a systematic review. In *Healthcare* (Vol. 13, No. 1, p. 89). MDPI.

content, a visible like count functions as feedback. A high count signals approval; a low count can signal rejection or indifference. This creates an incentive to check back, to monitor how a post is performing, and potentially to modify future posting behavior in pursuit of higher counts. For the user who views content, visible engagement counts provide a social comparison signal: This post received many likes, that one received few. Research on social comparison, tracing back to Festinger's (1954) foundational theory, establishes that people have a persistent tendency to evaluate themselves by comparing their outcomes to others.<sup>27</sup> Visible engagement counts make such comparisons easy, constant, and numerically precise. The combination of social reward feedback and social comparison helps explain why visible like counts in particular are associated with repeated checking and engagement behavior. The user is not just consuming content; the user is receiving ongoing, quantified feedback about their own social standing and about the relative standing of the content they encounter.

35. As with gamification, direct connection to the Act's enumerated harm of compulsive usage is well supported in the literature. The available literature described above supports the proposition that visible social-reward metrics, especially likes, can reinforce checking behavior and repeated engagement.

## **NOTIFICATIONS AND PUSH ALERTS**

36. The authoritative patent source for notifications and push alerts, currently assigned to Meta Platforms is US8751636B2, granted June 10, 2014.<sup>28</sup> This patent describes a system that

---

<sup>27</sup> Festinger, L. (1954). A theory of social comparison processes. *Human relations*, 7(2), 117-140.

<sup>28</sup> U.S. Patent No. 8,751,636 B2, *Timing for Providing Relevant Notifications for a User Based on User Interaction with Notifications* (Tseng & Braginsky, assigned to Facebook, Inc., granted June 10, 2014), <https://patents.google.com/patent/US8751636B2/en>.

tracks how individual users respond to notifications and then adjusts the frequency, type, and timing of future notifications so that they arrive when the user is most likely to engage with them. The patent gives concrete examples: lower default push rates during working hours and higher push rates during evening hours, along with learned patterns based on when individual users have historically responded. In practical terms, this patent describes a prompt system that is initiated by the service rather than the user, can interrupt the user's current activity, and can be tuned over time based on each user's response patterns to maximize the likelihood that the user will come back to the service. Notifications do not create new content, but instead primarily vary when content is delivered to the user, for the purpose of prompting particular user behavior. Alternative designs exist and are already in use. The most straightforward alternatives include batching notifications into scheduled delivery windows (as tested by Fitz et al., with positive well-being results) or other user-defined delivery schedules.<sup>29</sup>

37. The academic literature describes that notifications can function as re-entry prompts that increase engagement. Morrison et al. (2017), in an exploratory trial published in *PLOS ONE*, found that users in more frequent notification conditions viewed and acted on more notifications, and concluded that frequent notifications may encourage greater exposure to app content without deterring engagement.<sup>30</sup>

38. Notifications work through a different but related mechanism to infinite scroll and autoplay. Where those mechanisms remove stopping cues for an activity, notifications and push alerts work by providing starting cues and re-entry prompts. They interrupt whatever the user is

---

<sup>29</sup> Fitz, N., Kushlev, K., Jagannathan, R., Lewis, T., Paliwal, D., & Ariely, D. (2019). Batching smartphone notifications can improve well-being. *Computers in Human Behavior*, 101, 84–94. <https://doi.org/10.1016/j.chb.2019.07.016>.

<sup>30</sup> Morrison, L. G., Hargood, C., Pejovic, V., Geraghty, A. W. A., Lloyd, S., Goodman, N., Michaelides, D. T., Weston, A., Musolesi, M., Weal, M. J., & Yardley, L. (2017). The Effect of Timing and Frequency of Push Notifications on Usage of a Smartphone-Based Stress Management Intervention: An Exploratory Trial. *PLOS ONE*, 12(1), e0169162. <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0169162>.

currently doing, redirect attention, and create a fresh occasion for checking the service. The habit and cueing literature described in connection with earlier design features applies here, but from the opposite direction. Wood and Neal (2007) and Bouton (2021) describe how repeated behaviors become associated with contextual cues such that encountering the cue can trigger the behavior without much conscious deliberation.<sup>3132</sup> A push notification can serve exactly this function: It becomes a learned cue that prompts the user to pick up the device and re-enter the service. Over time, the association between the notification cue and the checking behavior can become habitual, meaning that the user responds to the prompt more or less automatically.

39. Notifications and push alerts are most directly connected to the Act's enumerated harm of compulsive usage. The connection runs through the mechanism described above: Notifications serve as service-initiated, behaviorally optimized re-entry cues that can prompt repeated, compulsive return to the service.

## IN-GAME PURCHASES

40. The primary patent source for this feature is US10226691B1, "Automation of in-game purchases" (granted March 12, 2019).<sup>33</sup> This patent describes a virtual shop embedded inside an online game where users can obtain virtual items through purchase rather than by earning them through gameplay. The system receives purchase instructions from the user, applies price criteria, debits the user's currency (which can be real money or virtual currency), and delivers the purchased virtual item. The items are usable within the game itself, meaning the purchase system is tied directly to gameplay rather than to generalized e-commerce. A

---

<sup>31</sup> Wood, W., & Neal, D. T. (2007). A new look at habits and the habit-goal interface. *Psychological review*, 114(4), 843.

<sup>32</sup> Bouton, M. E. (2021). Context, attention, and the switch between habit and goal-direction in behavior. *Learning & Behavior*, 49, 349–362. <https://pubmed.ncbi.nlm.nih.gov/34713424/>.

<sup>33</sup> U.S. Patent No. 10,226,691 B1, *Automation of In-Game Purchases* (DeLaet & Oshima, originally assigned to Kabam, Inc., later reassigned to Electronic Arts Inc., granted Mar. 12, 2019), <https://patents.google.com/patent/US10226691B1/en>.

supplemental source is US20150005054A1, “System and method for facilitating gifting of virtual items between users in a game” (filed June 30, 2014; abandoned).<sup>34</sup> Although this application was not granted, it is a useful descriptive source for the Act’s specific clause covering purchased items that can be shared with another user. It describes users being awarded or purchasing virtual items during gameplay and then having the option to keep the item or share at least part of it with one or more other users. Taken together, these sources describe a monetization system embedded in the play experience in which users buy digital items or tokens using virtual currency or real money, and in which purchased items can be transferred or gifted to other users. This feature does not present expressive content, but instead regulates a payment and transaction architecture: What currency is used, how the purchase is structured, and whether the item can be shared. Alternative designs exist and are well understood. Most trivially, they simply require transactions outside of the gameplay loop and can also include transparent real-money pricing instead of multistep virtual currency exchanges, and deterministic purchases of known items instead of randomized loot boxes.

41. The research literature on in-game purchases has primarily focused on specific purchase mechanisms, which I will describe in detail below. However more general research identifying player motivation and spending has also been conducted. On ordinary purchase motivations, Hamari et al. (2017), in a survey of 519 players, identified several different motivational dimensions for buying in-game content, and found that unobstructed play, social interaction, and economical rationale were associated with increased spending.<sup>35</sup> That finding is

---

<sup>34</sup> U.S. Patent No. 20,150,005,054 A1, *System and method for facilitating gifting of virtual items between users in a game* (Smalley et al., originally assigned to Kabam, Inc., later reassigned to Electronic Arts Inc., Filed July 1, 2013, abandoned) <https://patents.google.com/patent/US20150005054A1/en>

<sup>35</sup> Hamari, J., Alha, K., Järvelä, S., Kivikangas, J. M., Koivisto, J., & Paavilainen, J. (2017). Why do players buy in-game content? An empirical study on concrete purchase motivations. *Computers in Human Behavior*, 68, 538-546.

helpful for understanding the mechanics by which in-game purchases increase spending because it shows that design choices like artificial limitations on gameplay and social features can drive in-game purchase behavior.

42. On the most well-studied purchase mechanisms of in-game purchasing, loot boxes and chance-based purchases specifically, the evidence of harm is strong particularly for minors. Montiel et al. (2022), in a scoping review of loot-box research, concluded that engagement with loot boxes is frequently associated with problematic gaming and gambling indicators.<sup>36</sup> Raneri et al. (2022) found that microtransaction engagement is associated with gaming and gambling disorder measures, while emphasizing that loot boxes appear to pose greater risk than other types of microtransactions.<sup>37</sup> Hing et al. (2022) found that adolescent loot-box purchasing remained associated with at-risk and problem gambling even after controlling for monetary gambling participation.<sup>38</sup>

43. In-game purchases increase user spending through three related behavioral mechanisms. First, they reduce spending friction and induce the user to make purchasing decisions when they are in the middle of a play session. Second, they obscure the real cost of a purchase through virtual currency intermediation. And third, for loot boxes and chance-based purchases specifically, they employ variable-ratio reinforcement. When a game uses virtual currency, the user first converts real money into a platform-specific token (such as gems, coins,

---

<sup>36</sup> Montiel, I., Basterra-González, A., Machimbarrena, J. M., Ortega-Barón, J., & González-Cabrera, J. (2022). Loot box engagement: A scoping review of primary studies on prevalence and association with problematic gaming and gambling. *PloS one*, 17(1), e0263177. <https://doi.org/10.1371/journal.pone.0263177>

<sup>37</sup> Raneri, P. C., Montag, C., Rozgonjuk, D., Satel, J., & Pontes, H. M. (2022). The role of microtransactions in Internet Gaming Disorder and Gambling Disorder: A preregistered systematic review. *Addictive behaviors reports*, 15, 100415. <https://doi.org/10.1016/j.abrep.2022.100415>

<sup>38</sup> Hing, N., Rockloff, M., Russell, A. M. T., Browne, M., Newall, P., Greer, N., King, D. L., & Thorne, H. (2022). Loot box purchasing is linked to problem gambling in adolescents when controlling for monetary gambling participation. *Journal of behavioral addictions*, 11(2), 396–405. <https://doi.org/10.1556/2006.2022.00015>

or V-bucks) and then spends those tokens inside the game. This two-step process can make the actual cost of each purchase feel less real to users because they are spending tokens rather than dollars. The CFPB has identified this structure as a consumer protection concern, noting that the conversion step, combined with currency bundles that do not align neatly with item prices (leaving leftover balances), can reduce price transparency and make it easier for users, especially minors, to spend more than they intend.<sup>39</sup> Additionally, the core mechanism of loot boxes, variable-ratio reinforcement, is one of the most extensively studied principles in behavioral psychology. With loot boxes, the user may receive a rare and valuable item, or they may receive something common and unwanted. That uncertainty can encourage repeated purchasing in pursuit of the desired outcome, following the same behavioral principle that underlies slot machines and other variable-ratio reward schedules. Ferster and Skinner (1957) established that variable-ratio schedules produce the highest and most persistent response rates of any reinforcement schedule, meaning the behavior continues even during extended periods without reward.<sup>40</sup> This is the same reinforcement principle that underlies slot machines and other forms of gambling.

44. In-game purchases are most directly connected to the Act's enumerated harm of material financial injury.<sup>41</sup> As described above, there is strong support in the literature for users, including adolescents, spending more, and more than they intend, in settings with in-game purchasing mechanics. The connection is strongest where virtual currency obscures real cost, where exchange rates are confusing, where stored payment methods reduce friction, or where chance-based mechanics encourage repeated spending. Also as described above, a second

---

<sup>39</sup> CFPB, *Consumer Advisory: Video Games Are Targeting Your Children to Get into Your Wallet* (Aug. 2024), <https://www.consumerfinance.gov/about-us/newsroom/consumer-advisory-video-games-are-targeting-your-children-to-get-into-your-wallet/>.

<sup>40</sup> Ferster, C. B., & Skinner, B. F. (1957). Schedules of reinforcement.

<sup>41</sup> S.C. Code Ann. 39-80-20(A)(7)

connection exists to compulsive usage in adolescents, when in-game purchasing involves repeated or randomized purchasing systems such as loot boxes as described in Hing et al. (2022).<sup>42</sup>

#### **APPEARANCE-ALTERING FILTERS**

45. The primary patent sources for this feature are US10152778B2, “Real-time face beautification features for video images” (filed September 11, 2015) and US11328496B2, “Scalable real-time face beautification of video images” (granted May 10, 2022), both of which are currently assigned to Intel.<sup>43,44</sup> Together, these patents describe a system that detects a user’s face in a video feed, identifies a set of facial landmark points (including points around the eyes, lips, and other features), and then uses those landmarks to perform “beautification operations.” These operations include skin smoothing, face brightening, face whitening, red lips, big eyes, slim face, wrinkle removal, eye-bag removal, and dark-eye-circle removal. In plain terms, the system detects the user’s face, maps its features, and then digitally alters its appearance. This is not the same as placing a sticker, or pair of cartoon ears on top of a photo. Novelty overlays add a separate graphic on top of the image, whereas appearance-altering filters change the underlying depiction of the person’s own face using face detection, landmarking, and warping. That distinction means that the provision should be read to cover algorithmic appearance modification specifically, not every augmented-reality or camera effect.

---

<sup>42</sup> Hing, N., Rockloff, M., Russell, A. M. T., Browne, M., Newall, P., Greer, N., King, D. L., & Thorne, H. (2022). Loot box purchasing is linked to problem gambling in adolescents when controlling for monetary gambling participation. *Journal of behavioral addictions*, 11(2), 396–405. DOI: 10.1556/2006.2022.00015

<sup>43</sup> U.S. Patent No. 10,152,778 B2 *Real-time face beautification features for video images* (Chen et al., assigned to Intel Corp., granted Dec. 11, 2018), <https://patents.google.com/patent/US10152778B2/en>

<sup>44</sup> U.S. Patent No. 11,328,496 B2 *Scalable real-time face beautification of video images* (Chen et al., originally assigned to Intel Corp., later assigned to Tahoe Research Ltd., granted May 10, 2022) <https://patents.google.com/patent/US11328496B2/en>

46. This feature presents new, expressive content. Unlike infinite scroll, autoplay, notifications, or gamification, which operate on how content is delivered or how participation is incentivized, appearance-altering filters change the visual content of the user's own image or video.

47. Alternative designs are possible. The most straightforward alternative is to offer novelty overlays (hats, ears, stickers, backgrounds, artistic effects) without offering appearance-altering filters that algorithmically reshape the user's facial or body features. A platform can provide a full creative camera experience without including filters that smooth skin, enlarge eyes, slim faces, or whiten complexions. Some platforms already distinguish between these categories in their filter libraries.

48. The research literature on appearance-altering filters is extremely well developed in the cross-sectional and experimental literature, and it focuses primarily on body image, self-perception, and appearance-related distress. Ozimek et al. (2023), in a study published in *BMC Psychology*, found that photo-editing behavior on social media was negatively related to self-perceived attractiveness and self-esteem.<sup>45</sup> The relationship was mediated through self-objectification and physical appearance comparisons, meaning that the pathway ran from editing one's own photos, through increased self-objectification and comparison with others, to lower self-perceived attractiveness. A 2025 experiment published in *Computers in Human Behavior* specifically tested slimming beauty filters and found that using a slimming filter increased desire to lose weight, self-objectification, and anti-fat attitudes.<sup>46</sup> Body dysmorphia and social self-

---

<sup>45</sup> Ozimek, P., Lainas, S., Bierhoff, H. W., & Rohmann, E. (2023). How photo editing in social media shapes self-perceived attractiveness and self-esteem via self-objectification and physical appearance comparisons. *BMC psychology*, *11*(1), 99.

<sup>46</sup> Schroeder, M., & Behm-Morawitz, E. (2025). Digitally curated beauty: The impact of slimming beauty filters on body image, weight loss desire, self-objectification, and anti-fat attitudes. *Computers in Human Behavior*, *165*, 108519.

comparison were important mediators of these effects. Fioravanti et al. (2022), in a systematic review of 43 experimental studies published in *Adolescent Research Review*, concluded that exposure to idealized beauty content on social networking sites generally has a negative effect on body image.<sup>47</sup> The review identifies appearance comparison as a central explanatory pathway.

49. Appearance-altering filters work through a fundamentally different mechanism than the other covered design features. The mechanism here is the invitation to compare one's actual appearance to a digitally altered and idealized version of oneself. When a user applies a beautification filter, they see their own face with smoother skin, larger eyes, a slimmer jaw, or other modifications that conform to prevailing beauty ideals. The user then has the experience of seeing what they "could" look like, and of comparing that altered version to their unfiltered appearance. The psychological literature on self-objectification, tracing back to Fredrickson and Roberts (1997), describes how habitual monitoring and evaluation of one's own body from an external perspective can contribute to shame, anxiety, and reduced well-being.<sup>48</sup> Appearance-altering filters operationalize this process by providing a concrete, digitally generated comparison point: the filtered self versus the unfiltered self.

50. The appearance comparison pathway is also relevant. When users see filtered images of others (or post filtered images of themselves), they are comparing against a standard that is not naturally achievable. This is consistent with the broader social comparison literature and with Fioravanti et al.'s finding that appearance comparison is a central pathway between idealized social media content and negative body image outcomes.

---

<sup>47</sup> Fioravanti, G., Bocci Benucci, S., Ceragioli, G., & Casale, S. (2022). How the exposure to beauty ideals on social networking sites influences body image: A systematic review of experimental studies. *Adolescent research review*, 7(3), 419-458.

<sup>48</sup> Fredrickson, B. L., & Roberts, T. A. (1997). Objectification theory: Toward understanding women's lived experiences and mental health risks. *Psychology of women quarterly*, 21(2), 173-206.

51. Appearance-altering filters are most directly connected to the Act’s enumerated harms of severe psychological harm and severe emotional distress.<sup>49</sup> The connection runs through self-objectification, appearance comparison, and the internalization of beauty ideals that the filters themselves generate and reinforce. For appearance-altering filters, as described above there is plentiful evidence that they contribute to appearance-related anxiety, lower self-esteem, and body dissatisfaction, particularly among adolescents.

#### **“REASONABLE CARE” AND SOFTWARE ENGINEERING PROFESSIONAL ETHICS**

52. The Act requires covered online services to exercise “reasonable care” in the use of a minor’s personal data and in the design and operation of the service, including covered design features, to prevent enumerated harms to minors. NetChoice characterizes this standard as vague and unprecedented. But exercising reasonable care with respect to user data and platform design is not a novel or unusual obligation. It is the expected ethical norm for professional software engineers and computing professionals, as articulated by the field’s own professional organizations.

53. The Association for Computing Machinery Code of Ethics and Professional Conduct, last updated in 2018, is the primary ethical code for computing professionals worldwide.<sup>50</sup> The Association for Computing Machinery (or “ACM”) is the world’s largest computing professional society. The Code’s preamble states that it is formulated on the understanding that the public good is always the primary consideration. Principle 1.1 provides that computing professionals should contribute to society and to human well-being and that an essential aim is to minimize negative consequences of computing, including threats to health, safety,

---

<sup>49</sup> S.C. Code Ann. §§ 39-80-20(A)(2), -20(A)(3)

<sup>50</sup> ACM, *ACM Code of Ethics and Professional Conduct* (2018), <https://www.acm.org/code-of-ethics>.

personal security, and privacy. Principle 1.2 provides that computing professionals should avoid harm, and states that avoiding harm begins with careful consideration of potential impacts on all those affected by decisions. The Code further provides that when harm is unintended, those responsible are obliged to undo or mitigate the harm as much as possible, and that to minimize the possibility of indirectly or unintentionally harming others, computing professionals should follow generally accepted best practices. Principle 1.6 requires computing professionals to respect privacy, and the Code specifically notes that the consequences of data aggregation and emergent properties of systems should be carefully analyzed.

54. The joint ACM/IEEE-CS (the Institute of Electrical and Electronics Engineers Computer Society) Software Engineering Code of Ethics and Professional Practice, adopted by both ACM and the IEEE Computer Society, is similarly direct.<sup>51</sup> Its preamble states that in all professional judgments, concern for the health, safety, and welfare of the public is primary. Its first principle provides that software engineers shall act consistently with the public interest. Its third principle provides that software engineers shall ensure that their products and related modifications meet the highest professional standards possible.

55. The IEEE's own Code of Ethics, applicable to all IEEE members, states as its first commitment that members agree to hold paramount the safety, health, and welfare of the public; to strive to comply with ethical design and sustainable development practices; and to protect the privacy of others.<sup>52</sup>

56. These are not aspirational statements from a fringe movement. ACM and IEEE are the two largest professional organizations for computing and engineering worldwide. Their ethical codes represent the profession's own articulation of what responsible practice requires. The

---

<sup>51</sup> ACM, *ACM Code of Ethics and Professional Conduct* princ. 1.2 (2018), <https://www.acm.org/code-of-ethics>.

<sup>52</sup> IEEE, *IEEE Code of Ethics* (2020), <https://www.ieee.org/about/corporate/governance/p7-8>.

obligation they describe, to consider the potential impacts of one's design decisions on users, to minimize harm, to respect privacy, and to prioritize the public good, is precisely the kind of obligation the Act's "reasonable care" standard codifies. A reasonable computing professional, acting in accordance with the ethical norms of the profession, would already be expected to consider how design features affect users, including vulnerable users such as minors, and to take steps to mitigate foreseeable harms.

57. In that sense, the Act's "reasonable care" standard does not impose an alien obligation on the technology industry. It asks covered services to do what the profession's own ethical codes already say professionals should be doing.

I declare under penalty of perjury pursuant to 28 U.S.C. §1746, that the foregoing is true and correct to the best of my knowledge.



---

Laura Edelson, Ph.D.

April 6, 2026

**Laura Edelson, Ph.D.**

(203) 803-6953

[laura.edelson@gmail.com](mailto:laura.edelson@gmail.com)**SUMMARY**

I am a computer scientist with expertise in large online networks and extensive real-world experience building big data machine learning augmented systems. My current research involves large-scale analysis of ads and harmful content on major platforms such as Instagram, TikTok, and X, and auditing of algorithms, user-facing safety systems, and AI systems. I co-lead [Cybersecurity for Democracy](#), a multi-university research lab, am a co-PI for the [Institute for Information, the Internet, and Democracy](#) at Northeastern University, and am an Assistant Professor of Computer Science at Northeastern University. I am the former Chief Technologist of the Antitrust Division (2022-2023) and the Civil Rights Division (2024) of the Department of Justice.

**EDUCATION**

- Ph.D. Computer Science, New York University, 2022  
Dissertation: Characteristics of Misinformation and Political Content in Online Information Spaces  
Advisor: Damon McCoy
- B.S. Computer Science, Pace University, 2008

**REFEREED CONFERENCE & JOURNAL PUBLICATIONS**

[A Comparative Survey of Algorithmic Feed Recommendation System Designs](#), 2025. ACM Transactions on Recommender Systems. Laura Edelson, Frances Haugen, Damon McCoy.

[Characterizing the Usability and Usefulness of Ad Transparency](#), 2025. USENIX Security. Kevin Bryson, Arthur Borem, Phoebe Moe, Omer Akgul, Laura Edelson, Tobais Lauinger, Michelle L. Mazurek, Damon McCoy, Blase Ur.

[Measurement and Metrics for Content Moderation: The Multi-Dimensional Dynamics of Engagement and Content Removal on Facebook](#), 2025. Journal of Online Trust & Safety, Volume 2.5. Laura Edelson, Borys Kovba, Hanna Yershova, Austin Botelho, Damon McCoy, and Tobias Lauinger.

[AI Regulation: Competition, Arbitrage & Regulatory Capture](#), 2025. Theoretical Inquiries in Law Journal. Filippo Lancieri, Laura Edelson, Stefan Bechtold.

[Captured Innovation: Technology Monopoly Response to Transformational Development](#), 2025. The University of Chicago Business Law Review, Volume 4.1. Reed Showalter, Laura Edelson.

[Propaganda Política Pagada: Exploring U.S. Political Facebook Ads en Español](#), 2023. Proceedings of the ACM Web Conference (WWW). Bruno Coelho, Tobias Lauinger, Laura Edelson, Ian Goldstein, and Damon McCoy.

[An Audit of Facebook's Political Ad Policy Enforcement](#), 2022. USENIX Security. Victor LePochat, Laura Edelson, Tom Van Goethem, Wouter Joosen, Damon McCoy, and Tobias Lauinger.

[Understanding Engagement with US \(Mis\) information News Sources on Facebook](#), 2021. Proceedings of the 21st ACM Internet Measurement Conference (IMC). Laura Edelson, Minh-Kha Nguyen, Ian Goldstein, Oana Goga, Damon McCoy, Tobias Lauinger.

[A Security Analysis of the Facebook Advertising Library](#), 2020. IEEE Symposium on Security and Privacy (S&P). Laura Edelson, Tobias Lauinger and Damon McCoy.

## GRANTS

Through over \$3M in grants awarded to Damon McCoy which I contributed to writing, my work has been supported by the NSF, Reset.tech, Democracy Fund, Emerson Collective, NetGain, and Wellspring.

- NSF Collaborative Research: SaTC: CORE: Medium: Methods and Tools for Effective, Auditable, and Interpretable Online Ad Transparency (\$1.2M with \$383,395 NYU share)
- Belfer Fellowship (\$50,000), Anti-Defamation League, 2022
- Online Political Advertising Transparency Project (\$800,000) Democracy Fund, 2019-2022
- Cybersecurity for Democracy (\$1,400,000) Wellspring Philanthropic Fund, 2019-2022
- Cybersecurity for Democracy (\$100,000 NYU) Emerson Collective, Gift Funds 2021
- Cybersecurity for Democracy (\$100,000 NYU) NetGain, Gift Funds, 2021
- Political Transparency in German Elections (\$37,500 NYU), Reset.tech, 2021
- Digital Ecosystem Research Challenge (\$37,822 NYU) Government of Canada, 2019-2020
- Online Political Advertising Transparency Project (\$175,000 NYU) Luminare, 2019

## GOVERNMENTAL TESTIMONY

U.K. Parliament. “Joint Committee on the Online Safety Bill”. October 14th, 2021

U.S. House of Representatives Science Committee. “The Disinformation Black Box: Researching Social Media Data”. Sept. 28th, 2021

Washington State Public Disclosure Commission. “Big Data, Big Dollars: Shining a Light Digital Political Advertising”. Jan. 16th, 2020

## OTHER WRITINGS

[Teen Accounts, Broken Promises](#), Oct. 2025. With Arturo Bejar.

[We Need Product Safety Regulations for Social Media](#), Nov. 2023. Scientific American.

[It’s Time to Open the Black Box of Social Media](#), Apr. 2022. Scientific American. With Reneé DiResta, Brendan Nyhan, and Ethan Zuckerman.

[Platform Transparency Legislation: The Whos, Whats and Hows](#), Apr. 2022. Lawfare.

[How Facebook Hinders Misinformation Research](#), Sept. 2021. Scientific American. With Damon McCoy.

[We Research Misinformation on Facebook. It Just Disabled Our Accounts](#), Aug. 2021. New York Times. With Damon McCoy.

## NON-REFEREED JOURNAL AND OCCASIONAL PAPERS

[The Locknet: How China Controls Its Internet and Why It Matters](#), July 2025, China File

[Into the Driver’s Seat With Social Media Content Feeds](#), March 2025. Knight First Amendment Institute Occasional Papers Series. Laura Edelson, Frances Haugen, and Damon McCoy.

[A Standard for Universal Digital Ad Transparency](#), Dec. 2021. Knight First Amendment Institute Occasional Papers Series. Laura Edelson, Jason Chuang, Erika Franklin-Fowler, Michael Franz, and Travis Ridout.

[Political Advertisement and Personal Data](#), Jan. 2020. *In* Understanding the Digital Ecosystem: Findings from the 2019 Federal Election. Laura Edelson, Divam Jain and Damon McCoy

[An Analysis on United States Online Political Advertising Transparency](#), 2019, Laura Edelson, Shihkar Sakuja, Ratan Dey, and Damon McCoy. [56 Citations]

## PROJECTS

[Ad Observatory](#), 2020-2023, Website to increase practical transparency of Facebook political advertising.

[Ad Observer](#), 2020 - 2023, Browser extension to crowdsource observations of Facebook and YouTube political ads.

## SELECTED PRESENTATIONS & TALKS

[Computational Antitrust: The US DoJ Keynote](#), Computational Antitrust 2<sup>nd</sup> Annual Conference, 2022  
Workshop on Technology & Consumer Protection (ConPro 2022) Keynote

[Data: Sharing While Protecting?](#), 2022

[Pursuing Platform Transparency in 2022](#), 2022

[Online Political Ad Transparency](#), 2021

[A Security Analysis of Facebook's Political Ad Library](#), 2019

## AWARDS & FELLOWSHIPS

Pearl Brownstein Doctoral Research Award, New York University Tandon School of Engineering, 2022

Belfer Fellowship, Anti-Defamation League, 2022

Deborah Rosenthal, MD Award for Best Qualifying Exam, New York University Tandon School of Engineering, 2019

## SERVICE

USENIX Security, Program Committee 2023-2025

Workshop on Technology & Consumer Protection (ConPro 2023), Co-Chair 2023-2025

USENIX Security, Differential Privacy Session Chair, 2022

Workshop on Technology & Consumer Protection (ConPro 2022), Program Committee 2022

Workshop on Technology & Consumer Protection (ConPro 2021), Program Committee 2021

IEEE International Symposium on Technology and Society, Program Committee 2021

Editorial Board, Journal of Online Trust and Safety, 2021 - Present

I have volunteered with the IEEE extensively and have served in many roles. Some of my roles have included:

- Chair, Humanitarian Activities Committee, 2016-2017 - Managed a team of staff and volunteers to execute IEEE's humanitarian goals. Oversaw a \$2 million annual budget.
- President, Society on Social Implications of Technology, 2013-2014 - Led a team of volunteers managing the affairs of the society, including conferences, publications, partnership arrangements with other non-profits, and membership development.

## GOVERNMENT SERVICE

Chief Technologist, United States Department of Justice Civil Rights Division 6/24 - 12/24

Chief Technologist, United States Department of Justice Antitrust Division 8/22 - 7/23

**EMPLOYMENT**

Chief Scientist, Sigma Ratings

6/17 – 5/18

- Developed proprietary machine learning algorithm to detect financial crime risk to banking institutions Built and led technology team, including remote data collection teams to deliver Sigma's commercial offerings, including a low-cost screening platform as well as customized financial crime rating product

Software Engineer, Palantir Technologies

8/13 – 7/15

- Worked with the Data Science team to implement original bucketing algorithms for Machine Learning offering
- Integrated open source machine learning library mllib into Palantir's broader Data Warehousing offerings allowing it to be used on massive scale data sets.
- Developed a new API for Palantir's deployment toolset that was adopted company-wide.

Senior Software Engineer, FactSet Research Systems, Inc.

9/08 – 7/13

- Technical Lead for Quote Alerts, a real-time notification server of market threshold events. Developed proprietary algorithms for high-speed function evaluation.
- Developed a novel algorithm to project future dividend amounts and calculate the Fair Value of futures contracts for stock indexes, allowing FactSet to be the first to market with a streaming Fair Value product.
- Developed custom data compression scheme for transmission of market data, maintaining a high degree of compression (>80%) while being flexible enough to not require pre-defined message formats.

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF SOUTH CAROLINA  
COLUMBIA DIVISION**

NETCHOICE, LLC,

*Plaintiff,*

v.

ALAN WILSON, in his official capacity as  
South Carolina Attorney General,

*Defendant,*

and

HENRY DARGAN McMASTER, in his  
official capacity as Governor of the  
State of South Carolina,

*Intervenor-Defendant.*

Civil Action No.: 3:26-cv-543-sal

**DECLARATION OF  
DAMON McCOY, PH.D.**

I, Professor Damon McCoy, Ph.D., declare and state as follows:

1. I submit this declaration in support of Defendants’ Opposition to Plaintiff’s Motion for Preliminary Injunction.

**BACKGROUND & QUALIFICATIONS**

2. I am a tenured full professor in the Department of Computer Science and Engineering at New York University’s Tandon School of Engineering. I am also the Co-Director of the NYU Center for Cybersecurity, which is the hub for interdisciplinary cybersecurity and privacy research and education. My research has been cited more than 18,000 times, and my h-index, the most common metric for scientific impact, is 110. I have published over 100 peer-reviewed research papers, and my research has received many awards, including four

test-of-time awards, which honor academic papers published more than ten years ago that have maintained a significant, long-lasting impact on their field.

3. I have been conducting research into social media privacy and security for over 15 years and kids' online safety for over ten years. My research focuses on understanding how well security, privacy, and safety features are deployed by large social media companies, such as Google, LinkedIn, Meta, and X (formerly Twitter), actually protect users and how these companies' product design decisions affect the risk of harm to their users. My studies have also audited whether claims about product privacy and safety made by these large social media companies are accurate. During my work, I have consulted for Google and LinkedIn and collaborated with Google and Twitter on research studies focused on analyzing and improving their integrity systems. I have been invited to give research presentations to Google, LinkedIn, and Meta.

4. My curriculum vitae, which sets forth my experience and credentials in greater detail, is attached as Exhibit A.

5. I have testified as an expert in the following matters:

a. For the federal government in *United States v. Gatrel*, No. 2:19-cr-36 (C.D. Cal).

b. For the Federal Trade Commission in *FTC v. Facebook, Inc.*, No. 20-3590 (D.D.C.).

c. For New Mexico in *New Mexico v. Meta Platforms, Inc.*, No. D-101-CV-2023-02838 (N.M. 1st Jud. Dist. Ct.).

6. I am being compensated in the above-entitled case at an hourly rate of \$400/hour for preparing this declaration. My compensation is not in any way dependent on the outcome of this or any related proceeding.

7. The opinions in this declaration are my expert opinions, which are based on my education and training, my peer-reviewed published research and the research of others, my knowledge of relevant technologies (including my reading of the public technical documents offered by NetChoice's members about their capabilities), as well as my reading of the legislation.

### **SUMMARY OF OPINIONS**

8. I have reviewed H. 3431, the South Carolina Social Media Regulation Act ("Act"). This law is necessary to address the realities of modern social media applications, which have often been recklessly designed with little thought to the risks to minors' safety.

9. NetChoice members have made reckless design choices to engage in privacy-invasive profiling of minors. These choices have harmed minors in various ways, including by recommending that adults whom the company suspected of being child predators connect with minors.

10. Complying with the Act to avoid this privacy-invasive profiling is both possible and straightforward. The provisions are reasonable and technically feasible to adopt (i.e., the technologies necessary to comply are already in widespread use by NetChoice's members). Compliance with the Act isn't some Herculean engineering feat; it's a straightforward matter of limiting invasive, dangerous tracking vectors and finally incorporating basic safety and privacy heuristics into the design of the covered online services. The industry's reflexive outcry that taking into account minor safety is a "war on innovation" rings hollow when you consider we've

already normalized guardrails for online gambling, treating the exclusion of minors not as some digital autocracy, but as a baseline, common-sense safety requirement for an inherently high-risk environment. I believe there are real risks that would be addressed by the Act and that it takes a reasonable approach to children's online safety. Requiring online services to consider the harm they might have on their users seems reasonable and something that we already do for other products. The technologies needed to comply with the Act already exist and are already in widespread use.

### **GEOLOCATION IS NOT NECESSARY**

11. The NetChoice members' insistence that behavioral profiling is a necessary means of monetizing their services is, frankly, a failure of imagination, if not an outright redirection. We need to stop conflating "relevant advertising" with "surveillance capitalism." Contextual advertising proves that you can deliver value without building high-fidelity dossiers on every user; it's the difference between showing a sneaker ad because someone is currently reading a marathon blog versus showing it because you've tracked their GPS coordinates to a podiatrist's office. By mapping ads to the immediate environmental context (that is, the specific page or service being accessed), platforms can drive engagement based on real-time intent rather than historical exploitation. Under the Act, shifting to contextual models isn't just a privacy win; it's a technically trivial pivot that decouples revenue from the systematic harvesting of personal data.

### **USERS DO NOT SUFFICIENTLY UNDERSTAND THE PRIVACY ISSUES**

12. The argument that continued use of services implies a conscious endorsement of privacy-invasive profiling is a classic misreading of user agency in an information vacuum. The reality, backed by empirical research from Tsai, Egelman, Cranor, and other well-respected

academic researchers,<sup>1</sup> is that users can't optimize for privacy if the interface hides the trade-offs. When researchers presented subjects with search results annotated with clear privacy ratings, users, even those previously making choices based solely on price, were willing to pay a literal premium to protect their data. This demonstrates that “consent” in the current “notice and disclosure” regime is a convenient fiction. Without accessible, real-time telemetry on how their data is being harvested, users aren't making a choice. Instead, they're being funneled through a system designed to exploit their lack of visibility. The Act recognizes that the gap between a user's stated privacy preferences and their actual behavior isn't a sign of hypocrisy, but a direct consequence of a design architecture that often obscures the cost of engagement.

13. Some NetChoice members also employ the argument that their privacy policies and other transparency tools inform users about data collection and provide them with controls to manage data collection and usage. Even if we indulge the fantasy that users actually read these policies, the documents themselves are masterpieces of strategic ambiguity that make informed decision-making a literal impossibility. Under current frameworks like the California Consumer Privacy Act (CCPA),<sup>2</sup> platforms are only required to disclose broad “categories” of third-party data recipients, effectively masking a vast, invisible web of trackers whose specific identities—and subsequent data-handling practices—remain a black box to the consumer. This opacity is further compounded by the trend of “aggregated” policies from NetChoice members,

---

<sup>1</sup> Janice Y. Tsai Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. “The effect of online privacy information on purchasing behavior: An experimental study.” *Information systems research* 22, no. 2 (2011): 254-268.

Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. “Timing is everything? The effects of timing and placement of online privacy indicators.” In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 319-328. 2009.

Julia Gideon, Lorrie Cranor, Serge Egelman, and Alessandro Acquisti. “Power strips, prophylactics, and privacy, oh my!.” In *Proceedings of the Second Symposium on Usable privacy 28 and security*, pp. 133-144. 2006.

<sup>2</sup> <https://oag.ca.gov/privacy/ccpa>

such as Google, where the data practices for a map application are lumped in with an email service or a search engine,<sup>3</sup> offering a high-level overview that tells you everything and nothing at once. The Act targets this exact lack of granularity, recognizing that a “notice and consent” model is functionally worthless when, as my co-authored research<sup>4</sup> and that of other researchers<sup>5</sup> has found, the “notice” and transparency tools are often designed in ways that obscure the specific usages and downstream third-party destinations of a user’s most sensitive information.

### **MINORS ARE AT EVEN GREATER RISK**

14. This data monetization free-for-all is even more concerning when the data comes from minors who are unlikely to understand that this is happening, much less consent to it, but who could potentially face enormous impacts due to future usage and sharing of this data. An example of this negative impact on minors due to how features are designed and invasive profiling of minors is Meta’s (a NetChoice member) Instagram service, which includes a feature, “People You May Know,” that suggests new accounts to follow by analyzing shared data points such as mutual friends, synced phone contacts, and behavioral profiling data. As I have previously testified to in *FTC v. Meta Platforms*, Meta’s internal research found that overall, the People You May Know feature suggested “7% of all follow recommendations to adults were

---

<sup>3</sup> <https://policies.google.com/privacy?hl=en-US>

<sup>4</sup>Characterizing the usability and usefulness of US ad transparency systems, K Bryson, A Borem, P Moh, O Akgul, L Edelson, T Lauinger, ML Mazurek, D McCoy, B Ur, IEEE Symposium on Security and Privacy (SP), 2025, <https://ieeexplore.ieee.org/abstract/document/11023459>.

<sup>5</sup>Aleecia M. McDonald and Lorrie Faith Cranor. “The cost of reading privacy policies.” *Journal of Law and Policy for the Information Society*, 4 (2008): 543.

Yuanxiang Li et al. “Online privacy policy of the thirty Dow Jones corporations: Compliance with FTC Fair Information Practice Principles and readability assessment.” *Communications of the IIMA* 12.3 (2012): 5.

Carlos Jensen and Colin Potts. “Privacy policies as decision-making tools: an evaluation of online privacy notices.” *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2004.

George R. Milne, Mary J. Culnan, and Henry Greene. “A longitudinal assessment of online privacy notice readability.” *Journal of Public Policy & Marketing* 25.2 (2006): 238-249.

minors.”<sup>6</sup> Unfortunately, users that Meta flagged as likely “groomers” (i.e., child predators) but had not been suspended were suggested by the People You May Know feature to follow minors at an elevated rate: “27% of all follow recommendations to groomers were minors.”<sup>7</sup> Meta’s 2019 internal research found that, “We [Instagram] are recommending nearly 4X as many minors to groomers (nearly 2 million minors in the last 3 months). 22% of those recommendations resulted in a follow request.”<sup>8</sup> This demonstrates the risks of profiling minors and using that data in ways that are not required by the feature. A friend suggestion feature can function fine without requiring sensitive profiling data.

### **COMPANIES MISREPRESENT THEIR DATA COLLECTION PRACTICES**

15. Another example of privacy and profiling risks is companies’ inaccurate representations of the privacy of the data they collect. My co-authored study found that Google and Meta (both NetChoice members) publicly claimed that hashing<sup>9</sup> personally identifiable data, such as phone numbers and addresses, is sufficient for privacy.<sup>10</sup> The claim that hashing protects privacy has been debunked by researchers and the Federal Trade Commission in the past 12 years.<sup>11</sup> Re-identification of a specific person from a hashed email address is trivial when a

---

<sup>6</sup> [https://www.ftc.gov/system/files/ftc\\_gov/pdf/McCoy.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/McCoy.pdf), page 39

<sup>7</sup> Id.

<sup>8</sup> Id.

<sup>9</sup> Hashing is a mathematical process that transforms text such as an email address (e.g., user@example.com) into a consistent, fixed-length string of characters (the “hash”).

<sup>10</sup> Julia B Kieserman, Athanasios Andreou, Chris Geeng, Tobias Lauinger, Damon McCoy, Tracker Installations Are Not Created Equal: Understanding Tracker Configuration of Form Data Collection, Proceedings on Privacy Enhancing Technologies, 2025, <https://crysp.petsymposium.org/popets/2025/popets-2025-0151.pdf>.

<sup>11</sup> Levent Demir, Amrit Kumar, Mathieu Cunche, and Cédric Lauradoux. 2017. The pitfalls of hashing for privacy. IEEE Communications Surveys & Tutorials 20, 1 (2017), 551–565.

Ed Felten. 2012. Does Hashing Make Data “Anonymous”? <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashingmake-data-anonymous>.

company, such as Google or Meta, already knows your email address (because you have an account). Thus, if a third-party website shares a hashed list of visitors' email addresses with them, Google and Meta can simply hash their own database and find the matches. This allows them to know exactly which specific user visited which external website. My study also found that health websites were likely unwittingly duped into sharing potentially sensitive data with Google and Meta due to incorrect privacy claims in their tracking product documentation.<sup>12</sup> This again highlights the risk to users, especially minors, of these social media services' invasive tracking and profiling practices. The service can be designed and operated without invasive tracking or the collection of sensitive personal information.

16. The final example is from my co-authored study, where we found that Meta and TikTok (both NetChoice Members) share sensitive information about specific users with advertisers.<sup>13</sup> TikTok, Facebook, and Instagram allow third parties to run targeted advertising campaigns on sensitive attributes. These ads are interactive by default, meaning users can comment or "react" (e.g., "like" or "love") to them. We found that this design choice creates a privacy loophole such that advertisers can view the profiles of those who interact with their ads, thus learning potentially sensitive information about individuals who fulfill certain targeting criteria. A hypothetical example of the harms that could occur from this dangerous design choice would be a child predator who wants to identify minors on Facebook, Instagram, or TikTok. The predator could purchase ads targeted towards 13–17-year-olds and compile a list of minors who

---

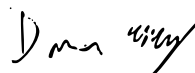
FTC. 2024. No, hashing still doesn't make your data anonymous. <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/nohashing-still-doesnt-make-y-our-data-anonymous>.

<sup>12</sup> Julia B Kieserman, Athanasios Andreou, Chris Geeng, Tobias Lauinger, Damon McCoy, Tracker Installations Are Not Created Equal: Understanding Tracker Configuration of Form Data Collection, Proceedings on Privacy Enhancing Technologies, 2025, <https://crysp.petsymposium.org/popets/2025/popets-2025-0151.pdf>.

<sup>13</sup> <https://arxiv.org/pdf/2603.03659>

commented on the ad. This behavior contradicts the promises made by Meta and TikTok to not share user data with advertisers. In addition, YouTube (another NetChoice member) designed ads in a way that this privacy loophole does not exist. This shows that it is unnecessary to design an ad system in a way that enables this dangerous sharing of potentially sensitive user information with advertisers.

I declare under penalty of perjury pursuant to 28 U.S.C. § 1746, that the foregoing is true and correct to the best of my knowledge.



---

Damon McCoy, Ph.D.

April 6, 2026

# Damon Liwanu McCoy

New York University  
 Department of Computer Science and Engineering  
 ☎ +1 720-810-3076  
 ✉ [mccoy@nyu.edu](mailto:mccoy@nyu.edu)  
<https://www.damonmccoy.com/>

## Academic Appointments

- 2024 - Present Co-Director Center for Cybersecurity, New York University
- 2023 - Present Professor, Department of Computer Science and Engineering, New York University
- 2019 - 2023 Associate Professor, Department of Computer Science and Engineering, New York University
- 2015 - 2019 Assistant Professor, Department of Computer Science and Engineering, New York University
- 2014 - 2018 Affiliated Research Staff, International Computer Science Institute
- 2014 - 2015 Visiting Research Scientist, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley
- 2012 - 2015 Assistant Professor, Department of Computer Science, George Mason University
- 2009 - 2011 Post-Doc, University of California, San Diego

## Education

- December 2009 **Ph.D., Computer Science**, *University of Colorado*, Boulder
- Co-Advisors Dirk Grunwald and Douglas Sicker
- Thesis Quantifying and Improving Wireless Privacy
- December 2007 **M.S., Computer Science**, *University of Colorado*, Boulder
- Advisor Douglas Sicker
- Thesis Anonymity Analysis of Freenet
- May 1999 **B.S., Computer Science**, *University of Colorado*, Boulder

## Funding (my total share \$9 M)

- Emerson (Sole PI) Cybersecurity for Democracy (\$200,000), Gift Award 2025
- WS (Sole PI) Cybersecurity for Democracy (\$350,000) Wellspring Philanthropic Fund 2025-2026
- HF (Sole PI) Cybersecurity for Democracy (\$290,493) Hopewell Fund, Gift Award, 2025
- DF (Sole PI) Cybersecurity of Democracy (\$250,000) Democracy Fund 2025-2026
- LFF (PI) Modernizing Section 230 (\$10,000) Lubetzky Family Foundation, Gift award 2025

Emerson (Sole PI) Cybersecurity for Democracy (\$200,000), Gift Award 2024  
LFF (PI) Modernizing Section 230 (\$50,000) Lubetzky Family Foundation, Gift award 2024  
WS (Sole PI) Cybersecurity for Democracy (\$350,000) Wellspring Philanthropic Fund 2024-2025  
NSF (PI) Collaborative Research: NSF-DFG: SaTC: CORE: Small: Requirements, Metrics, and Tools for Effective User Transparency (\$400,000) 2024-2026  
NSF (Sole PI) Veterans Research Supplement (VRS) (\$100,000), 2024  
NSF (Sole PI) Career Life Balance Supplement (\$45,000), 2024  
Reset (Sole PI) Cybersecurity of Democracy, \$50,000 2023-2024  
FordFound (Sole PI) PETS Travel Funding, \$75,000 2023-2026  
DF (Sole PI) Cybersecurity of Democracy (\$450,000) Democracy Fund 2023-2025  
NSF (PI) Collaborative Research: SaTC: CORE: Medium: Understanding and Combatting Impersonation Attacks and Data Leakage in Online Advertising (\$400,000) 2023-2027  
NSF (PI) Collaborative Research: SaTC: CORE: Medium: Methods and Tools for Effective, Auditable, and Interpretable Online Ad Transparency (\$383,395) 2022-2026  
DF (Sole PI) Online Political Advertising Transparency Project (\$400,000) Democracy Fund 2020-2022  
WS (Sole PI) Cybersecurity for Democracy (\$858,000) Wellspring Philanthropic Fund 2021-2022  
Emerson (PI) Cybersecurity for Democracy (\$100,000), Gift Award 2021  
NetGain (PI) Cybersecurity for Democracy (\$100,000), Gift Award 2021  
Reset (PI) Political Transparency in German Elections (\$37,500) 2021  
NSF (PI) D-ISN: TRACK 1: Collaborative Research: An Interdisciplinary Approach to Understanding, Modeling, and Disrupting Drug and Counterfeit Illicit Supply Chains (\$375,000) 2020-2025  
Google (PI) Investigating Online Communities of Intimate Partner Abusers (\$24,500), 2020  
NSF (Co-PI) SaTC: CORE: Medium: Collaborative: Threat Intelligence for Targets of Coordinated Harassment (\$800,000 My Share \$400,000) 2020-2024  
FordFound (Sole PI) PETS Travel Funding, \$50,000 2020-2021  
NSF (PI) Student Travel Support: Privacy Enhancing Technology Symposium (\$18,000 2020-2021)  
DF (Sole PI) Online Political Advertising Transparency Project (\$300,000) Democracy Fund 2020-2021  
WS (Sole PI) Online Political Transparency Project (\$300,000) Wellspring Philanthropic Fund 2019-2021  
Canada (Sole PI) Type C: Digital Ecosystem Research Challenge, Research Award (\$37,822) Government of Canada 2019-2020  
FordFound (Sole PI) PETS Travel Funding, \$20,000 2019  
NSF (PI) Student Travel Support: Privacy Enhancing Technology Symposium (\$18,000 2019-2020)

- DF (Sole PI) Online Political Advertising Transparency Project (\$100,000) Democracy Fund 2019-2020
- Lumin (Sole PI) Online Political Advertising Transparency Project (\$175,000) Luminate 2019-2020
- NSF (PI) SaTC: CORE: Medium: Collaborative: Digital Safety and Security for Victims of Intimate Partner Violence (\$350,000) 2019-2023
- NSF (PI) CAREER: Cryptocurrency Forensics Tools (\$510,000) 2018-2022
- NSF (PI) SaTC: CORE: Small: Collaborative: Understanding and Mitigating Adversarial Manipulation of Content Curation Algorithms, (\$241,000 NYU, Co-PI Rachel Greenstadt (Drexel), \$250,000) NSF, 2018-2021
- NSF (PI) Student Travel Support: Privacy Enhancing Technology Symposium (\$18,000 2018-2019)
- FordFound (Sole PI) PETS Travel Funding, \$20,000 2018
- DHS (Sole PI) MitigatINg IoT-based DDoS attacks via DNS DHS, \$250,000 2018-2022
- Google (PI) Understanding and Mitigating the Use of Spyware in Intimate Partner Violence (\$40,000 NYU, Co-PIs Nicola Dell, Thomas Ristenpart, \$40,000)
- CATT (PI) Understanding the Ecosystem of Streaming Copyright-Infringing Media Kodi Plugins (NYU) \$30,000 2017
- Comcast (PI) Understanding the Ecosystem of Streaming Copyright-Infringing Media Kodi Plugins (NYU) \$60,000 2017
- NSF (PI) Scalable and Meaningful Threat Intelligence Generation. (NYU) \$492,064 2017
- CDS (PI) Semi-supervised NLP Techniques for Automated Cybercrime Forum Analysis (NYU) \$25,000 2017
- LinkedIn (PI) Understanding Fraudulent Accounts. (NYU) \$25,000 2016
- Google (PI) Junior Faculty Google Security Privacy and Anti-abuse Applied Reward. (NYU) \$50,000 2016
- QNRF (NYU PI) Qatar National Research Fund: Enhancing the Performance, Security, and Blocking-Resistance of Anonymous Communication Networks \$900,000 (Lead PI: Mashael Al-Sabah \$100,000 to NYU). 2016-2017
- NSF (PI) Ideas Lab: Interdisciplinary Pathways towards a Secure Internet. (GMU) \$111,816 2013-2014
- Google (PI) Understanding the Business of Traffic Distribution System Services. (GMU) \$75,000 2013
- General Motors (PI) Cyber-security Pen Test. (GMU) \$241,608 2013-2015
- DHS (Co-PI) DHS Graduate Fellowship Training for Homeland Security. (GMU) \$256,336 2012-2017
- NSF (NYU PI) TWC: Frontier: Collaborative: Beyond Technical Security: Developing an Empirical Basis for Socio-Economic Perspectives. Award 1237076 \$10,000,000 (\$668,050 my share (\$316,432 Transferred to NYU)) 2012-2017

---

## Advising

### Graduated Ph.D. Students

Ian Gray, December 2025

Empirical Measurement and Analysis of the Ransomware Ecosystem

First Position: Flashpoint

Bruno Coelho, May 2025 (NYU)

Access to Political Information in Contemporary Digital Communications

First Position: Kensho Technologies

Paz Grimberg, May 2023 (NYU)

Thesis title: Empirical Analysis of Arbitrage Strategies in Centralized Cryptocurrency Exchanges and its Applications to Decentralized Finance

First Position: Startup Founder

Maxwell Aliapoulios, May 2022 (NYU)

Thesis title: Empirically Measuring Online Adversaries to Promote Tooling for Global Safety

First Position: Facebook

Laura Edelson, May 2022 (NYU)

Thesis title: Characteristics of Misinformation and Political Content in Online Information Spaces

First Position: Research Scientist, NYU

Rasika Bhalerao, May 2022 (NYU)

Thesis title: Adversarial "Intended" Usage of Technology and the Need for New Threat Models Addressing Human Harms

First Position: Instructor, Northeastern University

Periwinkle Doerfler, May 2021 (NYU)

Thesis title: Adversarial "Intended" Usage of Technology and the Need for New Threat Models Addressing Human Harms

First Position: Facebook

Mohammad Rezaeirad. December 2019 (GMU)

Thesis title: Methods For Reducing Threat Intelligence Pollution

First Position: Blue Cross Blue Shield

Mohammad Karami. May 2016 (GMU)

Thesis title: Understanding and Undermining The Business of DDoS Booter Services

First Position: Google

Sean Palka. December 2015 (GMU)

Thesis title: Automated Test Case Generator for Phishing Prevention using Generative Grammars

First Position: Booz Allen Hamilton

Jason Clark. July 2014 (GMU)

Thesis title: Profiling, Tracking, and Monetizing: An Analysis of Internet and Online Social Network Concerns

First Position: Insider Threat Research, CMU SEI

#### Graduated M.S. Students

Cameron Ballard (Co-Advised with Rachel Greenstadt), August 2022 (NYU)

First Position: Co-founder of RadiTube

Prashanth Ramakrishna, May 2021 (NYU)

First Position: Ph.D. Student, University of Virginia

Ryan Brunt, December 2019 (NYU)

First Position: Goldman Sachs

Prakhar Pandey, May 2017 (NYU)

First Position: RSA

Hitesh Dharmdasani. May 2013 (GMU)

Thesis title: Botnets and Crypto Currency - Effects of Botnets on the Bitcoin Economy

First Position: Researcher, FireEye

#### Current Ph.D. Students

Elaine Lee, Co-Supervised since 2025

Saja Alsulami, Supervised since 2025

Mitch Haszard, Supervised since 2024

Lexie Barthelemess, Supervised since 2024

Julia Kieserman, Supervised since 2023

Cat Mai, Supervised since 2022

#### [Undergraduate Research Advising](#)

Dominick Gordon, NSF REU Summer 2025

Michelle Zhou, NSF REU Summer 2024

Natalie Chen, NSF REU Summer 2023

Benjamin Brown, NSF REU Summer 2022

Sachi Parikh, NSF REU Summer 2022, 2023

Shikhar Sakhuja, Summer 2019

Luis Ramirez. NSF REU Summer 2013

Sam Zhang. NSF REU Summer 2013

---

[Publications \(As of July 10, 2025: Google Scholar citations: 17,800, h-index: 55, i10-index: 106\)](#)

#### [Journal Articles and Magazines](#)

- JEPS'25 Laura Edelson, Dominique Lockett, Celia Guillard, Tobias Lauinger, Zhaozhi Li, Jacob M Montgomery, Damon McCoy, What Drives Perceptions of the Political in Online Advertising?: The Source, Content, and Political Orientation, Journal of Experimental Political Science, 2025
- RecSys'25 Laura Edelson, Frances Haugen, Damon McCoy, A Comparative Survey Of Algorithmic Feed Recommendation System Designs, ACM Transactions on Recommender Systems, 2025
- PoPETS'25 Julia B Kieserman, Athanasios Andreou, Chris Geeng, Tobias Lauinger, Damon McCoy, Tracker Installations Are Not Created Equal: Understanding Tracker Configuration of Form Data Collection, Privacy Enhancing Technologies Symposium (PoPETS) 2025
- PoPETS'25 Cat Mai, Bruno Coelho, Julia Kieserman, Lexie Matsumoto, Kyle Spinelli, Eric Yang, Athanasios Andreou, Rachel Greenstadt, Tobias Lauinger, Damon McCoy, More and Scamier Ads: The Perils of YouTube's Ad Privacy Settings, Privacy Enhancing Technologies Symposium (PoPETS) 2025
- CSCW'25 Rafael Martinez, Chris Geeng, Damon McCoy, 'It Would Be a Lot Harder for Them to Change Their Mind....They Grew Up in Like a Very Different Time and a Very Different Location': Barriers to Misinformation Corrections in Online Black and Latine Private Spaces, Proceedings of the ACM on Human-Computer Interaction, 2025
- JoTS'25 Laura Edelson, Borys Kovba, Hanna Yershova, Austin Botelho, Damon McCoy, Tobias Lauinger, Measurement and Metrics for Content Moderation: The Multi-Dimensional Dynamics of Engagement and Content Removal on Facebook, Journal of Online Trust and Safety, 2025

- CSCW'24 Kejsi Take, Victoria Zhong, Chris Geeng, Emmi Bevensee, Damon McCoy, Rachel Greenstadt, Stoking the Flames: Understanding Escalation in an Online Harassment Community, Proceedings of the ACM on Human-Computer Interaction, Volume 8, Issue CSCW1
- PoPETS'24 Kejsi Take, Jordyn Young, Rasika Bhalerao, Kevin Gallagher, Andrea Forte, Damon McCoy, Rachel Greenstadt, What to Expect When You're Accessing: An Exploration of User Privacy Rights in People Search Websites, Privacy Enhancing Technologies Symposium (PoPETS) 2024
- IF'24 Andres Zapata Roza, Alejandra Campo-Archbold, Daniel Diaz-Lopez, Ian Gray, Javier Pastor-Galindo, Pantaleone Nespoli, Felix Gomez Marmol, Damon McCoy, Cyber democracy in the digital age: Characterizing hate networks in the 2022 US midterm elections, Information Fusion, Volume 110, 2024
- PoPETS'23 Enze Liu, Sumanth Rao, Sam Havron, Grant Ho, Stefan Savage, Geoffrey M Voelker, Damon McCoy, No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps, Privacy Enhancing Technologies Symposium (PoPETS 2023.1) 2023
- PLOS'22 Alberto Bracci, Matthieu Nadini, Maxwell Aliapoulios, Damon McCoy, Ian Gray, Alexander Teytelboym, Angela Gallo, Andrea Baronchelli, Vaccines and more: The response of Dark Web marketplaces to the ongoing COVID-19 pandemic, PLOS One, Volume 17, Issue 11, 2022
- PoPETS'22 Kejsi Take, Kevin Gallagher, Andrea Forte, Damon McCoy, Rachel Greenstadt, "It Feels Like Whack-a-mole": User Experiences of Data Removal from People Search Websites, 22nd Privacy Enhancing Technologies Symposium (PoPETS 2022.3) 2022
- EPJ'21 Alberto Bracci, Matthieu Nadini, Maxwell Aliapoulios, Damon McCoy, Ian Gray, Alexander Teytelboym, Angela Gallo, Andrea Baronchelli, Dark Web Marketplaces and COVID-19: before the vaccine, EPJ Data Science, 2021 [Impact Factor 5.08]
- BTLJ'17 Aniket Kesari, Amanda Maya, Chris Hoofnagle, Damon McCoy, Detering Cybercrime: The Focus on the Intermediaries, 32(3) Berkeley Technology Law Journal 2017. [Top ranked technology law journal by Google Scholar h5-index 22]
- JNSLP '16 Zachary K. Goldman and Damon McCoy. Detering Financially Motivated Cybercrime. Journal of National Security Law and Policy, Vol. 8, No. 3, 2016.
- CACM '16 Meiklejohn, Sarah and Pomarole, Marjori and Jordan, Grant and Levchenko, Kirill and McCoy, Damon and Voelker, Geoffrey M. and Savage, Stefan. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. Communications of the ACM Volume 59 Issue 4, April 2016
- ;Login '13 Mohammad Karami, Damon McCoy. Rent to Pwn: Analyzing Commodity Booter DDoS Services. USENIX ;login:, Vol. 38, No. 6, December 2013.
- ;Login '13 Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. USENIX ;login:, Vol. 38, No. 6, December 2013
- TMC '10 Jeffrey Pang, Ben Greenstein, Michael Kaminsky, Damon McCoy, Srinivasan Seshan. Wifi-Reports: Improving Wireless Network Selection with Collaboration. IEEE Transactions On Mobile Computing, Vol. 9 2010. [Impact Factor: 2.28]

Refereed Conference Publication

- eCrime'25 From Lamborghinis to Ladas: Empirical Analysis of LockBit's Business Operations, APWG Symposium on Electronic Crime Research (eCrime) 2025
- ICWSM'25 Julia Jose, Chris Geeng, Kediell O Morales, Damon McCoy, Rachel Greenstadt, What's in a Label? Propaganda Labels and User Sharing Behavior on Social Media Platforms, AAAI Conference on Web and Social Media, 2025
- S&P'25 Kevin Bryson, Arthur Borem, Phoebe Moh, Omer Akgul, Laura Edelson, Tobias Lauinger, Michelle L Mazurek, Damon McCoy, Blase Ur, Characterizing the Usability and Usefulness of U.S. Ad Transparency Systems, IEEE Symposium on Security and Privacy, 2025
- PAM'25 Victor Le Pochat, Cameron Ballard, Lieven Desmet, Wouter Joosen, Damon McCoy, Tobias Lauinger, Partnerka in Crime: Characterizing Deceptive Affiliate Marketing Offers, Passive and Active Measurement, 2025
- eCrime'24 Tom Meurs, Raphael Hoheisel, Marianne Junger, Abhishta Abhishta, Damon McCoy, What To Do Against Ransomware? Evaluating Law Enforcement Interventions, APWG Symposium on Electronic Crime Research (eCrime) 2024
- eCrime'24 Jack Cable, Ian W Gray, Damon McCoy, Showing the Receipts: Understanding the Modern Ransomware Ecosystem, APWG Symposium on Electronic Crime Research (eCrime) 2024
- SOUPS'24 Chris Geeng, Natalie Chen, Kieron Ivy Turk, Jevan Hutson, Damon McCoy, "Say I'm in public... I don't want my nudes to pop up." User Threat Models for Using Vault Applications, Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)
- CCS'23 ChangSeok Oh, Chris Kanich, Damon McCoy, Paul Pearce, Cart-ology: Intercepting Targeted Advertising via Ad Network Identity Entanglement, ACM SIGSAC Conference on Computer and Communications Security, 2023
- WWW'23 Bruno Coelho, Tobias Lauinger, Laura Edelson, Ian Goldstein, Damon McCoy, Propaganda Politica Pagada: Exploring U.S. Political Facebook Ads en Espanol, Proceedings of the Web Conference (WWW), 2023 [h5-index 90]
- ISTAS'22 Rasika Bhalerao and Damon McCoy, An Analysis of Terms of Service and Official Policies with Respect to Sex Work, IEEE International Symposium on Technology and Society 2022 (ISTAS 2022)
- CSCW'22 Rasika Bhalerao, Nora McDonald, Hanna Barakat, Vaughn Hamilton, Damon McCoy, Elissa M. Redmiles, Ethics and Efficacy of Unsolicited Anti-Trafficking SMS Outreach, ACM Conference on Computer-Supported Cooperative Work and Social Computing, Issue CSCW, 2022 [h5-index 58]
- WWW'22 Cameron Ballard, Ian Goldstein, Pulak Mehta, Genesis Smothers, Kejsi Take, Victoria Zhong, Rachel Greenstadt, Tobias Lauinger and Damon McCoy, Misinformation Brokers: Understanding the Monetization of YouTube Conspiracy Theories, Proceedings of the Web Conference (WWW), April 2022 [h5-index 90]
- Security'22 Victor Le Pochat, Laura Edelson, Tom Van Goethem, Wouter Joosen, Damon McCoy, Tobias Lauinger, An audit of Facebook's political ad policy enforcement, Proceedings of the USENIX Security Symposium, August 2022 [h5-index 81]

- IMC'21 Max Aliapoulios, Kejsi Take, Prashanth Ramakrishna, Daniel Borkan, Beth Goldberg, Jeffrey Sorensen, Anna Turner, Rachel Greenstadt, Tobias Lauinger, Damon McCoy, A Large-Scale Characterization of Online Incitements to Harassment Across Platforms, Proceedings of the ACM Internet Measurement Conference (IMC), October 2021 [h5-index 41]
- IMC'21 Laura Edelson, Minh-Kha Nguyen, Ian Goldstein, Oana Goga, Damon McCoy, Tobias Lauinger, Understanding Engagement with (Mis)Information News Sources on Facebook, Proceedings of the ACM Internet Measurement Conference (IMC), October 2021 [h5-index 41]
- CSCW'21 Periwinkle Doerfler, Andrea Forte, Emiliano De Cristofaro, Gianluca Stringhini, Jeremy Blackburn, Damon McCoy, "I'm a Professor, which isn't usually a dangerous job": Internet-Facilitated Harassment and its Impact on Researchers, ACM Conference on Computer-Supported Cooperative Work and Social Computing, Issue CSCW, 2021 [h5-index 58]
- Security'21 Maxwell Aliapoulios, Cameron Ballard, Rasika Bhalerao, Tobias Lauinger, Damon McCoy, Swiped: Analyzing Ground-truth Data of a Marketplace for Stolen Debit and Credit Cards, Proceedings of the USENIX Security Symposium, August 2021 [h5-index 81]
- Oakland'21 Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, Gianluca Stringhini, SoK: Hate, Harassment, and the Changing Landscape of Online Abuse, IEEE Symposium on Security and Privacy (Oakland), May 2021 [h5-index 79]
- CSCW'21 Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, Nicola Dell, "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums, ACM Conference on Computer-Supported Cooperative Work and Social Computing, Issue CSCW, 2021 [h5-index 58]
- IMC'20 Shehroze Farooqi, Alvaro Feal, Tobias Lauinger, Damon McCoy, Zubair Shafiq, Narseo Vallina-Rodriguez, Understanding Incentivized Mobile App Installs on Google Play Store, Proceedings of the ACM Internet Measurement Conference (IMC), October 2020 [h5-index 41]
- Security'20 Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, Thomas Ristenpart. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. Proceedings of the USENIX Security Symposium, August 2020 [h5-index 81]
- Oakland'20 Laura Edelson, Tobias Lauinger, Damon McCoy, A Security Analysis of the Facebook Ad Library, San Francisco, CA, May 2020 [h5-index 79]
- Oakland'20 Kevin A. Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy, The Many Kinds of Creepware Used for Interpersonal Attacks, San Francisco, CA, May 2020 [h5-index 79]
- WWW '20 Brown Farinholt, Mohammad Rezaeirad, Damon McCoy, Kirill Levchenko, Dark Matter: Uncovering the DarkComet RAT Ecosystem, Proceedings of the Web Conference (WWW), April 2020 [h5-index 90]

- WWW '20 Janith Weerasinghe, Bailey Flanigan, Aviel Stein, Damon McCoy, and Rachel Greenstadt, The Pod People: Understanding Manipulation of Social Media Popularity via Reciprocity Abuse, Proceedings of the Web Conference (WWW), April 2020 [h5-index 90]
- eCrime Rasika Bhalerao, Maxwell Aliapoulios, Iliia Shumailov, Sadia Afroz, Damon McCoy, Mapping the Underground: Supervised Discovery of Cybercrime Supply Chains, IEEE APWG Symposium on Electronic Crime Research (eCrime), Pittsburgh, PA, November 2019
- Security'19 Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, Thomas Ristenpart, Clinical Computer Security for Victims of Intimate Partner Violence, Proceedings of the USENIX Security Symposium, Santa Clara, CA, August 2019 [h5-index 81]
- Security'19 Arman Noroozian, Jan Koenders, Eelco van Veldhuizen, Carlos H. Ganan, Sumayah Alrwais, Damon McCoy, Michel van Eeten, Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting. Proceedings of the USENIX Security Symposium, Santa Clara, CA, August 2019 [h5-index 81]
- Security'19 Vector Guo Li, Matthew Dunn, Paul Pearce, Damon McCoy, Geoffrey M. Voelker, Stefan Savage, and Kirill Levchenko, Reading the Tea Leaves: A Comparative Analysis of Threat Intelligence, Proceedings of the USENIX Security Symposium, Santa Clara, CA, August 2019 [h5-index 81]
- WWW '19 Periwinkle Doerfler, Kurt Thomas, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, and Damon McCoy, Evaluating Login Challenges as a Defense Against Account Takeover, Proceedings of the Web Conference (WWW), San Francisco, CA, May 2019 [h5-index 90]
- Security'18 Mohammad Rezaeirad, Brown Farinholt, Hitesh Dharmdasani, Paul Pearce, Kirill Levchenko, Damon McCoy, Schrodinger's Rat: Profiling the Stakeholders in the Remote Access Trojan Ecosystem, Proceedings of the USENIX Security Symposium, Baltimore, MD, August 2018 [Acceptance Rate 19%]
- Oakland'18 Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Kylie McRoberts, Elie Bursztein, Jonathan Levin, Kirill Levchenko, Alex C. Snoeren, Damon McCoy, Tracking Ransomware End-to-end, IEEE Symposium on Security and Privacy (Oakland), San Francisco, CA, May 2018 [Acceptance Rate 11.5%]
- Oakland'18 Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, Thomas Ristenpart, The Spyware Used in Intimate Partner Violence, IEEE Symposium on Security and Privacy (Oakland), San Francisco, CA, May 2018 [Acceptance Rate 11.5%]
- eCrime Hongwei Tian, Stephen M. Gaffigan, D. Sean West, Damon McCoy, Bullet-Proof Payment Processors, IEEE Symposium on Electronic Crime, San Diego, CA, May 2018 [Acceptance Rate 35%]
- IMC'17 Peter Snyder, Periwinkle Doerfler, Chris Kanich, Damon McCoy, Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing, Proceedings of the ACM Internet Measurement Conference (IMC), 2017 [Acceptance Rate 23%]

- EMNLP'17 Greg Durrett, Jonathan K. Kummerfeld, Taylor Berg-Kirkpatrick, Rebecca S. Portnoff, Sadia Afroz, Damon McCoy, Kirill Levchenko, and Vern Paxson, Identifying Products in Online Cybercrime Marketplaces: A Dataset for Fine-grained Domain Adaptation, Conference on Empirical Methods on Natural Language Processing (EMNLP), 2017 [Acceptance Rate 26%]
- KDD'17 Rebecca S. Portnoff, Danny Yuxing Huang, Periwinkle Doerfler, Sadia Afroz and Damon McCoy, Backpage and Bitcoin: Uncovering Human Traffickers, Proceedings of the ACM SIGKDD Conference, Halifax, Nova Scotia, Canada, August 2017 [Oral presentation 5%, Overall Acceptance Rate 21.4%]
- RAID'17 Johannes Krupp, Mohammad Karami, Christian Rossow, Damon McCoy and Michael Backes, Linking Amplification DDoS Attacks to Booter Services, International Symposium on Research in Attacks, Intrusions and Defenses (RAID), Atlanta, GA, September 2017. [Acceptance Rate 20%]
- Oakland '17 Sumayah Alrwais, Xiaojing Liao, Xianghang Mi, Peng Wang, Xiaofeng Wang, Feng Qian, Raheem Beyah, Damon McCoy. Under the Shadow of Sunshine: Understanding and Detecting BulletProof Hosting on Legitimate Service Provider Networks. IEEE Symposium on Security & Privacy, San Jose, CA, May 2017. [Acceptance Rate: 13%]
- Oakland '17 Brown Farinholt, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharamdasani, Haikuo Yin, Stevens LeBlond, Damon McCoy, Kirill Levchenko. To Catch a Ratter: Monitoring the Behavior of DarkComet RAT Operators in the Wild. IEEE Symposium on Security & Privacy, San Jose, CA, May 2017. [Acceptance Rate: 13%]
- WWW '17 Rebecca S Portnoff, Sadia Afroz, Greg Durrett, Jonathan K Kummerfeld, Taylor Berg-Kirkpatrick, Damon McCoy, Kirill Levchenko and Vern Paxson. Automated Analysis of Cybercriminal Markets. Proceedings of the World Wide Web Conference (WWW), Perth, Australia 2017. [Acceptance Rate: 17%]
- Security '16 Kurt Thomas, Juan Antonio Elices Crespo, Ryan Rasti, Jean-Michel Picod, Cait Phillips, Marc-Andre Decoste, Chris Sharp, Fabio Tirelo, Ali Tofigh, Marc-Antoine Courteau, Lucas Ballard, Robert Shield, Nav Jagpal, Moheeb Abu Rajab, Panayiotis Mavrommatis, Niels Provos, Elie Bursztein, Damon McCoy. Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software. Proceedings of the USENIX Security Symposium, Austin, TX, August 2016. [Acceptance Rate: 16%]
- Security '16 Frank Li, Zakir Durumeric, Jakub Czyz, Mohammad Karami, Damon McCoy, Stefan Savage, Michael Bailey, Vern Paxson. You've Got Vulnerability: Exploring Effective Vulnerability Notifications. Proceedings of the USENIX Security Symposium, Austin, TX, August 2016. [Acceptance Rate: 16%]
- eCrime '16 Srikanth Sundaresan, Damon McCoy, Sadia Afroz, and Vern Paxson. Profiling Underground Merchants Based on Network Behavior. Proceedings of the IEEE Symposium on Electronic Crime Research (eCrime), Toronto, Canada, June 2016.
- WWW '16 Mohammad Karami, Youngsam Park and Damon McCoy. Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services. Proceedings of the World Wide Web Conference (WWW), Montreal, Canada, April 2016. [Acceptance Rate: 16%]
- WWW '16 Xiaojing Liao, Chang Liu, Damon McCoy, Elaine Shi and Raheem Beyah. Characterizing Long-tail SEO Spam on Cloud Web Hosting Services. Proceedings of the World Wide Web Conference (WWW), Montreal, Canada, April 2016. [Acceptance Rate: 16%]

- FC '16 Youngsam Park, Damon McCoy and Elaine Shi. Understanding Craigslist Rental Scams. Proceedings of Financial Cryptography and Data Security Conference (FC), Barbados, February 2016.
- NDSS '16 Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, and Damon McCoy. Do You See What I See: Differential Treatment of Anonymous Users. Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2016. [Acceptance Rate: 15%]
- Oakland '15 Kurt Thomas, Elie Bursztein, Chris Grier, Grant Ho, Nav Jagpal, Alexandros Kapravelos, Damon McCoy, Antonio Nappa, Vern Paxson, Paul Pearce, Niels Provos, Moheeb Abu Rajab. Ad Injection at Scale: Assessing Deceptive Advertisement Modifications. IEEE Symposium on Security & Privacy, San Jose, CA, May 2015. [Acceptance Rate: 14%]
- CHI '15 Jason W. Clark, Peter Snyder, Damon McCoy, Chris Kanich. "I Saw Images I Didn't Even Know I Had:" Understanding User Perceptions of Cloud Storage Privacy. Proceedings of the ACM Conference on Computer-Human Interaction, Seoul, Korea, April 2015 [Acceptance Rate: 19%]
- CCS '14 Kurt Thomas, Dima Iatskiv, Elie Bursztein, Tadek Pietraszek, Chris Grier, Damon McCoy. Dialing Back Abuse on Phone Verified Accounts. Proceedings of the ACM Conference on Computer and Communications Security, Scotsdale, AZ, November 2014. [Acceptance Rate: 19%]
- CCS '14 Paul Pearce, Vacha Dave, Chris Grier, Kirill Levchenko, Saikat Guha, Damon McCoy, Vern Paxson, Stefan Savage, and Geoffrey M. Voelker. Characterizing Large-Scale Click Fraud in ZeroAccess. Proceedings of the ACM Conference on Computer and Communications Security, Scotsdale, AZ, November 2014. [Acceptance Rate: 19%]
- IMC '14 David Wang, Matthew Der, Mohammad Karami, Lawrence Saul, Damon McCoy, Stefan Savage, and Geoffrey M. Voelker. Search + Seizure: The Effectiveness of Interventions on SEO Campaigns. Proceedings of the ACM Internet Measurement Conference, Vancouver, BC, Canada, November 2014 [Acceptance Rate: 23%]
- eCrime '14 Jackie Jones and Damon McCoy. The Check is in the Mail: Monetization of Craigslist Buyer Scams. Proceedings of the IEEE eCrime Research Summit, Birmingham, AL, September 2014. [Acceptance Rate: 40%]
- Oakland '14 Sadia Afroz, Aylin Caliskan Islam, Ariel Stolerman, Rachel Greenstadt, Damon McCoy. Doppelganger Finder: Taking Stylometry to the Underground. Proceedings of the IEEE Symposium and Security and Privacy, San Jose, CA, May 2014. [Acceptance Rate: 14%]
- NDSS '14 Danny Yuxing Huang, Hitesh Dharmdasani, Sarah Meiklejohn, Vacha Dave, Kirill Levchenko, Alex C. Snoeren, Stefan Savage, Nicholas Weaver, Chris Grier, and Damon McCoy. Botcoin: Monetizing Stolen Cycles. Network and Distributed System Security. San Diego, CA, 2014. [Acceptance Rate: 18%]
- NDSS '14 Youngsam Park, Jackie Jones, Damon McCoy, Elaine Shi, Markus Jakobsson. Scambaiter: Understanding Targeted Nigerian Scams on Craigslist. Network and Distributed System Security. San Diego, CA, 2014. [Acceptance Rate: 18%]
- eCrime '13 Mohammad Karami, Shiva Ghaemi and Damon McCoy. Folex: An Analysis of an Herbal and Counterfeit Luxury Goods Affiliate Program. APWG eCrime Researchers Summit. San Francisco, CA, 2013. [Acceptance Rate: 42%]

- eCrime '13 Sadia Afroz, Vaibhav Garg, Damon McCoy, Rachel Greenstadt. Honor Among Thieves: A Common's Analysis of Cybercrime Economics. APWG eCrime Researchers Summit. San Francisco, CA, 2013. [Acceptance Rate: 42%]
- IMC '13 Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. Proceedings of the ACM Internet Measurement Conference 2013. Barcelona, Spain. [Acceptance Rate: 19%]
- Security '13 Kurt Thomas, Damon McCoy, Chris Grier, Alek Kolcz, and Vern Paxson. Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse. Proceedings of the USENIX Security Symposium, Washington D.C., August 2013. [Acceptance Rate: 16%]
- CCS '12 Damon McCoy, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M. Voelker and Stefan Savage. Priceless: The Role of Payments in Abuse-advertised Goods. Proceedings of the ACM Conference on Computer and Communications Security, Raleigh, NC, October 2012. [Acceptance Rate: 19%]
- CCS '12 Chris Grier, Kurt Thomas, Lucas Ballard, Juan Caballero, Neha Chachra, Christian J. Dietrich, Kirill Levchenko, Panayiotis Mavrommatis, Damon McCoy, Antonio Nappa, Andreas Pitsillidis, Niels Provos, Zubair Rafique, Moheeb Abu Rajab, Christian Rossow, Vern Paxson, Stefan Savage, and Geoffrey M. Voelker. Manufacturing Compromise: The Emergence of Exploit-as-a-Service. Proceedings of the ACM Conference on Computer and Communications Security, Raleigh, NC, October 2012. [Acceptance Rate: 19%]
- Security '12 Damon McCoy, Andreas Pitsillidis, Grant Jordan, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey M. Voelker, Stefan Savage, and Kirill Levchenko. PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. Proceedings of the USENIX Security Symposium, Bellevue, WA, August 2012. [Acceptance Rate: 19%]
- IMC '11 Marti Motoyama, Damon McCoy, Stefan Savage, and Geoffrey M. Voelker. An Analysis of Underground Forums. Proceedings of the ACM Internet Measurement Conference, Berlin, Germany, November 2011. [Acceptance Rate: 25%]
- Security '11 Stephen Checkoway, Damon McCoy, Danny Anderson, Brian Kantor, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno. Comprehensive Experimental Analysis of Automototive Attack Surfaces. Proceedings of the USENIX Security Symposium, San Francisco, CA, August 2011. [Acceptance Rate: 16%]
- Security '11 Marti Motoyama, Damon McCoy, Kirill Levchenko, Geoffrey M. Voelker, Stefan Savage. Dirty Jobs: The Role of Freelance Labor in Web Service Abuse. Proceedings of the USENIX Security Symposium, San Francisco, CA, August 2011. [Acceptance Rate: 16%]
- Security '11 Chris Kanich, Nicholas Weaver, Damon McCoy, Tristan Halvorson, Christian Kreibich, Kirill Levchenko, Vern Paxson, Geoffrey M. Voelker, Stefan Savage. Show Me the Money: Characterizing Spam-advertised Revenue. Proceedings of the USENIX Security Symposium, San Francisco, CA, August 2011. [Acceptance Rate: 16%]
- PETS '11 Mashaal AlSabah, Kevin Bauer, Ian Goldberg, Dirk Grunwald, Damon McCoy, Stefan Savage, Geoffrey M. Voelker. DefenestraTor: Throwing out Windows in Tor. Privacy Enhancing Technologies Symposium, Waterloo, Canada, July 2011. [Acceptance Rate: 25%]

- Oakland '11 Kirill Levchenko, Neha Chachra, Brandon Enright, Mark Felegyhazi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Andreas Pitsillidis, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, Stefan Savage. Click Trajectories: End-to-End Analysis of the Spam Value Chain. Proceedings of the IEEE Symposium and Security and Privacy, Oakland, CA, May 2011. [Acceptance Rate: 11%]
- FC '11 Damon McCoy, Jose Andre Morales, Kirill Levchenko. Proximax: A Measurement Based System for Proxies Dissemination. Financial Cryptography and Data Security, St. Lucia, February 2011. [Acceptance Rate: 35%]
- Globecom '10 Harold Gonzales, Kevin Bauer, Janne Lindqvist, Damon McCoy, Douglas Sicker. Practical Defenses for Evil Twin Attacks in 802.11. IEEE Globecom Communications and Information Security Symposium, Miami, FL, December 2010. [Acceptance Rate: 36%]
- Security '10 Marti Motoyama, Kirill Levchenko, Chris Kanich, Damon McCoy, Geoffrey M. Voelker, Stefan Savage. Re: CAPTCHAs – Understanding CAPTCHA Solving from an Economic Context. Proceedings of the USENIX Security Symposium, Washington, D.C., August 2010. [Acceptance Rate: 16%]
- Oakland '10 Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage. Experimental Security Analysis of a Modern Automobile. Proceedings of the IEEE Symposium and Security and Privacy, Oakland, CA, May 2010. [Acceptance Rate: 12%]
- Globecom '09 Kevin Bauer, Damon McCoy, Eric Anderson, Markus Breitenbach, Greg Grudic, Dirk Grunwald, Douglas Sicker. The Directional Attack on Wireless Localization - or - How to Spoof your Location with a Tin Can. Proceedings of the IEEE Globecom Communications and Information Security Symposium , Honolulu, HI, USA, November, 2009. [Acceptance Rate: 35%]
- PETS '09 Kevin Bauer, Damon McCoy, Ben Greenstein, Dirk Grunwald, Douglas Sicker. Physical Layer Attacks on Unlinkability in Wireless LANs. Proceedings of the 9th Privacy Enhancing Technologies Symposium (PETS 2009) , Seattle, WA, USA, August, 2009. [Acceptance Rate: 29%]
- MobiSys '09 Jeffrey Pang, Ben Greenstein, Michael Kaminsky, Damon McCoy, Srinivasan Seshan. Wifi-Reports: Improving Wireless Network Selection with Collaboration. MobiSys '09: 7th International Conference on Mobile Systems, Applications, and Services. Krakow, Poland, 2009. [Acceptance Rate: 20%]
- PETS '08 Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, Douglas Sicker. Shining Light in Dark Places: Understanding the Tor Network. Proceedings of the 8th Privacy Enhancing Technologies Symposium (PETS 2008) , Leuven, Belgium, July, 2008. [Acceptance Rate: 26%]
- MobiSys '08 Ben Greenstein, Damon McCoy, Jeffrey Pang, Tadayoshi Kohno, Srinivasan Seshan, David Wetherall. Improving Wireless Privacy with an Identifier-Free Link Layer Protocol. MobiSys '08: 6th International Conference on Mobile Systems, Application, and Services , Breckenridge, CO, June, 2008. [Acceptance Rate: 18%]

Security '06 Jason Franklin, Damon McCoy, Parisa Tabriz, Vicentiu Neagoie, Jamie Van Randwyk, Douglas Sicker. Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. Proceedings of the 15th USENIX Security Symposium , Vancouver, BC, Canada, August, 2006. [Acceptance Rate: 13%]

#### Refereed Workshop Publication

- WOOT '16 Sahar Mazloom, Mohammad Rezaeirad, Aaron Hunter and Damon McCoy. A Security Analysis of an In Vehicle Infotainment and App Platform. 10th USENIX Workshop on Offensive Technologies (WOOT 16), Austin, TX, August 2015.
- BITCOIN '16 Khaled Baqer, Danny Yuxing Huang, Damon McCoy and Nicholas Weaver. Stressing Out: Bitcoin "Stress Testing". Workshop on Bitcoin and Blockchain Research (BITCOIN), Barbados, February 2016.
- WOOT '15 Sean Palka and Damon McCoy. Fuzzing E-mail Filters with Generative Grammars and N-Gram Analysis. 9th USENIX Workshop on Offensive Technologies (WOOT 15), Washington, D.C., August 2015.
- WEIS '15 Kurt Thomas, Danny Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J. Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, Giovanni Vigna. Framing Dependencies Introduced by Underground Commoditization. Workshop on the Economics of Information Security, Amsterdam, NL, June 2015.
- SecTest '15 Sean Palka and Damon McCoy. Dynamic Phishing Content Using Generative Grammars. Proceedings of the IEEE Workshop on Security Testing, Graz, Austria, April 2015.
- WEIS '14 Neha Chachra, Damon McCoy, Stefan Savage, and Geoffrey M. Voelker. Empirically Characterizing Domain Abuse and the Revenue Impact of Blacklisting. Proceedings of the Workshop on the Economics of Information Security (WEIS), State College, PA, June 2014.
- IWCC '14 Hamed Sarvari, Ehab Abozinadah, Alex Mbaziira, and Damon McCoy. Constructing and Analyzing Criminal Networks. Proceedings of the IEEE International Workshop on Cyber Crime (IWCC 2014), San Jose, CA, August 2014
- CSET '13 Christopher E. Everett and Damon McCoy. OCTANE (Open Car Testbed and Network Experiments): Bringing Cyber-Physical Security Research to Researchers and Students. Proceedings of the Workshop on Cyber Security Experimentation and Test, Washington D.C., August 2013.
- LEET '13 Jason W. Clark and Damon McCoy. There Are No Free iPads: An Analysis of Survey Scams as a Business. Proceedings of the USENIX Workshop on Large-Scale Exploits and Emergent Threats, Washington D.C., August 2013.
- LEET '13 Mohammad Karami and Damon McCoy. Understanding the Emerging Threat of DDoS-as-a-Service. Proceedings of the USENIX Workshop on Large-Scale Exploits and Emergent Threats, Washington D.C., August 2013.
- CSET '11 Chris Kanich, Neha Chachra, Damon McCoy, Chris Grier, David Wang, Marti Motoyama, Kirill Levchenko, Stefan Savage, Geoffrey M. Veolker. Proceedings of Workshop on Cyber Security Experimentation and Test (CSET) San Francisco, CA, August 2011.

- CSET '11 Kevin Bauer, Micah Sherr, Damon McCoy, Dirk Grunwald. Experimentor: A Testbed for Safe and Realistic Tor Experimentation. To appear at 4th USENIX Workshop on Cyber Security Experimentation and Test (CSET) San Francisco, CA, August 2011.
- WIFS '09 Kevin Bauer, Damon McCoy, Dirk Grunwald, Douglas Sicker. BitStalker: Accurately and Efficiently Monitoring BitTorrent Traffic. Proceedings of the 1st IEEE Workshop on Information Forensics and Security , London, United Kingdom, December, 2009.
- WIDA '08 Kevin Bauer, Harold Gonzales, Damon McCoy. Proceedings of 1st IEEE International Workshop on Information and Data Assurance (WIDA 2008) in conjunction with the 27th IEEE International Performance Computing and Communications Conference (IPCCC 2008) , Austin, TX, USA, December, 2008.
- ALPACa '08 Kevin Bauer, Damon McCoy, Dirk Grunwald, Douglas Sicker. BitBlender: Light-Weight Anonymity for BitTorrent. Proceedings of the Workshop on Applications of Private and Anonymous Communications (ALPACa 2008) in conjunction with SecureComm 2008 , Istanbul, Turkey, September, 2008.
- HotNets '07 Jeffrey Pang, Ben Greenstein, Damon McCoy, Srinivasan Seshan, David Wetherall. Tryst: The Case for Confidential Service Discovery. HotNets VI: The Sixth Workshop on Hot Topics in Networks , Atlanta, GA, USA, October, 2007.
- WPES '07 Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno, Douglas Sicker. Low-Resource Routing Attacks Against Tor. Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2007) , Alexandria, VA, USA, October, 2007.
- SECON '07 Damon McCoy, Douglas Sicker, Dirk Grunwald. A Mechanism for Detecting and Responding to Misbehaving Nodes in Wireless Networks. IEEE SDR Workshop, 2007.

### Op-Eds

Laura Edelson, Damon McCoy, How Facebook Hinders Misinformation Research, Scientific American, 2021

Laura Edelson, Damon McCoy, Facebook is obstructing our work on disinformation. Other researchers could be next, The Guardian, 2021

Laura Edelson and Damon McCoy, We Research Misinformation on Facebook. It Just Disabled Our Accounts, New York Times, 2021

Nicki Dell, Karen Levy, Damon McCoy, and Thomas Ristenpart, How domestic abusers use smartphones to spy on their partners, Vox 2018

Damon McCoy, When Studying Doxing Gets You Doxed, Huffington Post, 2018

---

### Teaching

NYU CS-GY 6823/CS-UY3933: Network Security (Fall 2024) Instructor Rating: 4.9/5

NYU CS-GY 9223CS-UY 3943 Special Topics in Computer Science: Security Analytics (Spring 2023) Instructor Rating: 4.9/5

NYU CS-GY 6823/CS-UY3933: Network Security (Fall 2022) Instructor Rating: 4.8/5

NYU CS-GY 6823/CS-UY3933: Network Security (Spring 2021) Instructor Rating: 4.6/5

NYU CS-GY 9223CS-UY 3943 Special Topics in Computer Science: Natural Language Processing (Fall 2020) Instructor Rating: 4.8/5

NYU CS-GY 6823/CS-UY3933: Network Security (Spring 2020) Instructor Rating: 4.8/5  
 NYU CS-GY 9223/CS-UY 3943 Special Topics in Computer Science: Security Analytics (Fall 2019) Instructor Rating: 4.8/5  
 NYU CS-GY 6823/CS-UY3933: Network Security (Spring 2019) Instructor Rating: 4.6/5  
 NYU CS-GY 9223 Special Topics in Computer Science: Security Analytics (Fall 2018) Instructor Rating: 4.7/5  
 NYU CS-GY 6823/CS-UY3933: Network Security (Spring 2018) Instructor Rating: 4.7/5  
 NYU CS-GY 6823/CS-UY3933: Network Security (Fall 2017) Instructor Rating: 4.5/5  
 NYU CS-GY 6813/CS-UY3923: Information Security and Privacy (Spring 2017) Instructor Rating: 4.6/5  
 NYU CS-GY 6823/CS-UY3933: Network Security (Fall 2016) Instructor Rating: 4.8/5  
 NYU CS-GY 6823/CS-UY3933: Network Security (Spring 2016) Instructor Rating: 4.8/5  
 NYU CS-GY 6823/CS-UY3933: Network Security (Fall 2015) Instructor Rating: 4.6/5  
 GMU CS 468: Secure Programming and Systems (Spring 2014) Instructor Rating: 4.4/5  
 GMU ISA 656: Network Security (Fall 2013) Instructor Rating: 4.6/5  
 GMU ISA 656: Network Security (Spring 2013) Instructor Rating: 4.7/5  
 GMU ISA 797/CS 795 Cyber Crime (Fall 2012) Instructor Rating: 4.7/5  
 GMU ISA 656: Network Security (Spring 2012) Instructor Rating: 4.4/5  
 Minority Engineering Summer Bridge Program, Introduction to Computer Science, University of Colorado (Summer 1996)

## Selected Talks

- MIT Cybersecurity for Democracy: Providing Independent Auditing Frameworks for Platform Accountability, Invited Talk 2022
- Cambridge Cybersecurity for Democracy: Providing Independent Auditing Frameworks for Platform Accountability, Invited Talk 2021
- UBristol Cybersecurity for Democracy: Providing Independent Auditing Frameworks for Platform Accountability, Invited Talk 2021
- UTulsa Cybersecurity for Democracy: Providing Independent Auditing Frameworks for Platform Accountability, Invited Talk 2021
- Cambridge Tech Abuse in the Intimate Partner Violence Setting: Issues, Challenges, and Mitigations, Invited Talk 2020
- 28C3 Online Political Advertising, Chaos Computer Congress 2019
- NSC Panelist, Digital Currencies Workshop, National Security Council 2018
- FTC Injuries 101 Panel, Informational Injury Workshop, 2017
- CRA/NSF Understanding the Harms of Doxing, 2017
- DHS Panelist, Transnational Organized Crime Conference, 2017
- FTC Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software, FTC Privacy Con, 2017

- UTulsa Framing Dependencies Introduced by Underground Commoditization, University of Tulsa Invited Speaker, 2016
- Princeton Framing Dependencies Introduced by Underground Commoditization, Center for Information Technology Policy (CITP) Luncheon Speaker Series, 2016
- Google The Case for Deception, Google Tech Talk, 2016
- Qualcomm The Case for Deception, Qualcomm Invited Speaker, 2016
- Facebook Framing Dependencies Introduced by Underground Commoditization, Beers and Breakage, 2016
- FS-ISAC Framing Dependencies Introduced by Underground Commoditization, FBI - Financial - Information Sharing and Analysis Centers, 2016
- ENIGMA Bullet-proof Credit Card Processing, USENIX Enigma Conference, 2016
- NAAG Drug Purchases on the Dark Web Panel, National Association of Attorneys General Eastern Meeting, 2015
- VISA Understanding and Undermining the Business of Cybercrime, Visa Cybersecurity Awareness, 2014
- SXSW An Inside Look at How the Auto Industry is Safeguarding Connected Cars, Panel, SXSW Connected Car Conference, 2014
- SRI Experiences with Automotive Security: Vulnerabilities, Causes and Challenges, Cybersecurity for Government Vehicles Workshop, 2014
- NSF CPS Diversity in CPS. Panel, NSF Cyber-Physical Systems PI Meeting, 2013
- GOOGLE Investigating the Underground in the Name of Science. Google Tech Talk, 2013
- LEET Understanding the Emerging Threat of DDoS-as-a-Service. Conference Talk, USENIX Workshop on Large-Scale Exploits and Emergent Threats, 2013
- CSET Conducting Research Using Data of Questionable Provenance, Panel, Workshop on Cyber Security Experimentation and Test, 2013
- UMD Tracing Money Flows in Bitcoin. Syschat talk, University of Maryland, 2013
- UMD Exploring the Underground Economy. Syschat talk, University of Maryland, 2013
- DCAPS Tracing Money Flows in Bitcoin. D.C. Anonymity and Privacy Seminar, 2013
- DCAPS Stylometry and Underground Markets. D.C. Anonymity and Privacy Seminar, 2012
- DCW Manufacturing Compromise: The Emergence of Exploit-as-a-Service. ISC/CAIDA Data Collaboration Workshop, 2012
- SAFEMEDS Payment Processing and Unlicensed Online Pharmacies. Partnership for Safe Medicines Interchange 2012
- CCS Priceless: The Role of Payments in Abuse-advertised Goods. Conference Talk, ACM Conference on Computer and Communications Security, 2012
- SECURITY PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. Conference Talk, USENIX Security Symposium, 2012
- DCAPS Proximax: A Measurement Based System for Proxies Dissemination. D.C. Anonymity and Privacy Seminar, 2012

- IMC An Analysis of Underground Forums. Conference Talk, ACM Internet Measurement Conference, 2011
- PETS The Ethics of Research on Tor Users. Panel, Privacy Enhancing Technologies Symposium, 2011
- HOTPETS Using Wireless Physical Layer Information to Construct Implicit Identifiers. HotPETS, 2008
- TOORCON BitBlender: Light-Weight Anonymity for BitTorrent. Toorcon, 2007
- DEFCON Zulu: A Command Line Wireless Frame Injector. DefCon, 2007
- SECURITY Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. Conference Talk, USENIX Security Symposium, 2006

## Service

## External Reviewer

SEcurity and RIghts in the CyberSpace (SERICS) 2023 - 2025 (116 million EUR NextGenerationEU Funded)

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN) 2020 - 2024 (7 million GBP UKRI Funded)

## Program Committee Co-Chair

- PoPETs De Gruyter Open Proceedings on Privacy Enhancing Technologies. 2017,2018
- HotSec USENIX Hot Security Topics Workshop, Co-located with USENIX Security Symposium. 2016
- eCrime IEEE Symposium on Electronic Crime Research. 2016, 2017

## Program Committees

- PoPETs De Gruyter Open Proceedings on Privacy Enhancing Technologies. 2022, 2023
- IMC ACM Internet Measurement Conference. 2020,2024, 2025
- ENIGMA USENIX Enigma Conference. 2017, 2018
- WWW ACM International World Wide Web Conference. 2016, 2020, 2024
- WEIS Workshop on the Economics of Information Security. 2016, 2017, 2018
- eCrime IEEE Symposium on Electronic Crime Research. 2014, 2018, 2019
- NDSS Network and Distributed System Security Symposium 2019
- CCS ACM SIGSAC Conference on Computer and Communications Security 2019
- SECURITY USENIX Security Symposium. 2014, 2015, 2016, 2017, 2018, 2020
- ACSAC Annual Computer Security Applications Conference. 2013,2014,2015
- RAID The International Symposium on Research in Attacks, Intrusions and Defenses. 2013,2014
- CSET USENIX Workshop on Cyber Security Experimentation and Test. 2012, 2013
- ICDCS IEEE International Conference on Distributed Computing Systems. 2012, 2015
- PETS Privacy Enhancing Technologies Symposium. 2011, 2012, 2013, 2015
- MCCS ACM Workshop on Mobile Cloud Computing and Services. 2011

### General Service

- NYU PhD admission committee chair, 2019, 2020
- NYUSH Systems Security Faculty Hiring Search Committee, 2019
- NYU Computing@NYU website committee, 2019
- NYU ML Faculty Hiring Search Committee, 2018
- NYU PhD admission committee, 2015, 2016, 2017, 2018
- SECURITY Invited talks committee, USENIX Security, 2014,2015
- NSF General Chair, NSF Cybersecurity Ideas Lab, 2014
- TAPIA Travel scholarship committee, ACM Richard Tapia Celebration of Diversity in Computing, 2010,2012
- MobiSys General Co-Chair, ACM MobiSys Ph.D. Forum Workshop, 2010
- NSF Panelist for a number of NSF funding programs.

---

### Awards

- 2025 PoPETS Best Student Paper Award
- 2022 USENIX Security Test of Time Award
- 2024 ACM Internet Measurement Conference Test of Time Award
- 2022 USENIX Security Distinguished Paper
- 2021 IEEE Security and Privacy Test of Time Award
- 2020 Facebook Internet Defense Prize, Third Place, Declined
- 2020 USENIX Security Distinguished Paper
- 2020 IEEE Security and Privacy Test of Time Award
- 2019 ACM Senior Member
- 2019 Google Research Award (\$24,500)
- 2018 Google Research Award (\$40,000)
- 2016 Junior Faculty Google Security Privacy and Anti-abuse Applied Reward. (\$50,000)
- 2015 Best Practical Paper, IEEE Security and Privacy
- 2013 Best Paper, IEEE APWG eCrime Researchers Summit
- 2012 Google Research Award (\$75,000)
- 2009,2010 NSF/CRA Computer Innovation Fellow (\$250,000 award)
- 2009 Best Presentation, ACM MobiSys PhD Forums Workshop
- 2009 ACM Tapia Celebration of Diversity travel scholarship
- 2008 Best Paper, ACM Mobisys
- 2008 American Indian Science and Engineering Society (AISES) Google travel scholarship
- 1995 - 1999 Minority Engineering Program Scholarship, University of Colorado, Boulder

---

### Testimony

2021 DoJ Expert Witness, United States of America V. MATTHEW GATREL  
2024-2025 FTC Expert Witness, Anti-trust United States of America V. Meta

---

## Memberships

ACM Senior Member, American Indian Science & Engineering Society (AISES) Sequoyah  
Fellow, Cherokee Nation