COMMENT

SURVEILLANCE CLASS ACTIONS: RECONSTRUCTING A FEDERAL DATA PRIVACY PRIVATE RIGHT OF ACTION

NABIL SHAIKH†

Class actions against online platforms alleging improper data collection and sharing practices have increased dramatically in recent years. In 2022, the Federal Trade Commission solicited public comment on governing these practices, which it termed “commercial surveillance,” through rulemaking. This Comment highlights the rise of private commercial surveillance and how both regulation and litigation have been employed to address ensuing harms. This Comment then discusses procedural barriers to these class actions, particularly Rule 23(b)(3)’s predominance requirement and Article III standing, and how some courts have relied on the U.S. Supreme Court’s decisions in Comcast v. Behrend and TransUnion v. Ramirez to heighten those barriers. Finally, this Comment makes several substantive recommendations for a federal privacy law that might overcome these procedural barriers, give effect to a private right of action, and complement regulatory authority.

INTRODUCTION ................................................................. 866
I. REMEDYING STATUTORY SURVEILLANCE HARMs ............ 868
   A. The Problem of Private Digital Surveillance .................. 870
   B. The Regulatory Approach ........................................ 873
   C. The Litigation Approach ........................................ 875
II. PROCEDURAL PROBLEMS WITH SURVEILLANCE CLASS ACTIONS ........................................ 879
   A. The Rule 23(b)(3) Predominance Hurdle ....................... 879

† Executive Editor, Volume 172, University of Pennsylvania Law Review. J.D. Candidate, 2024, University of Pennsylvania; MPA, Princeton University, 2021; A.B., Princeton University, 2017. I am indebted to Judge Anthony Scirica, Professor Cary Coglianese, and Professor Catherine Struve for their guidance on this project. I am also grateful to the editors of the University of Pennsylvania Law Review—especially Will McDonald and Caroline Ribet—for their invaluable feedback and corrections. For support and inspiration, I thank Mostafa El-Harazi and Nergis Chemssy Khan.
1. Damages Class Actions Under Rule 23(b)(3)................................. 879
2. How Comcast Altered the Predominance Standard............... 881
3. Applying the Comcast Predominance Standard to
   Surveillance Class Actions ............................................. 884
   a. The Gmail Class ...................................................... 884
   b. The Facebook Class ................................................. 887
   c. The Google Chrome Class .......................................... 891
B. The Article III Standing Hurdle for Class Members ................. 893
   1. Before TransUnion: The Battle for Concreteness ............... 894
   2. After TransUnion: The Search for a Common Law
      Analogue ...................................................................... 897

III. SUBSTANTIVE SOLUTIONS: TOWARD A WORKABLE PRIVATE
   RIGHT OF ACTION................................................................. 899
   A. Statutory Damages .......................................................... 899
      1. Statutory Damages and Theories of Injury ..................... 899
      2. Statutory Damages and the DirecTV Factors ................. 905
   B. Reworking Consent Exceptions ........................................ 907
   C. A Hybrid Regulatory-Private Enforcement Model ............. 909

CONCLUSION........................................................................... 912

INTRODUCTION

In the past year, nearly a dozen class actions have alleged that the popular
social media application TikTok surveils its users.¹ The complaints argue that
TikTok monitors users’ clicks and keystrokes by attaching JavaScript code to
its in-app browser and collects highly personal information about users,
including revealing browsing patterns, without user consent.² TikTok’s
interest in this information is apparent. As one of the lawsuits points out,
data has become a commodity more valuable than oil,³ and the third-party
data brokerage practice has exploded in tandem with the rise of targeted
behavioral advertising.⁴ TikTok is not alone; class actions targeting the data

¹ Skye Witley, Does TikTok ‘Wiretap’ Users? Mounting Privacy Suits Press Claim, BLOOMBERG
² See, e.g., Complaint at 17, Fugok v. TikTok, No. 23-00779 (E.D. Pa. filed Feb. 28, 2023)
(offering the example of a user who navigates to the Planned Parenthood website in the in-app
browser and then navigates to webpages on topics such as sexual orientation, gender identity, and
abortion).
³ Id. at 1.
privacy practices of large online platforms by alleging violations of laws like the federal Wiretap Act—a statute at the core of the TikTok lawsuits—saw a significant upick in 2022.5 Plaintiff’s lawyers are using statutes designed to apply to government surveillance techniques to instead target private enterprises (which arguably collect and use even more personal data than law enforcement).6 These lawsuits come at a time when the Federal Trade Commission (FTC) has initiated its most ambitious consumer protection rulemaking in decades—an effort meant to curb “commercial surveillance.”7

This objective among litigators and regulators of curbing certain types of private sector data-sharing and monetization is shared by lawmakers. These class actions come at a time of intense legislative debate over a potential federal data privacy law intended both to address privacy harms like those posed by commercial surveillance and to update outdated and highly sectoral federal privacy statutes. Proposals for Congress to pass omnibus data privacy

5 See Jason Stiehl, Precautions for New Wave of Digital Privacy Class Actions, LAW360 (Sept. 26, 2022), https://www.law360.com/articles/1533083/precautions-for-new-wave-of-digital-privacy-class-actions [https://perma.cc/3G4L-FZRR] ("In the past two months alone, these statutes have accounted for well over two dozen class actions across the country, with two to three filed nearly every day, and undoubtedly the wave has not crested."); Kevin Hylton, Data Privacy Class Actions on the Rise, LEXISNEXIS: LEGAL INSIGHTS (June 8, 2023), https://www.lexisnexis.com/community/insights/legal/b/practical-guidance/posts/data-privacy-class-actions-on-the-rise [https://perma.cc/MN52-3EEA] (noting that, along with a major increase in recent years in data breach class actions, consumers have increasingly brought litigation under federal and state wiretap laws against online platforms); see also Joshua Briones, Crystal Lopez & Sofia Nuño, Data Privacy and Website Accessibility: Class Action Trends to Watch in 2023, LAW.COM: CORP. COUNS. (Jan. 24, 2023), https://www.bloomberglaw.com/document/XCA3SMCK0000007cssearch-gmd45mgfeffjzite [https://perma.cc/WP5D-REZZ] (rating data privacy class actions as the number-one type of consumer class action to watch in 2023).

6 See Briones, Lopez & Nuño, supra note 5 (noting plaintiffs’ attorneys usage of “older privacy laws to cover modern online activity” in filing class actions against digital platforms).

legislation frequently entail debate over the inclusion of a private right of action as one enforcement tool in conjunction with regulatory enforcement, agency lawsuits, and state action. But the experiences of putative federal class actions alleging injuries under anti-surveillance statutes, such as the Wiretap Act, the Stored Communications Act (SCA), the Video Privacy Protection Act (VPPA), and Computer Fraud and Abuse Act (CFAA), against online platforms are informative of whether private rights of action actually move the needle on personal data protection. And, if they do move the needle, how can Congress write an omnibus privacy statute to make them more effective?

I call this category of aggregate litigation “surveillance class actions,” in part to echo the FTC’s terminology and in part to distinguish it from the related but distinct category of data breach litigation. Notably, several procedural requirements, including Federal Rule of Civil Procedure 23 and Article III standing, often doom surveillance class actions. Moreover, these procedural problems are informed by the substance of the statute under which litigants bring suit. For example, user consent, which is a total defense under anti-surveillance statutes, often precludes Rule 23 class certification. In addition, statutory damages options under these statutes raise both Article III standing difficulties and Rule 23(b)(3) problems due to two landmark Supreme Court cases: TransUnion v. Ramirez and Comcast v. Behrend, respectively. This interplay of substance and procedure is critical to understanding both judicial trends in surveillance class actions and potential legislative fixes.

In Part I, this Comment highlights the rise of private commercial surveillance and details how both regulation and litigation have been employed to address ensuing harms. Part II discusses procedural barriers to surveillance class actions, particularly Rule 23(b)(3)’s predominance requirement and Article III standing’s concreteness standard. Finally, in Part III, this Comment makes several substantive recommendations for a federal privacy law that can give effect to a private right of action. If Congress were to implement these recommendations, it could overcome many of the existing anti-surveillance statutes’ deficiencies that courts have seized on to preclude recovery. This Comment concludes that litigation can be an effective tool against private commercial surveillance, but only if lawmakers pay special thought to making the private right of action workable in the face of essentially immovable federal procedural barriers.

I. REMEDYING STATUTORY SURVEILLANCE HARMs

Attempts at private enforcement of individual privacy rights have become increasingly common in the wake of both widescale data breaches and alleged
interception of sensitive communications by large companies. Plaintiffs alleging significant privacy harms tend to seek monetary damages in addition to declaratory and injunctive relief under various state consumer protection statutes, state common law of torts and contracts, and federal and state anti-wiretapping laws. Each legal claim poses distinct challenges for plaintiffs seeking to remedy those harms. Despite these challenges, such class actions provide a useful, if flawed, vehicle for aggregating privacy harms into cost-justified suits.

Rather than examining data privacy class actions and regulation as a whole, this Comment focuses on remedies for harms stemming from private commercial surveillance as an especially active area of enforcement and litigation in the modern consumer law arena. This Comment treats this category of aggregate litigation—surveillance class actions—as a subset of many types of data privacy-related litigation, including data breach litigation and lawsuits alleging improper disclosures of circumscribed...
categories of individual information, as well as even non-consumer litigation, such as § 1983 actions raising Fourth Amendment claims.

A. The Problem of Private Digital Surveillance

The FTC recently called attention to the growth of the “surveillance economy” through commercial data practices that run the risk of compromising consumers’ privacy. FTC Chair Lina Khan described this modern landscape as one that allows firms to collect individual data “on a massive scale and in a stunning array of contexts,” creating for consumers “probably the most highly surveilled environment in the history of humanity.” Social media companies play an integral role in the growth of this economy, but so do smartphone makers, mobile application developers, data brokers, and a host of internet-based enterprises. Each type of firm is part of a complex web of data transactions, wherein data is collected and

---

12 For example, under the Driver Privacy Protection Act, a consumer can recover for improper disclosures of their personal information contained in state motor vehicles departments. 18 U.S.C. § 2721; see also Marach v. Spears, 570 U.S. 48, 52-56 (2013) (describing a case in which attorneys, after obtaining names from the South Carolina Department of Motor Vehicles in preparation for a lawsuit against car dealerships in the state, were sued by South Carolina residents under the DPPA); but see Baysal v. Midvale Indem. Co., 78 F.4th 976, 977 (7th Cir. 2023) (affirming dismissal of a putative DPPA class action on standing grounds).

13 Actions under § 1983 alleging Fourth Amendment violations can touch on both personal privacy and unjustified searches of one’s personal property. Compare Doe v. Broderick, 225 F.3d 440, 450-51 (4th Cir. 2000) (holding that substance-use-disorder patient had a legitimate expectation of privacy in his methadone clinic records in his § 1983 lawsuit against police detective who searched those records without probable cause), with Soldal v. Cook Cnty., 506 U.S. 56, 65-66 (finding a § 1983 cause of action in plaintiffs’ allegations that deputy sheriff deprived their Fourth Amendment rights during a search of their mobile homes, notwithstanding lack of invasion of plaintiffs’ privacy).

14 See Trade Regulation Rule on Commercial Surveillance and Data Security, supra note 7, at 512-87 (noting that the surveillance economy capitalizes on information asymmetries by exploiting users’ personal data in various sectors, including health care and employment); see also Fed. Trade Comm’n, Statement of Chair Lina M. Khan Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking Commission File No. R111004, at 2 (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Statement%20of%20Chair%20Lina%20M.%20Khan%2000%20Commercial%20Surveillance%20ANPR%20008112022.pdf [https://perma.cc/7RCW-MSLR] (“The fact that current data practices can have such consequential effects heightens both the importance of wielding the full set of tools that Congress has given us, as well as the responsibility we have to do so.”).

15 Statement of Chair Lina M. Khan, supra note 14, at 1 (quoting NEIL RICHARDS, WHY PRIVACY MATTERS 84 (2021)).

transferred in a lucrative market of user profiling and monetization through strategic targeting.\(^\text{17}\)

As private companies, nearly all social media platforms are incentivized to employ aggregated data-based methods of driving user engagement and offering targeted digital advertising.\(^\text{18}\) Social media companies argue that behavioral or targeted advertising, in particular, is at the core of their business models. Without it, profitability would require membership fees or some other subscription model. There is, of course, the possibility of running non-targeted advertisements, too. But as the recent European Union holding against Meta's targeted advertising practices reveals, large social media companies and other enterprises that offer free services in exchange for running ads will tend to argue that this business model is essential to both their bottom line and much of the digital ecosystem.\(^\text{19}\)

Businesses can thwart users’ expectations of which of their private online activities, communications, and digitally stored content are protected from second- or third-party disclosures. As the FTC’s proposal for commercial surveillance rulemaking suggests, these user expectations implicate significant privacy interests, including both liberty and dignitary interests.\(^\text{20}\) These interests are especially likely to be frustrated as technology in the targeted advertising industry becomes more advanced.

For example, “beacons” are Bluetooth tracking devices hidden in grocery stores, shopping malls, and other shopping areas to communicate with customers’ mobile applications regarding how long the customer spent in certain sections of the store, when they arrived and exited, and, most

\(^{17}\) See Trade Regulation Rule on Commercial Surveillance and Data Security, supra note 7, at 51273-51274 ("Companies ... develop and market products and services to collect and monetize this data. An elaborate and lucrative market for the collection, retention, aggregation, analysis, and onward disclosure of consumer data incentivizes many of the services and products on which people have come to rely.").

\(^{18}\) See Tarleton Gillespie, Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media 206 (2021) (explaining the extent to which private firms are dependent on targeted advertising and the level of data collection that it demands).


importantly, inform which advertisements should be displayed on the customer’s phone.\textsuperscript{21} With respect to dignitary interests, beacon technology might cause some consumers to feel some degree of loss of what Professor James Whitman, in his seminal article on American versus European conceptions of privacy, calls “the right to informational self-determination.”\textsuperscript{22} Specifically, they might feel like such a pervasive catalogue of their activities in a particular space amounts to a loss of the ability to withhold information about their location and movements.\textsuperscript{23} Relatedly, as to liberty interests, customers surveilled in this manner might feel a deprivation of freedom approaching what the Carpenter majority termed “a comprehensive chronicle of [one’s] past movements.”\textsuperscript{24} Whitman’s framework reads liberty interests to focus primarily on the American concern of intrusions by the state.\textsuperscript{25} But in the nineteen years since Whitman’s article, private data collection and concerns about consumer information asymmetry and inadequate consent have raised perhaps even greater alarm than data privacy vis-à-vis the government and law enforcement.\textsuperscript{26}

As an example of just how deeply users can find their privacy interests undermined by this data-sharing ecosystem, take a recent class action against Oracle. Plaintiffs challenged Oracle’s data brokering business wholesale: they alleged that Oracle (1) extracts personal information from internet users, (2) creates individual profiles based on that user data, and then (3) sells that data on the company’s marketplace.\textsuperscript{27} The plaintiffs named various technological tools that Oracle uses to sustain this business model, such as cookies, tracking

\begin{footnotesize}
\begin{enumerate}
\item[22] Whitman, \textit{supra} note 20, at 1161.
\item[23] This concern finds resonance in the European Union’s General Data Protection Regulation’s codification of the rights to rectification and erasure—the latter of which is also known as the “right to be forgotten.” See EU Regulation 2016/679, General Data Protection Regulation, Art. 16, 2016 J.O. (L 119) 43 (“The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.”); EU Regulation 2016/679, General Data Protection Regulation, Art. 17, 2016 J.O. (L 119) 43 (“The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay . . . ”).
\item[25] See Whitman, \textit{supra} note 20, at 1161 (“At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one’s own home.”).
\item[26] According to a recent survey, 81% of individuals are concerned about how \textit{companies} are using their data, and 71% about how \textit{government} uses it. \textit{How Americans View Data Privacy}, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ [https://perma.cc/HR4G-X9EB].
\end{enumerate}
\end{footnotesize}
pixels, cross-device tracking, and certain proprietary code. They further argued that this data business is “ubiquitous throughout the internet” and “requires no relationship between the internet user and Oracle to occur,” such that internet users “may not know Oracle is amassing data about them.” The putative class raised several anti-surveillance statutory claims, including under the federal Wiretap Act.

This is an existential moment for data brokers, social media platforms, and the advertising industry, as more users are taking collective action to hold these players accountable for practices that were once taken for granted as just par for the online course. And as the next section discusses, regulators are trying to follow in lockstep.

B. The Regulatory Approach

American privacy law is famously sectoral, with different statutes regulating different industries. Examples include the financial sector (regulated by FCRA), healthcare (regulated by HIPAA), telephony (regulated by the TCPA), and education (regulated by FERPA). The closest regulatory mandate to a general authority to enforce individual privacy rights and remedy the harms posed by the online tracking and data-sharing practices outlined above belongs to the FTC. Section 5 of the FTC Act allows the agency to penalize companies that partake in “deceptive” or “unfair” practices. “Deception” essentially refers to lying to consumers about a

---

28 Id.
29 Id.
30 See id. at *3.
practice, while the “unfairness” prong covers practices that cause substantial injury to consumers without notable countervailing benefits.34

In recent years, the FTC has pursued aggressive enforcement actions related to modern consumer protection challenges. These have included a settlement with Snapchat over its representations about the disappearing nature of the platform’s “snaps,”35 a lawsuit against Kochava for alleged sales of users’ health data,36 and an order mandating Chegg to strengthen its information security, among other remedial actions.37 The Kochava and Chegg actions saw the FTC branch out more into bringing “unfairness” actions. These are more difficult to prove than Section 5 actions because they require actual showings of consumer harm rather than mere deception.38

Furthermore, the FTC is pursuing the rigorous and arguably cumbersome process of Magnuson-Moss rulemaking to crack down on harmful forms of commercial surveillance.39 The FTC’s proposed rule is a relatively rare move for the agency.40 Although some have called the FTC’s recent rulemaking efforts ambitious, the FTC has defended them as part of the agency’s unambiguous authority to crack down on “unfair” or “deceptive” business practices.41 Although regulators like the FTC do not have to prove harm in the way private plaintiffs might have to,42 regulatory enforcement and other

38 See Citron & Solove, supra note 10, at 814 (2022) ("The definition of unfairness is much more directly focused on harm . . . . [The] definition explicitly includes "likely" harm.").
39 See supra Section I.A. But see Kurt Walters, Reassessing the Mythology of Magnuson-Moss: A Call to Revise Section 18 Rulemaking at the FTC, 16 HARV. L & POL’Y REV. 519, 539-59 (2022) (arguing that Magnuson-Moss rulemaking’s strictures are not significantly more burdensome than Administrative Procedure Act rulemakings).
40 See Chris D. Linebaugh, Cong. Rsch. Serv., LSB10839, FTC Considers Adopting Commercial Surveillance and Data Security Rules 5 (2022) (noting that the FTC’s use of Magnuson-Moss rulemaking is rare but motivated ultimately by the significant economic impact of data privacy requirements).
41 See Trade Regulation Rule on Commercial Surveillance and Data Security, supra note 7, at 51290 ("Some have balked at this ANPR as overly ambitious for an agency that has not previously issued rules in this area, or as coloring outside the lines of our statute in the topics it addresses . . . . But our authority is as unambiguous as it is limited, and so our regulatory ambit is rightfully constrained . . . .").
42 See Andrew D. Selbst & Solon Barocas, Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law, 171 U. PA. L. REV. 1023, 1045 (2023) (noting that the legal standard for an FTC Section 5 unfairness action is likelihood of substantial consumer injury, "an inherently less demanding standard of proof" when compared to the burden of alleging
types of regulatory activity depend on channeling limited personnel and resources toward areas of priority that are in flux across political administrations and time.43

C. The Litigation Approach

The debate over incorporating a private right of action to allow private consumers to hold companies accountable for harmful data privacy practices has been intense.44 Proponents of this change argue a few points. First, a private right of action could empower compensatory goals by equipping individuals with the means to remedy privacy violations and enforce individual rights.45 Second, the threat of private lawsuits can act as a deterrent because it encourages firms to take data privacy seriously.46 Lawsuits hold organizations accountable for their actions and offer a strong incentive to comply with privacy regulations. Third, a private right of action fills in the gaps of resource-constrained government enforcement.47

43 See Citron & Solove, supra note 10, at 844.
44 See, e.g., STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. R.SCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 59-62 (2019) (noting the interwoven nature of the debates over a legislative conferment of both a private right of action and the creation of statutory standing for data privacy harms); Paula Bruenig, How to End the Deadlock on the Private Right of Action, IAPP (Jan. 20, 2022), https://iapp.org/news/a/how-to-end-the-deadlock-on-the-private-right-of-action [https://perma.cc/RX8H-SCCM] (“Whether a [federal privacy] law should include a private right of action has been a persistent point of disagreement for stakeholders and is often cited as an impediment to its passage.”).
46 See Lauren Henry Scholz, Private Rights of Action in Privacy Law, 63 WM. & MARY L. REV. 1639, 1657 (2022) (arguing that the threat of monetary damages makes private suits more of a deterrent than even the threat of public regulatory sanctions).
47 See A Private Right of Action Is Key to Ensuring that Consumers Have Their Own Avenue for Redress, NEW AM., https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/a-private-right-of-action-is-key-to-ensuring-that-consumers-have-their-own-avenue-for-redress [https://perma.cc/g88E-ZTJB] (last visited May 3, 2023) (“If a single federal agency is responsible for privacy enforcement, some individual harms likely would not be addressed . . . . Such under-enforcement could encourage companies to engage in privacy-harming practices if they believe that enforcement would be unlikely. A private right of action is critical for aggrieved individuals who would then be able to intervene and pursue enforcement on their own, without relying on the federal enforcer.”); see also Alec Wheatley, Do-It-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation with a Private Right of Action, 45 GOLDEN GATE U. L. REV. 265, 269 (2015) (noting that the FTC, as “the primary enforcer of privacy law” lacks capacity to respond to every consumer data privacy claim and that its limited enforcement budget is mostly targeted toward the biggest violators).
Opponents of including a private right of action first argue that the burden it places, especially on small and medium-sized firms, is not cost-justified. Second, they argue that regulatory enforcement would be more efficient, as exemplified by high rates of litigation under the Telephone Customer Protection Act, Fair Credit Reporting Act, Video Privacy Protection Act, and the Biometric Information Privacy Act. Third, opponents contend that the potential for inconsistent rulings in different jurisdictions can lead to divergent standards, judicial confusion, and legal uncertainty over which types of privacy practices are sufficient to meet federal standards. Fourth, a supposedly pro-consumer argument against the private right of action is that the cost of litigation is baked into product pricing.

The proposed American Data Privacy and Protection Act (ADPPA) has a unique structure for a private right of action. Essentially, it is a private right of action that becomes available only after the plaintiff jumps through a panoply of procedural hoops. First, the plaintiff has to notify both the FTC

---


49 See U.S. CHAMBER INST. FOR LEGAL REFORM, ILL-SUITED: PRIVATE RIGHTS OF ACTION AND PRIVACY CLAIMS 15 (2019) (describing “rampant litigation” under these statutes for consumer grievances as “drain[ing] judicial resources,” a “breeding ground for long-lasting litigation where procedural violations exist without concrete harm,” and “try[ing] to fit a square peg into a round hole”). One estimate puts the cost of “duplcat[ive] enforcement” stemming from European regulators and consumer protection authorities in both U.S. states and in the federal government itself—in a world with a federal private right of action—at $2.7 billion. Alan McQuinn & Daniel Castro, INFO. TECH. & INNOVATION FOUND., THE COSTS OF AN UNNECESSARILY STRINGENT FEDERAL DATA PRIVACY LAW 16-17 (2019), https://itif.org/publications/2019/08/09/costs-unnecessarily-stringent-federal-data-privacy-law [https://perma.cc/XW5E-8BUH]. Those figures are based on several assumptions, including imputing both dismissal rates from the securities class actions context and the overall proportion of federal to state consumer class actions onto hypothetical rates of data privacy class actions under a federal right of action. See id. at 16 (postulating a 50% rate of dismissal based on the 54% rate for securities class actions in 2017, and a rate of 100 annual lawsuits). Those figures do not account for the likely changes in corporate data collection practices that would take place in advance of the opening of any enforcement window.

50 See ILL-SUITED, supra note 49, at 14 (noting the potential for “a series of inconsistent and dramatically varied, district-by-district court rulings”).

51 See McQuinn & Castro, supra note 49, at 14 (“Lawyers may be happy with extraneous lawsuits, but consumers will ultimately pay the price, as organizations are forced to spend money on duplicative and often frivolous lawsuits, rather than ... lowering prices, offering discounts, or creating new products and services.”). Of course, these pro-consumer effects have to be considered both in the context the actual revenue model of online platforms, many of which do not charge an explicit fee for use, and in light of other consumer protection harms that a private right of action might help mitigate.

52 American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 403 (2022).
and the attorney general of their state of residence of their intent to bring an action.53 Second, each agency has sixty days to consider bringing their own suit.54 Third, the ADPPA presumes bad faith if the party attempts to demand monetary payment before those sixty days are complete.55 Fourth, all demand letters by the plaintiff must link to an FTC webpage outlining the defendant’s rights under the Act.56

Under current law, especially the anti-surveillance laws that this Comment explores as models of current data privacy private enforcement, private rights of action vary in terms of their statutory schema.

First, the federal Wiretap Act provides one useful case study of how private rights of action work in the context of enforcing individual privacy rights against commercial surveillance practices. The Electronic Communications Protections Act of 1986 (ECPA), Title I of which is known as the Wiretap Act, provides a private right action against an entity who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication,” but exempts from liability defendants who can prove that the plaintiff consented to the interception.57 Statutory provisions relating to damages and other available remedies take center stage in courts’ certification analyses under Rule 23.58 Under ECPA, plaintiffs can recover the greater of the following two totals: “(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.”59 I discuss how courts apply this and other remedies provisions to aggregated claims of privacy harms for money damages below.60 Surveillance class actions under the federal Wiretap Act, its companion the Stored Communications Act, and various state analog statutes have started to attract the attention of the defense bar in particular.61

54 Id.
55 Id. § 403(a)(3)(B).
56 American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 403(d).
58 See infra Part II and Section III.A.
59 Id. § 2520(c)(2). Although both provisions technically concern statutory damages, I will refer to subpart (a) as the sum of “actual damages” and “profit damages,” and to subpart (b) as “statutory damages.”
60 See infra Part II.
61 See John Smith, For Your 2023 Worry List: Anti-Wiretap Class Actions Against Website Operators Surge, but Proper Consent Can Reduce Risk, JD SUPRA (May 14, 2023), https://www.jdsupra.com/legalnews/for-your-2023-worry-list-anti-wiretap-9941279 [https://perma.cc/BMM2-XYSR] ("Plaintiffs filed even more cases in 2022, and such class actions present legal risk for any company using session replay technology or other technology that captures
Second, compared to ECPA, the Video Privacy Protection Act (VPPA) is narrower: it bars renters and sellers of videos from disclosing “personally identifiable information” about consumers without first obtaining the “informed, written consent . . . of the consumer that (i) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer,” and (ii) is either given at the time of disclosure or given in advance for a set period of time “not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner.”\textsuperscript{62} The statute permits entities to obtain consent “through an electronic means using the Internet.”\textsuperscript{63} The VPPA provides for various forms of relief including monetary relief, statutory damages of up to $2,500 per breach, attorneys’ fees, and preliminary injunctive relief.\textsuperscript{64}

Third, similar in scope to both ECPA and the VPAA, the Computer Fraud Abuse Act (CFAA) generally proscribes various types of access by private third parties of an individual’s computer or phone “without authorization.”\textsuperscript{65}

Because data privacy class actions have long faced difficulties overcoming threshold Article III standing requirements, due to the difficulty in concretizing the harms alleged,\textsuperscript{66} the robust scholarly debate on data privacy class actions has been over how to allege justiciable harms.\textsuperscript{67} There has been comparatively minimal scholarly treatment of certification trends and challenges in data privacy class actions.\textsuperscript{68} But even the literature on standing and data privacy has not looked at this more particular set of class actions that take aim at surveillance and anti-wiretapping harms—suits in which proving concreteness of harm for Article III can be more tenuous. Accordingly, the next Part of this Comment zeroes in on how procedural barriers to certification and standing complicate private lawsuits under these surveillance statutes, and how those complications arise from the contested

\textsuperscript{62} 18 U.S.C. §§ 2710(b)(1)–(2)(B).
\textsuperscript{63} 18 U.S.C. §§ 2710(b)(1)–(2)(B).
\textsuperscript{64} 18 U.S.C. § 2710(c)(2).
\textsuperscript{65} 18 U.S.C. § 1030.
\textsuperscript{66} See Thomas D. Haley, Data Protection in Disarray, 95 WASH. L. REV. 1193, 1235 (2020) (reporting that courts found that data breach plaintiffs had Article III standing in only 47% of cases, compared to a 61% rate of standing in other types of cases).
\textsuperscript{67} See generally Citron & Solove, supra note 10; Andrew Grindstaff, Article III Standing, the Sword, and the Shield: Resolving a Circuit Split in Favor of Data Breach Plaintiffs, 29 WM. & MARY BILL. RTS. J. 851 (2021).
\textsuperscript{68} See, e.g., Nathan Webster, Note, Whose Data Anyway? The Inconsistent and Prejudicial Application of Ascertaintability in Data Privacy Class Actions, 105 MINN. L. REV. 2531, 2553 (2021) (“The limited treatment of ascertainability in data privacy so far paints a worrying picture of inconsistent decisions, penalization of data privacy classes, and no accountability for defendants.”)
nature of issues in privacy law, such as consent, harm, and whether a type of content is actually subject to statutory protections.

This debate over a private right of action can confuse what should be apparent: litigation and regulation serve crucial and, often, distinct purposes. A hybrid enforcement regime, as discussed in Part III, is well-suited to the complex task of protecting individual privacy in the digital age. To underscore this point, consider Professors Stephen Burbank, Sean Farhang, and Herbert Kritzer's in-depth study of the question of private enforcement of so-called public rights. They note that hybrid enforcement regimes require the delegation of some powers to administrative agencies and others to private litigants and courts, where one form of enforcement might have a “dominant role” and the other “a more ancillary one.” Although this Comment focuses largely on private enforcement, Congress will need to give serious thought to the relative strengths of regulatory action in the commercial surveillance context—whether that action is dominant or ancillary.

II. PROCEDURAL PROBLEMS WITH SURVEILLANCE CLASS ACTIONS

If lawmakers seek to provide for a private right of action in a potential federal data privacy law, it is useful to examine how plaintiffs have employed similar rights of action in existing federal privacy laws. This Part analyzes two procedural barriers that putative classes engaged in litigation under the aforementioned anti-surveillance laws often confront: Rule 23(b)(3) predominance and Article III standing. Courts have taken divergent approaches to the legal questions these barriers present. These approaches and the ensuing confusion for plaintiffs and defendants alike provide crucial information for Congress as it considers various federal privacy bills.

A. The Rule 23(b)(3) Predominance Hurdle

1. Damages Class Actions Under Rule 23(b)(3)

Given that civil anti-surveillance claims are litigated in aggregate, plaintiffs will usually seek to certify a damages class to obtain monetary recovery. Class actions for damages are thought not just to help redress harm but especially—in the case of high-volume, small-value claims—to “protect

---

70 Id. at 661.
71 See id. at 668-69 (discussing how hybrid regimes empower administrators to articulate substantive law or to prosecute enforcement actions, regulate complex and uncertain policy areas by promulgating broad rules, and mount litigation campaigns to advance certain policy goals).
broader societal interests," including through deterrence of future harm.\textsuperscript{72} A damages class seeking certification under Rule 23(b)(3) must satisfy additional requirements beyond those in Rule 23(a), which apply to all class actions irrespective of relief sought.\textsuperscript{73} Rule 23(a) lists four prerequisites that named plaintiffs must satisfy for certification, often summarized as numerosity, commonality, typicality, and adequacy of representation.\textsuperscript{74} Rule 23(b)(3) requires courts to confirm two additional facts before certifying a damages class: “[T]hat the questions of law or fact common to class members \textit{predominate} over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.”\textsuperscript{75}

The Rule 23(b)(3) predominance requirement shares some content with the Rule 23(a) commonality requirement, but the former is ultimately more exacting than the latter.\textsuperscript{76} They are similar in that each requires some level of showing that class members share legal and factual issues enough to justify aggregating the claims. However, whereas the commonality requirement demands the existence of common issues of law or fact, the predominance requirement demands that those common issues outweigh, to some extent, each class member’s individual issues. Courts assessing whether predominance is present in a class under Rule 23(b)(3) take two steps.\textsuperscript{77} The court first characterizes the issues presented by the class as either individual or common.\textsuperscript{78} Then, the court weighs these two buckets of issues, determining

\textsuperscript{72} Citron & Solove, \textit{supra} note 10, at 819; see also Stephen P. Burbank & Sean Farhang, Rights and Retrenchment: The Counterrevolution Against Federal Litigation 138-39 (2017) (“Rule 23 \textit{is} used to aggregate a massive number of people asserting the same small, even technical, \textit{statutory} violations . . . .”); Alexandra Lahav, The Continuum of Aggregation, 53 Ga. L. Rev. 1393, 1395-97 (2019) (noting that class actions help “provide global peace subject to judicial approval” by precluding future claims and solving the principal-agent problem via judicial monitoring).

\textsuperscript{73} Fed. R. Civ. P. 23(a)–(b).

\textsuperscript{74} Fed. R. Civ. P. 23(a).

\textsuperscript{75} Fed. R. Civ. P. 23(b)(3) (emphasis added).

\textsuperscript{76} See Amchem Prods. v. Windsor, 521 U.S. 591, 623-24 (1997) (“Even if Rule 23(a)’s commonality requirement may be satisfied by that shared experience, the predominance criterion is far more demanding.”).

\textsuperscript{77} See id. at 245 (6th ed. 2022) (“The predominance analysis logically entails two steps—the characterization step and the weighing step.”).

\textsuperscript{78} See id. at 247-51. Newberg and Rubenstein on Class Actions § 4:50, at 245 (6th ed. 2022) (“The predominance analysis logically entails two steps—the characterization step and the weighing step.”).
which is more substantial. This second “weighing” step is considered more qualitative than quantitative.  

The two requirements differ not only in terms of what plaintiffs must demonstrate to achieve certification but also in their ultimate purposes. As with the other Rule 23(a) prerequisites, the commonality requirement is a procedural safeguard guaranteeing that the named plaintiffs sufficiently represent the class’s interests. The additional requirements in Rule 23(b)(3), however, are meant to promote judicial economy and “uniformity of decision as to persons similarly situated, without sacrificing procedural fairness or bringing about other undesirable results.” Such concerns—judicial economy, uniformity, and procedural fairness—manifest in damages class actions in particular, given that parties to such actions could, as a practical matter, pursue their own individual suits for damages without foreclosing other class members’ own potential damages actions.

2. How Comcast Altered the Predominance Standard

A near-universal question across Rule 23(b)(3) class actions is how to approach individualized damages calculations for each class member despite the assignment of classwide liability to the defendant. A damages class at minimum should have a “common grievance,” but it may not present injuries fit for identical disseminations of damages to each member. Courts have generally not interpreted this fact of most damages class actions to pose a particular certification problem because the predominance inquiry focuses on the requirement’s core purpose: preserving judicial economy by preventing the expenditure of the district court’s resources on individualized

79 Id. at 252-55 (“Once the issues have been characterized, courts then loosely compare the issues subject to common proof against the issues subject solely to individualized proof to assess whether the common issues predominate. This is more of a qualitative than quantitative analysis.”).

80 See Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 349 (2011) (“Rule 23(a) ensures that the named plaintiffs are appropriate representatives of the class whose claims they wish to litigate.”).

81 Amchem, 521 U.S. at 615 (quoting the Federal Rules Advisory Committee’s note).

82 Whereas class actions for equitable relief under Rule 23(b)(2) and for avoiding inconsistent or widely dipositive adjudications under Rule 23(b)(1) “are presumed to have inter-related members,” members of Rule 23(b)(3) classes could theoretically pursue money damages on their own without implicating other litigants who are similarly situated. 2 RUBENSTEIN, supra note 77, § 4:49, at 195.


84 Alex Parkinson, Comcast Corp. v. Behrend and Chaos on the Ground, 81 U. CHI. L. REV. 1213, 1216 (2014); see Proposed Amendments to Rules of Civil Procedure for the United States District Courts, 39 F.R.D. 69, 103 (1966) (noting the appropriateness of class actions in cases where common liability is found, notwithstanding the necessity of individualized determinations of damages suffered by class members).
determinations of liability. The idea that the need in most damages class actions to calculate individual damages does not undermine Rule 23(b)(3) predominance was broadly accepted until ten years ago.

Then, in 2013, the Supreme Court in Comcast v. Behrend articulated a new framework for the predominance analysis, applying heightened scrutiny to whether the class’s damages model requires consideration of enough individualized issues to frustrate Rule 23(b)(3)’s judicial economy concerns.

In Comcast, the Court was confronted with a challenge to the Rule 23(b)(3) certification of a class of Comcast cable-television subscribers who alleged that Comcast had violated the Sherman Act § 1 by participating in illegal swap agreements. The plaintiffs asserted four theories of antitrust impact, but the district court accepted only one, the “overbuilder” theory, when it certified the class. Plaintiff’s expert, however, had provided only one damages model that, rather than parsing out the damages resulting from each proposed theory of impact, collated all the theories of injury into his calculations. A divided Third Circuit panel affirmed, but the Supreme Court reversed and decertified the class, holding that the plaintiffs had failed to establish that damages could be measured classwide, resulting in a predominance of individual issues over common questions with respect to damages. Specifically, the Court found that disaggregation of the relationship between each theory of impact and the calculated damages was impossible based on the presentation of expert evidence at the district court.

Whether this holding changed the predominance standard is an open question. On the one hand, the Court prescribed two distinct tracks for the predominance analysis: (1) Did the defendant cause injury that is capable of proof common to the class rather than to individual members? (2) Are the damages resulting from that injury measurable on a classwide basis through

---

85 See Comcast Corp. v. Behrend, 569 U.S. 27, 41 (2013) (Ginsburg, J., and Breyer, J., dissenting) (“In particular, when adjudication of questions of liability common to the class will achieve economies of time and expense, the predominance standard is generally satisfied even if damages are not provable in the aggregate.”).

86 Id. at 42.

87 Id. at 34.

88 Id. at 30. The Sherman Act was the first federal antitrust statute in the United States. The Antitrust Laws, FED. TRADE COMM’N, https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws [https://perma.cc/8ZYQ-GTHV] (last visited Nov. 28, 2023). A § 1 violation specifically involves anticompetitive agreements between or among parties. See Sherman Antitrust Act of 1890, 15 U.S.C. § 1 (“Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal.”).

89 Comcast, 569 U.S. at 31.

90 Id.

91 Id. at 34.

92 Id. at 37-38.
the use of a “common methodology.” On the other hand, the Comcast Court stated that its holding relied on a “straightforward application of class-certification principles.” But as the dissent—unusually authored jointly by two Justices—noted, applying the predominance analysis as a two-part determination undermines the well-established doctrinal rule that the presence of damages issues unique to individual class members does not justify denial of 23(b)(3) certification.

Three judicial approaches to analyzing predominance as to liability and predominance as to damages models arose in the wake of Comcast. First, the court may find that plaintiffs’ damages calculation model is related to their liability theory, so predominance is satisfied. Second, a court may reject class certification because, as in Comcast itself, the damages model lacks connection with the liability theory. Third, a court may certify a class only as to liability but not as to damages—the so-called “bifurcation approach.” The second and third approaches seem to accord with the notion that Comcast changed the predominance analysis from one that merely required characterization and weighing to one that required slightly different analysis for liability and damages. Some scholars have argued that, together with Dukes, where the Supreme Court heightened the commonality certification requirement under Rule 23(a), Comcast signifies “a marked shift in the Court’s class action jurisprudence—from requiring common questions to requiring common answers.”

This shift and the trend of competing approaches among lower courts are both captured in certification orders on data privacy class actions. The cases discussed below highlight two litigations, one in which a court refused certification after finding a lack of common-issue-predominance as to liability only, and another in which a court found predominance as to liability but not as to damages.

93 Id. at 30. That the Comcast court used the phrase “resulting from” in its second predominance question supports the notion that this is a sequential, two-step inquiry. Id.
94 Id. at 34.
95 See id. at 42 (Ginsburg, J., and Breyer, J., dissenting) (“Recognition that individual damages calculations do not preclude class certification under Rule 23(b)(3) is well-nigh universal.”).
97 Id.
98 Id.
99 Id.
100 Ormerod, supra note 8, at 305 (2022).
101 See infra Section II.A.3.
3. Applying the Comcast Predominance Standard to Surveillance Class Actions

When courts aim to establish predominance of common issues over individual ones before certifying a Rule 23(b)(3) class, they first must consider whether the facts and legal questions before them evince a classwide theory of liability.102 Prior to Comcast, the crux of the predominance analysis was this question of liability, while the ability to prove damages using classwide proof was at most one of many factors that some courts used to inform the liability inquiry.103 Today, identifying a collective theory of liability remains a crucial first step in many courts’ interpretation of Comcast. Class members must establish that the defendant caused individual injury “capable of proof at trial through evidence . . . common to the class rather than individual to its members.”104

In the cases I discuss below, several district courts considered whether theories of privacy infringement and breach were capable of classwide proof. At issue were federal and state anti-wiretapping law claims, common law and statutory consumer protection claims, common law tort and contract claims, and statutory privacy claims. The complicated webs of liability theories in these cases produced multiple putative subclasses and, in some cases, frustrated certification. Notably, some courts interpreting Comcast went beyond merely looking for a classwide theory of liability, and searched additionally for a damages model that would not necessitate overly individualized inquiries. Accordingly, I also examine whether the classes that survived the predominance inquiry on the liability prong in these cases were able to demonstrate damages models that passed muster on the second step of the Comcast framework.

a. The Gmail Class

In In re Google Inc. Gmail Litigation, the district court denied Rule 23(b)(3) certification to a putative class of both users of Google’s Gmail service and those who exchanged messages with Gmail users.105 These plaintiffs

---

102 See supra notes 83–100 and accompanying text.
103 See Parkinson, supra note 84, at 1213-14; see also, e.g., McLaughlin v. Am. Tobacco Co., 522 F.3d 215, 231 (2d Cir. 2008) (“And while the fact that damages may have to be ascertained on an individual basis is not, standing alone, sufficient to defeat class certification . . . it is nonetheless a factor that we must consider in deciding whether issues susceptible to generalized proof ‘outweigh’ individual issues.” (citations omitted)); cf. Shelter Realty Corp. v. Allied Maint. Corp., 75 F.R.D. 34, 37 (S.D.N.Y. 1977) (“The predominance requirement calls only for predominance, not exclusivity, of common questions.”).
104 Comcast Corp. v. Behrend, 569 U.S. 27, 30 (citation omitted).
challenged Google’s operation of Gmail under state and federal anti-
wiretapping laws, including ECPA and other state anti-wiretapping acts, such
as California’s Invasion of Privacy Act (CIPA). They alleged that Google
(1) read contents of emails received by @gmail.com email addresses for
keywords, (2) extracted concepts from the content of the emails, and (3)
acquired and stored metadata from the content of the emails.

The district court denied certification on predominance grounds entirely
and did not reach Google’s alternate theories for disposition: ascertainability
under Rule 23(a) and superiority under Rule 23(b)(3). The action was split
across four classes and three subclasses. The four classes all alleged federal
ECPA violations, and the three subclasses alleged violations of California,
Florida, and Maryland anti-wiretapping statutes. The court noted the
ECPA consent exemption and then claimed that the state anti-wiretapping
statutes all contained similar consent exemptions. But there was a critical
difference between the federal consent exemption and the state versions:
although the federal provision also exempts defendants from liability even
where just one of the parties to a communication gives consent, the three
state laws “require[d] all parties to the intercepted communication to have
consented.”

Notwithstanding these differences, the court collapsed its determination
of whether the consent exemption raised sufficiently common questions of
liability into one inquiry for all of the federal-law classes and state-law
subclasses. It determined that individual questions of consent overwhelmed
the common ones. The first step the court took was to separate the consent
analysis into distinct questions of express and implied consent. The express
consent analysis focused on whether the members of the different classes
could establish consent to Google’s alleged interceptions through agreement
to the platform’s terms of service, privacy policies, and disclosure policies.
The court accepted Google’s argument that proving explicit consent would

106 Id. at *1.
107 Id. at *3.
108 Id. at *11.
109 Id. at *10
110 Id. at *1, *10.
111 Id. at *12-13 (“It shall not be unlawful . . . for a person acting under color of law
to intercept a wire, oral, or electronic communication, where such person . . . has given prior consent
to such interception.” (quoting 25 U.S.C. § 2511(2)(c))); see also supra notes 56–60 and accompanying
text.
113 Gmail, 2014 WL 1102660, at *13 (emphasis added).
114 See id. at *14, *21.
115 Id. at *14.
116 Id. at *14-15.
require substantial individual questions as to only one of the four classes. Because Google lacked a uniform privacy policy for all administrators of Google Apps, the court reasoned, “end users received vastly different disclosures depending on with which educational institution they were affiliated.” Moreover, the differences in disclosures among educational institutions were substantial enough such that a fact-finder would need to analyze the context on a highly individualized, user-by-user basis in order to conclude whether these institutions consented to Google’s policies.

As to the other three classes, the court declined to reach a conclusion with respect to Google’s lack of classwide liability on an express consent theory, given the court’s subsequent holding that determining whether implied consent was present across all four classes necessitated overly individualized inquiries. The court grounded this holding in the proposition that establishing users’ implied consent to Google’s alleged interceptions is a fact-intensive determination. A court would have to examine “all of the circumstances surrounding the interceptions to determine whether an individual knew that her communications were being intercepted.” Furthermore, the court found that it would have to look at a “panoply of sources” from which the class members could have learned of Google’s interceptions beyond Google’s internal policies and terms of service. These sources include other webpages on Google describing privacy policies and newspaper articles. Determining users’ implied consent would require probing what each user knew about interception practices. The court therefore refused to certify the class on the basis of a lack of predominance in the plaintiffs’ theory of liability without reaching the question of common proof of damages.

117 Id. at *15. The class was a group of Google Apps for Education users. Id. at *10, *15.
118 Id. at *15.
119 Id. at *17 (“[T]he Court finds that individual issues regarding consent are likely to overwhelmingly predominate over common issues.”).
120 Id. at *16.
121 Id. at *18 (“This fact-intensive inquiry will require individual inquiries into the knowledge of individual users.”).
122 Id. at *16.
123 Id. at *17.
124 Id.
125 Id. at *18 (“Such inquiries . . . will lead to numerous individualized inquiries that will overwhelm any common questions.”).
126 Id. at *21 (“[T]he Court cannot conclude that Plaintiffs have met their burden of demonstrating that the proposed Classes satisfy the predominance requirement.”).
b. The Facebook Class

The plaintiffs’ claims in *Campbell v. Facebook* were similar to those in *In re Google Inc. Gmail Litigation*. They pled that Facebook’s alleged practice of intercepting the platform users’ messages violated ECPA and the CIPA.127 Specifically, the putative class members claimed that if Facebook found links to webpages while scanning users’ private messages on the platform, Facebook would treat the shared link as a “like” of the linked webpage.128 The plaintiffs also alleged that Facebook used these webpage “likes” to deliver targeted advertising to the users.129

The district denied Rule 23(b)(3) certification to the class, which was defined as “all natural-person Facebook users located within the United States who have sent or received private messages that included URLs in their content, from within two years before the filing of this action up through and including the date when Facebook ceased its practice.”130 In this section, I consider the *Campbell* court’s initial Rule 23(b)(3) predominance determination as to Facebook’s liability, which the court held was capable of common proof.131 I then discuss the court’s opposite conclusion as to the plaintiffs’ damages model.

The *Campbell* court held that common proof could establish two core issues of liability: (1) that Facebook’s practices violated ECPA and CIPA and (2) whether plaintiffs implicitly consent to Facebook’s practices.132 On the first issue, the court weighed arguments as to whether Facebook had intercepted message “contents” or the messages’ “record information”—ECPA permits interception only of the latter.133 The court rejected Facebook’s argument that determining whether the company had intercepted “contents” would require a “URL-by-URL, message-by-message, sender-by-sender analysis.”134 Instead, the court accepted the plaintiffs’ argument that common evidence, such as the company’s source code, could readily resolve the “contents” question under the statutory scheme.135

However, the court’s conclusion on the second issue concerning consent stood in stark contrast to the *Gmail* court’s holding just two years prior. The

---

128 *Id.* at 255.
129 *Id.* at 255-56.
130 *Id.* at 256, 269.
131 Cf. *id.* at 266-67 ("While it is ultimately plaintiffs' burden to show that common issues predominate over individual ones, if plaintiffs have made such a showing, it falls to Facebook to rebut that showing and to present the court with a basis for reaching the opposite result.").
132 *Id.* at 264-66.
133 *Id.* at 265.
134 *Id.* (citations omitted).
135 *Id.*
Campbell court sought to distinguish Facebook’s message-scanning practices from the alleged interceptions in Gmail. In Campbell, only implied consent, not express consent, was at issue. The plaintiffs argued that common evidence could substantiate a determination of whether they, as Facebook users, implicitly consented to the platform’s message-scanning policies. The plaintiffs pointed to evidence of Facebook employees objecting to, as well as the company’s attempts to hide, the practices at issue. Furthermore, the court observed that “the evidence in this case is a far cry from the evidence cited in [Gmail],” given that Facebook had produced only one document that disclosed its message-scanning practices, whereas Google had several privacy and disclosure policy documents, terms of service, and other platform webpages that discussed its practices. Thus, the court held that determining implied consent would not require as individualized an inquiry.

The Campbell court concluded that individual issues predominated only for a single issue: whether the plaintiffs had implicitly consented to the practice of increasing the “like” counter every time a URL was shared in private messages. Citing the same idea posited in Gmail, the Campbell court explained that no matter where a plaintiff learns of a practice, mere knowledge of the practice can establish implied consent. Here, Facebook’s practice of increasing webpages’ “Like” counters through the sharing of links to those pages in private messages had been reported by news outlets in 2012. Consequently, the various “media reports” of the practice created a wide base of sources from which the plaintiffs could have learned of, and therefore implicitly consented to, the practice. But while Facebook disclosed its “Like” counter practice publicly, the company never disclosed its

---

136 Id.
137 Id. at 265.
138 See id. at 265 (“Plaintiffs also point out that both the ECPA and CIPA require that the alleged interception occur without consent, and they argue that the class members’ lack of consent will be established through common proof.”).
139 Id. at 266.
140 Compare id. (“Even if Facebook hid its practice, as long as users heard about it from somewhere and continued to use the relevant features, that can be enough to establish implied consent.”), with In re Google Inc. Gmail Litig., No. 13-MD-02430, 2014 WL 1102660, at *17, *19 (“[W]here consent may only be implied in a narrow set of circumstances, a broad set of materials are relevant to determining whether such consent should be implied.”).
141 Campbell, 315 F.R.D. at 267.
142 Id. at 266.
143 See id. (“Even if Facebook hid its practice, as long as users heard about it from somewhere and continued to use the relevant features, that can be enough to establish implied consent.”); see also In re Google Inc. Gmail Litig., 2014 WL 1102660, at *16 (“[A]ll materials to which an individual has notice are relevant to consent, not just contractual agreements.”).
144 Campbell, 315 F.R.D. at 266.
145 Id.
general message-scanning practices. It is for this reason that the court held that the same "panoply of sources" in Google that frustrated common-issue-predominance was not present in Campbell with respect to those practices.

The Campbell court ultimately denied Rule 23(b)(3) certification under the damages prong of the Comcast framework, although it initially found general predominance of common issues with respect to Facebook's alleged liability under ECPA and the CIPA. The plaintiffs in Campbell sought two types of damages: (a) profit damages—i.e., the sum of the "profits made by the violator as a result of the violation"—under ECPA, and (b) statutory damages under both ECPA and the CIPA. Although the ECPA scheme provided that profit damages should be added to the plaintiffs' actual damages, the Campbell plaintiffs chose not to seek any "actual damages," instead relying entirely on profit damages and statutory damages.

Analyzing the claims for profit damages, the court concluded that the plaintiffs' damages model was insufficient, because their expert neglected to provide a method for calculating individual damages based on Facebook's profits. As a preliminary matter, the court noted that the plaintiffs' expert analyzed profit damages in two ways: (1) the company's benefits from using improperly intercepted data to enhance its "Social Graph" (a measure of the strength of Facebook's social network), and (2) the benefits that Facebook derived from inflating its "Like" counter via its message-scanning practices.

The court found that the expert did tie the former set of benefits to profits that the company derived from advertising. But the expert made no similar connection between the latter set of benefits and any profits for the company, the court concluded. Even as to the relationship between the intercepted messages and the benefits to the platform's Social Graph, the expert made

---

146 Id.
147 See id. at 267 ("This dearth of evidence regarding implied consent stands in stark contrast to the extensive evidence cited by the Gmail court, leaving the court no basis to find, as the Gmail court did, that 'some class members likely viewed some of these . . . disclosures.'").
148 Id. at 266-67.
149 Id. at 267.
150 Id.; see also 18 U.S.C. § 2520(c)(2) (stipulating that the court can set damages as the greater value between (A) the sum of actual damages suffered by the plaintiff and profits made by the violator and (B) statutory damages).
151 Campbell, 315 F.R.D. at 268 ("[P]laintiffs' expert's report falls short . . . [I]t makes no attempt to actually calculate the profit attributable to each individual interception.").
152 Id. at 267.
153 Id.
154 Id.
what the court claimed to be an improper assumption that every intercepted message amounted to an equal quantity of profit to Facebook.\textsuperscript{155}

The court found that the plaintiffs’ expert’s method for attributing the classwide measure of profit damages to individual members’ damages would require individualized inquiries into the extent to which each alleged interception contributed to Facebook’s profits.\textsuperscript{156} Although this calculation could theoretically result in a straightforward distribution of damages, the court observed that the expert left open the crucial issue of what common method could “actually calculate the profit attributable to each individual interception.”\textsuperscript{157} The court was frank in recognizing “the difficulty, if not impossibility” of ascertaining profit damages under anti-wiretapping laws. The court claimed, “[I]t does not intend to foreclose all privacy-related class actions under Rule 23(b)(3), [but] the court’s finding simply illustrates the difficulty of calculating non-statutory damages under the ECPA.”\textsuperscript{158}

Still, given the difficulties in succeeding on a profit damages theory under ECPA, the court contended, “Indeed, statutory damages are designed to cover situations exactly like this, where actual damages are ‘uncertain and possibly unmeasurable.’”\textsuperscript{159} The court then considered several factors that other courts have come to apply when determining whether statutory damages awards under ECPA are appropriate.\textsuperscript{160} These factors originate in various anti-pirating actions brought by DirecTV in the early 2000s under ECPA.\textsuperscript{161} The court concluded that only some of these “DirecTV factors” can be analyzed in a manner common to the class—e.g., “whether there was a reasonable purpose for the [statutory] violation” and “whether there is any useful purpose to be served by imposing the statutory damages amount.”\textsuperscript{162} Conversely, factors such as “the severity of the violation” and “the extent of any intrusion into the plaintiff’s privacy” would require more individualized inquiries in the court’s view.\textsuperscript{163} But the most persuasive factor was “whether or not there was actual damage to the plaintiff,” which the court concluded would vary across all of the class members and “would be answered in the

\textsuperscript{155} See id. at 267-68 (explaining that the plaintiffs’ expert’s report fell short because it relied on the assumption that each challenged interception resulted in an equal amount of profit to Facebook).

\textsuperscript{156} Id. at 268.

\textsuperscript{157} Id.

\textsuperscript{158} Id. (emphasis added).

\textsuperscript{159} Id. (quoting Kehoe v. Fidelity Fed. Bank & Tr., 421 F.3d 1209, 1213 (11th Cir. 2005)).


\textsuperscript{161} See DIRECTV, Inc. v. Huynh, 318 F. Supp. 2d 1122, 1132 (M.D. Ala. 2004).

\textsuperscript{162} Campbell, 315 F.R.D. at 268.

\textsuperscript{163} Id.
negative for many class members, including one of the named plaintiffs.”

The court then concluded not only that the statutory damages analysis would fail the second Comcast predominance prong, but would also result in several excessive awards, such that “sorting out those disproportionate damages awards would require individualized analyses that would predominate over
common ones.”

c. The Google Chrome Class

Another recent class action against Google met a fate similar to the Gmail class. In Brown v. Google, L.L.C., plaintiffs alleged that “Google surreptitiously intercepts and collects users’ data even while users are in a private browsing mode,” also known as Incognito Mode. That user data included user IDs issued by visited websites, the user’s browser software information, geolocation, and cookie information saved on the user’s device. The class alleged Wiretap Act claims, in addition to state statutory and common law claims. The plaintiffs’ expert presented various damages models, including (1) an unjust enrichment model, which calculated Google advertising and search revenue and YouTube advertising revenue derived from this Incognito Mode data; (2) a restitution model, in which he aimed to approximate “the payment amount necessary to incentivize individuals to knowingly relinquish their online privacy as a base rate”; and (3) a statutory damages model. Google tried to argue that the expert’s models failed to account for uninjured class members and should thus be excluded. The court rejected that argument, noting that Rule 23(b)(3) does not require resolution of uninjured class members at the class certification stage.

164 Id.
165 Id. at 269.
167 Id.
168 Id. at *1.
169 Id. at *3-4.
170 Id. at *5. Compare Theane Evangelis & Bradley J. Hamburger, Article III Standing and Absent Class Members, 64 EMORY L.J. 383, 385 (2014) (arguing that, because Article III standing is an “irreducible constitutional minimum,” the named plaintiff should be required to prove at the certification stage that it can prove absent class member standing on the basis of classwide proof), with 1 RUBENSTEIN, supra note 77, § 2:3 (“[The TransUnion Court] passed on addressing the antecedent question of whether every class member must demonstrate standing before a court certifies a class, remanding for the Ninth Circuit to consider the class certification ramifications of the Court’s core holding that most of the class in that matter lacked Article III standing. While the implication of that remand could be read as requiring all class members to demonstrate standing at class certification, courts have declined to read TransUnion so broadly.” (citations omitted) (internal quotation marks omitted)).
Turning more squarely to the 23(b)(3) predominance analysis, the court again made it only to the liability prong of the Comcast framework.\textsuperscript{171} And again, the court focused this liability analysis on implied consent.\textsuperscript{172} Specifically, the court considered whether “consumers consented to, or had adequate notice of, the data collected, stored, and disclosed” by Google.\textsuperscript{173} In its defense, Google argued that class members’ awareness of this Incognito Mode data collection varied considerably, that the members likely had varying exposure to media and academic reports concerning this data collection, and that there were several other ways users could have differed in their awareness of this collection, including a “Learn More” hyperlink on the Incognito opening screen that mentioned the possible visibility of some private user browsing data.\textsuperscript{174} Plaintiffs responded that Google waived its implied consent defense via form contract, that Google’s internal documents revealed employee awareness that Incognito data was collected without user consent, and that the media articles Google highlighted did not cover the data collection at issue in this case.\textsuperscript{175}

The court held that, in order to analyze Google’s consent defense, it would have to rely on “individual, and subjective, interactions of what certain class members knew, read, saw, or encountered.”\textsuperscript{176} In other words, this defense analysis rested on overly individualized inquiries.\textsuperscript{177} The court even touched on the judicial economy concerns at play here, noting that it would fall to the jury to sift through the evidence of each individual class member’s consent.\textsuperscript{178} Although the court consequently denied certification to the putative damages class, the court did certify a 23(b)(2) class\textsuperscript{179} and recently denied summary judgment to Google, finding that Google could not establish its express consent defense as a matter of law.\textsuperscript{180}

\textsuperscript{172} Id. at *17-19.
\textsuperscript{173} Id. at *18.
\textsuperscript{174} Id. at *18-19.
\textsuperscript{175} Id. at *19.
\textsuperscript{176} Id.
\textsuperscript{177} See id. (“A factfinder, in determining whether class members impliedly consented to the alleged conduct would have to determine the sources of information to which each class member was exposed. Given the plaintiffs’ strategy, this would require individualized assessment into class members’ experience.”).
\textsuperscript{178} See id. (“[If the class was certified, the jury would be tasked with filtering out what members consented to the alleged conduct, and how. Identifying what members impliedly consented to the alleged conduct, and what members did not, would undoubtedly drive the litigation.”).
\textsuperscript{179} Id. at *19-20.
B. The Article III Standing Hurdle for Class Members

In the past half-century, the Supreme Court has more fully clarified the requirements of Article III standing, including the three fundamental rules of applying standing doctrine to class actions. First, if at least one class representative has standing to pursue her own claims individually, then she also has standing to pursue a class action.181 Second, the class representative does not derive standing from other unnamed class members; she must herself have standing.182 Third, a case is justiciable as long as the class representative has standing; she is not required to demonstrate that each class member, including an absent one, has standing.183

Per Article III’s requirement of an injury-in-fact to retain standing, the Supreme Court has emphasized that the harm has to be “concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.”184 In Clapper, the Court held that an overly speculative injury did not reach the level of concreteness to confer Article III standing on plaintiffs challenging the 2008 FISA Amendment Acts’ authorization of certain types of foreign intelligence-gathering and government surveillance.185

Later, in TransUnion, the Court held that a class cannot merely allege statutory injuries to acquire Article III standing without alleging actual injury.186 But at the class certification stage, the named plaintiffs do not have to prove that every class member has an actual injury that will lead to a collection at the damages stage. Rather, those uninjured class members may merely be prevented from recovery at that later stage.187 Notably, TransUnion was a data privacy case: it concerned the defendant’s accidental practice of incorrectly labeling plaintiffs as potential terrorists in the plaintiffs’ credit reports.188 The TransUnion Court reasoned that only those who actually had that negative mark placed on their credit report had suffered a concrete injury, because their injury was akin to a “traditionally recognized” harm—namely, “the reputational harm associated with the tort of defamation.”189 But plaintiffs who did not suffer that traditionally recognized harm and alleged

185 See id. at 401.
186 See TransUnion, 141 S. Ct. at 2208.
187 See id.
188 See id. at 2195.
189 See id. at 2208 (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
only statutory harms under the Fair Credit Reporting Act (FCRA) were uninjured class members for the purposes of Article III. “Traditionally recognized” privacy harms could match Prosser’s definition of related torts, including intrusion upon plaintiff’s seclusion and public disclosure of a plaintiff’s private life.\textsuperscript{190}

But in addition to traditional common law causes of action to redress privacy harms, Congress has legislated statutory causes to remedy private rights, as discussed above. Similar to FCRA in TransUnion, the Wiretap Act, SCA, and VPPA all lack a harm requirement.\textsuperscript{191} Professors Danielle Citron and Daniel Solove have explained how courts have limited recovery for privacy harms on a statutory private rights theory by superimposing a harm requirement onto statutory liability to satisfy Article III concreteness, “interpreting statutes with statutory damages in ways that require proof of harm to obtain statutory damages,” and limiting which harms they recognize.\textsuperscript{192} A major challenge arising from this jurisprudence is that, in class actions brought under private rights of action created by anti-surveillance statutes, the plaintiffs must allege concrete harm at the class definition stage for all class members—a difficult bar to clear.\textsuperscript{193} This goes beyond predominance of common proof; the plaintiff’s lawyers must aver that there is a shared concrete harm itself.

This Section considers the challenge of finding “traditionally recognized” harms in surveillance class actions. First, I review relevant cases preceding the U.S. Supreme Court’s decision in TransUnion. It appears that a general judicial skepticism toward the justiciability of surveilled classes’ claims was eroding at the turn of this decade. But second, I find that, since TransUnion, courts have started to splinter on the most sensible common law analogue to apply in the Court’s “close relationship to a traditionally recognized harm” test. These disputes turn on relatively squishy analytical distinctions, including which kinds of data collection are “personal” or “offensive” enough to generate a concrete harm.

1. Before TransUnion: The Battle for Concreteness

A relatively early case in this space illustrates the lower courts’ struggle with surveillance class injury claims long before TransUnion and its progeny. In In re Google Android Consumer Privacy Litigation, plaintiffs alleged that Google had placed “spyware” in Android devices in the form of software “hooks” that tracked a user’s activity on a mobile device, which application

\textsuperscript{191} See Citron & Solove, supra note 10, at 811-12.
\textsuperscript{192} See id. at 813.
\textsuperscript{193} See id. at 812.
developers could then use to track users by employing software development kits also provided by Google. The plaintiffs specifically claimed that the spyware collected their personally identifiable information, such as name, gender, geolocation, and application activity. They sought to certify a class and pled, among other allegations, that Google had violated the CFAA. But the court rejected each of the class’s Article III injury arguments. The plaintiffs argued, for example, that Google’s practices diminished the value of their personally identifiable information. The court disagreed that this bare allegation of diminution sufficed to confer standing, because the plaintiffs could not allege with particularity which Android apps accessed that information, nor could they allege to what extent each application decreased the information’s value.

Standing hurdles can often doom VPPA class actions, too. For example, in a putative class action against Barnes & Noble, the named plaintiff alleged that the bookstore disclosed personally identifiable consumer video purchase records to Facebook without her consent. The data transfer included her IP address and purchase information from her phone. The plaintiff argued that this practice violated her privacy and her ability to control what information she shared. The district court adopted the magistrate judge’s recommendation to deny standing to the plaintiff’s claim for preliminary injunctive relief. The plaintiff’s sworn declaration that she would cease to purchase DVDs from Barnes & Noble online until it changed its interface connectivity with Facebook deprived her of standing because she intended to avoid any future harm. “The fact that the VPPA provides for preliminary relief in appropriate circumstances does not trump the standing requirements of the U.S. Constitution,” the magistrate judge concluded.
More recently, in *In re Facebook Internet Tracking Litigation*, the district court heard a challenge to Facebook’s practice of using plug-ins to track the browsing histories of users of the platform who were logged out and visiting third-party websites. The putative class alleged that Facebook developed personal profiles of each user based on their third-party browsing activity and sold it to advertisers. These allegations are a textbook example of a private commercial surveillance harm typified in the social media case law: the parties alleged wiretapping harms under the Wiretap Act, the SCA, and California law. But the district court initially denied standing to the class, claiming that “generalized assertions of economic harm based solely on the alleged value of personal information” were insufficient to confer standing on the plaintiffs. Even if the logged out users’ personal information from which the platform benefitted had “some modicum of identifiable value,” that value, absent connection “to a realistic economic harm or loss that is attributable to Facebook’s alleged conduct,” did not satisfy Article III’s requirement of a concrete harm.

The Ninth Circuit reversed the standing holding. Writing for the panel, Chief Judge Sidney Thomas argued that the plaintiffs had alleged harms to historical privacy rights that Congress and the California legislature both sought to protect in anti-wiretapping statutes. The harm here was an actual injury to—or material risk of such an injury to—each user’s “interest in controlling their personal information.” This relatively recent opinion drew on the advances in technology that had transformed the social media and targeted advertising landscape. As a result, the use of cookies and more attenuated third-party data collection and sharing practices supercharged both the advertising industry and the potential for individual loss of control of private information. Accordingly, the Ninth Circuit held that the class had both constitutional and statutory standing on its Wiretap Act, SCA, and state law claims.

---

204 *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 925 (N.D. Cal. 2015).
205 Id. at 926.
206 Id. at 929-30.
207 Id. at 930; see id. at 932 (noting that plaintiffs did not allege more than a limited market for their browsing histories).
209 See *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 597 (9th Cir. 2020).
210 See id. at 598.
211 Id. at 599.
212 See id. (“[A]dvances in technology can increase the potential for unreasonable intrusions into personal privacy.” (quoting Patel v. Facebook, 932 F.3d 1264, 1272 (9th Cir. 2019))).
213 Id.
2. After TransUnion: The Search for a Common Law Analogue

Although the Ninth Circuit’s reversal on standing with respect to the Facebook internet tracking class action recognizes that privacy harms have concretized in lockstep with technological enhancements in the behavioral advertising industry, TransUnion, decided a year later, complicates the extension of this holding. Most lower courts have yet to apply the TransUnion Court’s “close relationship to a traditionally recognized harm” test to surveillance class actions like the Facebook tracking litigation. But the past two years of case law offer some initial clues.

In Massie v. General Motors, L.L.C., for example, a district court denied standing on “close relationship” grounds in a commercial surveillance case.214 The putative class alleged that General Motors’ websites’ use of “Session Replay” software—which records users’ “mouse movements, clicks, and keystrokes,” as well as “the date, time, and duration of a user’s visit, . . . the user’s IP address, location at the time of the visit, browser type, and device’s operating system”—infringed the class members’ privacy under the Wiretap Act and CIPA.215 The court rejected the plaintiffs’ attempt to analogize the collection of their information via Session Replay to the traditional harms of invasion of privacy and invasion of one’s “interest in controlling their personal information.”216 Crucially, the court reasoned that the information collected about them was not “personal or private within the common law understanding of a privacy right.”217 The court distinguished the pieces of information collected here via Session Replay to information collected in other cases in which courts found standing—e.g., users’ names, email, phone number, addresses, private messages exchanged on a platform.218 Here, the court observed, plaintiffs’ collected information was “anonymized.”219 The court thus reasoned that, under TransUnion, the plaintiffs had failed to allege beyond mere statutory prohibitions and plead actual concrete injuries.220

Another district court recently reached a similar decision in a putative class action against Amazon based on state-law anti-surveillance claims.221

---

215 Id. at *2 (internal quotation marks omitted).
216 Id. at *3. The court quoted the U.S. Supreme Court’s exposition on the latter invasion harm: “[B]oth the common law and the literal understandings of privacy encompass the individual’s control of information concerning his or her person.” U.S. Dept. of Just. v. Reps. Comm. for Freedom of Press, 489 U.S. 749, 763-64 (1989).
217 Massie, 2022 WL 534468, at *2-4 (emphasis added).
218 Id. at *5 (citing Mastel v. Miniclip SA, 21-cv-00124, 2021 WL 2983198, at *6 (E.D. Cal. July 15, 2021)).
219 Id.
220 Id. at *4.
221 See Lugo v. Amazon.com, Inc., 22-cv-01230, 2023 WL 6241200, at *4 (W.D. Wash. Sept. 26, 2023) (“Plaintiffs here allege only that Defendant has retained their personally identifiable..."
The plaintiffs’ claims concerned Amazon’s retention of the types of information at the center of VPPA’s disclosure prohibition: video rental history on Amazon’s Prime Video service.\footnote{222 See id. at *2 (“Plaintiffs allege that Defendant unlawfully retains their personally identifiable information, including their names, addresses, credit card information, and video rental history, in violation of New York and Minnesota state law.”).} Sitting in diversity, the district court rejected plaintiffs’ attempted analogue to an invasion of privacy—much like the \textit{Massie} court did—based on the mere failure to delete records.\footnote{223 Id. at *2; see supra notes 198–203 and accompanying text.} But here, the district court relied on a recent Ninth Circuit decision holding that “the retention of the allegedly illegally obtained records at issue, without more, does not give rise to a concrete injury necessary for standing.”\footnote{224 Phillips v. U.S. Customs & Border Prot., 74 F.4th 986, 988 (9th Cir. 2023).} The Ninth Circuit grounded that holding by referring directly to the facts of \textit{TransUnion}: there, the defendant had, in some instances, merely retained consumer records with false alerts, and as to those instances, the Supreme Court found against concreteness.\footnote{225 TransUnion v. Ramirez, 141 S. Ct. 2190, 2208 (2021); see supra notes 186–90 and accompanying text.} 

But a different district court in the Ninth Circuit, hearing a putative class action against the Walt Disney Company, went the other way.\footnote{226 See James v. Walt Disney Co., No. 23-02500, 2023 WL 7392285, at *5 (N.D. Cal. Nov. 8, 2023).} In \textit{James v. The Walt Disney Company}, the putative class’s claims more closely resembled ones raised in the General Motors litigation—the plaintiffs alleged that the defendant’s website ESPN.com used Oracle software to record user information, including pages viewed, purchase intent, keystrokes, mouse clicks, and search terms.\footnote{227 Id. at *1.} The Walt Disney Company argued that the plaintiff must prove that the interception of that information was “offensive” to sustain standing via analogy to an intrusion upon seclusion harm. The court rejected that argument and, citing to the Ninth Circuit’s decision in \textit{In re Facebook Inc. Internet Tracking Litigation},\footnote{228 In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 597 (9th Cir. 2020); see supra notes 187–96 and accompanying text.} noted that other privacy rights, including an “individual’s control of information concerning his or her person,”\footnote{229 Id. at 598.} could be at issue in \textit{James}.\footnote{230 \textit{James}, 2023 WL 7392285, at *5.} The court even distinguished \textit{Massie}, arguing that plaintiffs here, unlike the \textit{Massie} plaintiffs, alleged that the
information collected was not anonymized. The court also highlighted three cases in which courts found that the same type of user information that the Oracle software had collected was “sufficiently personal.” The court concluded that “to the extent [plaintiffs] have referred to webpages viewed, searches conducted, purchase behavior, and so forth,” they had met their standing burden under TransUnion, notwithstanding their other claims about keystrokes and mouse clicks.

These cases reveal that new battles are taking shape in the surveillance class action landscape in the wake of TransUnion. These battles are over what type of common law analogue a surveillance class can compare its harm to; whether information is sufficiently “personal” to sustain an analogy to the tortious invasion of privacy; and what types of business practices are immune from this new concreteness standard. It remains to be seen how other circuits will handle these issues, especially under federal anti-surveillance laws, and what claims will arise from potential new privacy harms stemming from advances in the fast-paced ad tech industry.

III. SUBSTANTIVE SOLUTIONS: TOWARD A WORKABLE PRIVATE RIGHT OF ACTION

This Part proposes substantive provisions that a federal data privacy law could incorporate to give effect to a private right of action in the face of the procedural hurdles I explored earlier. Each solution is in some way “substantive”—they don’t pretend to change the procedural constraints that exist independent of federal privacy law. But this final section goes further to discuss a hybrid approach—typified by the proposed ADPPA—that combines a regulatory apparatus with a private right of action.

A. Statutory Damages

1. Statutory Damages and Theories of Injury

To give fuller effect to a data privacy private right of action, lawmakers should move past damages calculations based on profit gleaned from illicit wiretaps and interceptions of user information—the calculations that form

231 Id. at *6; see also id. at *6 (“Plaintiffs have made sufficient allegations to create a question of fact as to whether there is sufficiently personal information to support standing.”).
233 James, 2023 WL 7392285, at *6.
234 Id. at *7.
the statutory damages scheme in ECPA. Instead, Congress should legislate a damages provision that lays out the host of tangible and intangible harms that result from data collection and certain forms of targeted advertising—especially when predicated on dubious consent.\(^\text{235}\) Although alleging these harms in federal court would still require accompanying claims of sufficient Article III concreteness,\(^\text{236}\) this explicit congressional embrace of a more comprehensive injury-in-fact paradigm could encourage courts to find standing.\(^\text{237}\)

Such a provision would also encourage finding both Article III concreteness and common-issue predominance as to damages. Whereas derivation of profits from user data is a highly individualized calculation, the harms stemming from data collection and sharing practices that apply to all users of a platform are more amenable to classwide proof.\(^\text{238}\) Specifically, Congress could require a lower level of specificity for those harms that the plaintiff could plead to the district court. In other words, the named plaintiffs could allege that the entire class has experienced some sort of vague detrimental privacy practice (e.g., the sale of their biometric data) that has led to a general set of damages (e.g., dignitary harms, loss of that data’s value).\(^\text{239}\) This legislative action would provide clearer avenues for class counsel to articulate both traditionally recognized harms and damages models capable of common proof.

First, for standing purposes, Congress must identify the common law analogues that courts search for when analyzing statutory harms under a TransUnion analysis. A court might be more inclined to certify a damages class seeking to redress data privacy harms if that class alleges more traditional consumer protection injuries under state common law or statutes, rather than by invoking private rights of action under federal or state anti-wiretapping statutes like ECPA or CIPA.


\(^\text{236}\) See Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016) (reversing the Ninth Circuit for only considering whether the alleged harm was particularized and thus ignoring the concreteness requirement).

\(^\text{237}\) The Spokeo Court made explicit the proposition that Congress’s judgment on the status of different intangible harms is relevant to the Article III inquiry. See id. at 1549 (calling such judgment “instructive and important”).

\(^\text{238}\) A putative class would merely have to offer a model for how a platform has, as a whole, benefitted from a platform-wide, privacy-infringing practice, rather than prove to what extent each user’s subjection to that practice has contributed to the platform’s profit.

\(^\text{239}\) This would avoid the result, in one court’s words, of plaintiffs’ counsel defining a class that “includes a large number of uninjured persons” tending to preclude Rule 23(b)(3) predominance. Krakauer v. Dish Network, L.L.C., 925 F.3d 643, 657 (4th Cir. 2019); cf. id. at 657–58 (certifying the class after construing the TCPA’s private right of action to conclude that the class did not actually include uninjured persons).
But Congress can assist plaintiffs by clarifying the clear intent of a federal privacy law to offer remedies for invasions of individual privacy writ large. By “writ large,” I mean broader categories of personally identifiable information than the buckets of information—names, email addresses, private massages—that the Massie court identified as necessary to sustain an analogy to common law invasion of privacy. These broader categories should clearly include anonymized data that the James court found to be “sufficiently personal,” such as browser activity and viewing activity. Because Congress’s judgment on what types of harms are concrete is “instructive and important,” this sort of explicit clarification—whether in the definition of personally identifiable information, or in a committee or conference report noting the broad categories of privacy harms the statute intends to cover, or, ideally, both—would significantly open the doors to surveillance class actions.

Furthermore, Congress might even be able to curb the impact of the recent series of holdings coming out of the Ninth Circuit on the concreteness of records retention. Recall that in a class action against Amazon, a district court applied a Ninth Circuit holding that the mere retention of users’ illegally obtained private information did not amount to a concrete injury, given TransUnion’s holding that actual disclosure was necessary for a traditional reputational harm. Congress cannot itself supersede that bare constitutional requirement, but it could offer avenues for class allegations that the use of that retained (and illegally obtained) information somehow affects the services or ads that users receive—even without disclosure to third-parties. There is a meaningful difference between the TransUnion fact pattern of users’ records sitting dormant with false alerts attached to them and a major online platform’s retention of private information that feeds into platform algorithms and service provision. Congressional hearings and reports could call attention to that distinction, at the very least.

Second, for predominance purposes, the capability of proving the plaintiffs’ theory of harm on a classwide basis improves when their damages model relates to a financial loss, psychological deficits, and emotional harms that the plaintiffs suffered, rather than profits that a company lost. It is possible to identify both a theoretical and a tentative doctrinal basis for this claim. As a doctrinal matter, several courts have held in favor of Rule 23(b)(3).
predominance on an overpayment theory of injury in consumer protection cases.\textsuperscript{245} At the same time, it appears that virtually no court has endorsed ECPA profit damages as a basis for common-issue predominance as to damages.\textsuperscript{246} As a theoretical matter, a model of injury stemming from a breach of individuals’ privacy rights is more capable of common proof when the class can demonstrate their reliance on the defendant’s implicit promise of privacy-protecting service led to their spending as much as they did on the defendant’s services—or even using the services at all.\textsuperscript{247}

But when the defendant’s business model is driven not by user costs but by advertising revenue, plaintiffs under the current statutory regime have a stronger case if they propose other theories of injury, such as profit or statutory damages. The issue is the speculative nature of damages calculations that rely on a connection between class members’ experiences of privacy infringements and the defendant’s profit from practices that resulted in those privacy harms.\textsuperscript{248} These calculations are also highly individualized. This is the wrong way to apply the predominance analysis: although proving the connection between each interception and the defendant’s profits is speculative at best, demonstrating this connection is required neither by the text of ECPA nor by Comcast. Yet, courts tend to see the application of Comcast in the opposite way, and it would do well for Congress to understand how ambiguities in ECPA’s language contributes to this trend.

Specifically, ECPA outlines the suggested damages calculation only as “the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation.”\textsuperscript{249} Since the Campbell plaintiffs did

\begin{footnotesize}
\textsuperscript{245} See, e.g., Allegra v. Luxottica Retail N. Am., 341 F.R.D. 373, 461 (E.D.N.Y. 2022) (holding that the theory that eyeglass manufacturer’s alleged misrepresentations resulted in consumers’ overpayment for its products was capable of common proof).

\textsuperscript{246} Neither the Campbell court nor even the Campbell plaintiffs’ motion for class certification cites to any precedent that analyzes how to prove—on a classwide basis—that alleged interceptors of ECPA-covered communications. See Plaintiff’s Motion for Class Certification at 21, Campbell v. Facebook Inc., 315 F.R.D. 250 (N.D. Cal. 2016) (No. 13-cv-5996).

\textsuperscript{247} See, e.g., In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig., 341 F.R.D. 128, 163 (D. Md. 2022), vacated and remanded sub nom. In re Marriott Int’l, Inc., 78 F.4th 677 (4th Cir. 2023) (“[The] overpayment theory can be summarized as follows: Marriott was able to charge higher prices for hotel rooms than they would have in a hypothetical ‘but-for’ world in which consumer willingness to pay for a hotel room had shifted in response to consumer knowledge of Starwood’s inadequate data security; consequently, named plaintiffs overpaid for their respective hotel stays as a result of Marriott’s alleged data security failures.”); cf. In re Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 149 (3d Cir. 2015) (noting that plaintiffs failed to allege, when pleading a “damage or loss” under the CFAA, that they “incurred costs” or “lost opportunities to sell” their data due to Google’s cookie practices).

\textsuperscript{248} The Campbell court said as much. See Campbell v. Facebook Inc., 315 F.R.D. 250, 268 (N.D. Cal. 2016) (“[Plaintiffs’ damages model] makes no attempt to actually calculate the profit attributable to each individual interception.”).

\textsuperscript{249} 18 U.S.C. § 2520(c)(2)(A) (emphasis added).
\end{footnotesize}
not seek actual damages, one could argue that the court only had to consider whether the total profits that Facebook generated from its message-scanning practices were capable of measurement on a common basis. Although this task might itself prove difficult as a merits question, it need not lead to overly individualized inquiries. The Campbell plaintiffs alleged privacy harms in the form of nonconsensual scanning of private messages—the data Facebook used to generate more valuable targeted advertising and for other benefits to its social network. And the Campbell court tentatively approved of the plaintiffs’ theory of consent at this procedural stage. Thus, the court could even have defined the individual recovery scheme as an equal share of the profits Facebook derived from the message data it allegedly scanned.

ECPA could be read to allow this “divide the profits equally” approach to a damages predominance analysis. But the most convincing argument against this reading is that “as a result of the violation” refers to the platform’s violation against each user. In today’s era of online platforms with large user bases, it strains reason to define their privacy practices solely as individual violations against each user, rather than a pervasive harm perpetrated against all users.

How does this track onto (b)(3) predominance? Recall that the requirement’s emphasis is whether, for the purposes of class certification, named plaintiffs can make a substantial showing of common-issue-predominance such that the Advisory Committee on Rules’ interests in judicial economy and decision uniformity underpinning Rule 23(b)(3) would be served by certifying profit damages classes. One argument in favor of the equal division of profits approach is that any alleged practice of intercepting digital platform users’ messages likely stems from a common algorithmic practice of scanning and retaining messages that are not end-to-end encrypted. Under that reading, any user of that platform would have suffered an anti-wiretapping statutory injury. The Campbell court itself noted that

250 See Campbell, 315 F.R.D. at 267 (“Plaintiffs do not appear to seek any sum for ‘actual damages.’”).

251 The plaintiffs’ reply in support of their motion of class certification made this very argument. Plaintiffs’ Reply in Support of Motion for Class Certification at 16-17, Campbell v. Facebook, 315 F.R.D. 250 (N.D. Cal. 2016) (“Whether or not Facebook successfully or fully exploited each interception . . . while arguably relevant to an actual damage theory, does not impact the profits and other benefits generated from its broad course of misconduct. Thus, by definition, [plaintiffs’ expert’s model] does not invite any . . . individualized issues.”). The Campbell plaintiffs’ claim for profit damages, when construed in this way, would clearly have satisfied the Comcast requirement “that the damages resulting from that injury were measurable ‘on a class-wide basis’ through use of a ‘common methodology.’” Comcast Corp. v. Behrend, 569 U.S. 27, 30 (2013) (citation omitted).


the source code was one potential basis for finding predominance as to liability. The Campbell court could have then reached an alternate conclusion, at least on the basis of Rule 23(b)(3)’s underlying values of judicial economy and global peace, because litigation at the later remedies stage would focus simply on which plaintiffs were subject to the message-scanning practices, not the extent to which each interception generated company profits.

ECPA does not seem to allow for this argument, as these cases reveal. But Congress could give life to it by amending the statute to specify that “violations” include privacy practices that perpetrate widespread harms on users, irrespective of profit generation on a user-by-user basis. This discussion reveals the weak aptitude of ECPA to modern data protection challenges, as many commentators have argued.

One counterargument to broadening statutory damages provisions in federal laws meant to rein in commercial surveillance is partially convincing: where actual damages are marginal, large consumer protection class actions often result in low plaintiff compensation rates and large class counsel fees. It is telling that the Campbell plaintiffs actually had the option under ECPA of seeking a sum of both profit damages and actual damages, but they chose to reduce their damages model to just profit damages. There might be cause for concern when plaintiffs in surveillance class actions can only articulate statutory damages, if we accept the premise that such damages classes are inefficient as a means of compensation to redress real harms.

In response, I argue a few points. First, it would frustrate the legislative intent apparent in the text of existing anti-wiretapping statutes that plaintiffs, when unable to prove actual damages, can still rely on profit damages as a basis for recovery. Second, although such damages class actions may

[https://perma.cc/EH6N-VDFL] (explaining that messages that are not end-to-end-encrypted pose heightened security risks because they are often sent to external servers).

254 See Campbell, 315 F.R.D. at 264-65 (“Plaintiffs point out that the relevant issues under the ECPA are whether Facebook intercepted its users’ messages while in transit, and whether such interception was conducted in the ordinary course of business, and argue that both issues are susceptible to common proof, such as Facebook’s source code.”).


256 See generally Jason Scott Johnston, High Cost, Little Compensation, No Harm to Deter: New Evidence on Class Actions Under Federal Consumer Protection Statutes, 2017 COLUM. BUS. L. REV. 1, 5 (observing that attorneys’ fees average 300% to 400% of the amount paid to the class).

257 See Campbell, 315 F.R.D. at 267 (explaining that the plaintiffs only sought profit damages, but not actual damages).

258 Recall that, under ECPA, plaintiffs can recover the greater of the following two totals: “(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a
overcompensate class counsel, giving anti-wiretapping statutes full effect via private enforcement will serve an important deterrent interest by incentivizing online platforms to seek affirmative consent to data collection and sharing practices. Third, the Supreme Court’s holding in *TransUnion* might help address the problem of insufficiently injured members remaining in the class at the recovery stage. Indeed, many class members alleging privacy harms often have been subjected to the very wrong that consumer protection and anti-wiretapping statutes aim to prevent: interception and misappropriation, all of which are compounded by the information asymmetry that has long defined the disclosure policies of “free” online platforms like social media applications.

Given the societal and commercial changes in online ecosystems and individual privacy since the last amendments to ECPA, it is due time to broaden, not limit, consumer remedies. Legislating beyond ECPA to provide further protection to consumers from nonconsensual misappropriation of personal data is imperative. Reform-minded lawmakers who want to make it easy for plaintiffs to demonstrate harm in anti-surveillance class actions should follow the Ninth Circuit’s holding in *Facebook Internet Tracking*, where the panel recognized that the unique loss of control that characterizes modern targeted advertising-driven online ecosystems is a sufficient reason to find concrete injury to plaintiffs’ privacy interests.

2. Statutory Damages and the *DirecTV* Factors

Lawmakers should also discourage the application of the *DirecTV* factors to Rule 23(b)(3) predominance for data privacy harms. The factors are judicially innovated strictures on statutory damage awards with little payoff to judicial economy and global peace. These factors, which guide courts in determining whether to award purely statutory damages in privacy cases, have been widely adopted in guiding courts’ ECPA statutory damages analyses. The *DirecTV* factors are difficult to satisfy under a Rule 23(b)(3) result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $1,000,000.” 18 U.S.C. § 2520(c)(2) (emphasis added).

259 *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2280 (2021) (holding that the plaintiffs’ injury bears a “close relationship” to a traditionally recognized harm).

259 *See supra* notes 165–72 and accompanying text.


260 *See supra* notes 165–72 and accompanying text.

261 *See Campbell*, 315 F.R.D. at 268–69 (applying the factors to deny decertification on Rule 23(b)(3) predominance grounds); *see also* Kang v. Credit Bureau Connection, Inc., No. 18-cv-01359, 2022 WL 658105, at *7 (E.D. Cal. Mar. 4, 2022) (same). Recall that these factors include “whether there was a reasonable purpose for the [statutory] violation,” “whether there is any useful purpose to be served by imposing the statutory damages amount,” “the severity of the violation,” and “the extent of any intrusion into the plaintiff’s privacy.” *Campbell*, 315 F.R.D. at 268.
analysis, because, as the *Campbell* court concluded, several are meant to be considered on an individual basis and go to the question of actual damage to the plaintiff.262

As with the preceding discussion on profit damages, heavily weighing factors like the presence of actual damage or the severity of the defendant’s statutory violation seems to collapse multiple distinct inquiries into a single determination of whether ECPA statutory damages are warranted. These inquiries include (1) whether users experienced privacy harms, (2) whether the defendant violated ECPA such that the statutory language clearly provides for a remedy, and (3) whether the defendant profited from the violation such that ECPA profit damages would be appropriate. Theoretically, plaintiffs can fail to establish common-issue-predominance with respect to their entitlement to a share of the profits the defendant derived from unlawful interceptions while still establishing that the defendant committed those interceptions. This circumstance would trigger § 2520(c)(2)(B), which specifies the calculation of statutory damages.263

The *DirecTV* factors are misplaced in any Rule 23(b)(3) predominance analysis because each of the class’s claims for damages should be analyzed in the two-step “characterization” and “weighing” procedure, rather than collapsing into a single determination of the fitness of statutory damages. The *Campbell* court should not have frustrated its analysis under the first *Comcast* prong by finding the statutory violations capable of common proof, but not the related statutory damages.264

Moreover, analyzing at the class certification stage whether there is predominance as to fitness of statutory damages belies the real purpose of Rule 23(b)(3) and *Comcast*: the mere assessment of whether class damages as a general matter (as opposed to a deeper equitable analysis of the fitness of statutory damages) is capable of common proof.265 All plaintiffs should be required to do to certify a class is to allege justiciable injury, not to

262 See supra Section III.A.1.

263 That is, because § 2520(c)(2)(A) is not triggered due to the lack of actual and profit damages, (c)(2)(B) would be triggered because the specified calculation would necessarily be greater. See 18 U.S.C. § 2520(c)(2)(B).

264 This alternate holding would not have violated *Comcast* either, because defining the damages awards that Facebook would theoretically have to have paid out would require a straightforward model that merely catalogues all the class members who were confirmed to have been subjected to its message-scanning practices.

265 Indeed, the thrust of the *DirecTV* factors seems to be an analysis of how equitable a statutory damages award is, given that those factors include questions of whether the defendant had a reasonable purpose to commit the statutory violation and whether the plaintiff’s privacy was intruded upon, among other questions. But this analysis is merely an additional, judicially-engineered hurdle for plaintiffs to satisfy specifically in anti-surveillance cases. This hurdle arose from a particular history of cases that are certainly not applicable to modern anti-commercial surveillance class actions.
demonstrate that statutory damages awards would be equally distributed across the entire class in order to satisfy Comcast’s second prong. Clear legislation that simplifies the factors courts consider when determining statutory damages awards would cure these judicially-created deficiencies in surveillance class actions’ damages holdings.

**B. Reworking Consent Exceptions**

Another core set of issues in these cases is the statutory paradigms around consent as an element of non-liability, or affirmative defense to liability. The *Campbell* court concluded that, while establishing the *Gmail* class members’ consent would have required a fact-intensive inquiry into which of the many disclosures at issue effectuated their consent, the *Campbell* plaintiffs could likely defeat the implicit consent argument on the more limited evidence base in the case.266

The emphasis in the predominance analysis is whether resolving the consent defense issue would require highly individualized proof and *not* whether plaintiffs can defeat a consent defense on the merits. It is thus more appropriate for courts to ask in an ECPA class action whether the plaintiffs can establish that a defendant-company’s disclosure policies *objectively* established user consent through common proof. The *Campbell* court reached this conclusion when it considered the extent of the sources from which users could have learned of Facebook’s practices and implicitly consented to them. The court found *objectively* that the significantly wider range of such sources in *Gmail* justified that court’s consent exemption holding.267 But in *Brown*, the court denied (b)(3) certification entirely on the basis of the inquiry that would be required to establish Google’s affirmative defense of implied consent.

Given that courts may deny certification to surveillance classes based on individualized proof of consent, lawmakers ought to consider legislative provisions that categorically bar certain types of user-platform agreements and digital products from establishing user consent. For example, some courts have rejected the argument that a software licensing agreement or other user-

---

266 *Campbell*, 315 F.R.D. at 266-67 (“This dearth of evidence regarding implied consent stands in stark contrast to the extensive evidence cited by *Gmail* court, leaving the court no basis to find, as the *Gmail* court did, that ‘some class members likely viewed some of these . . . disclosures.’”). This holding aligns with other courts’ determinations that plaintiffs could surmount the reliance hurdle both because the relevant statutes did not require the heightened criterion of individual reliance and the defendant had objectively obtained business from the class members by covering up its susceptibility to a compromising data breach. See, e.g., *In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 341 F.R.D. 128, 159-60 (D. Md. 2022) (holding that the plaintiffs can prove their claims without individualized inquiries overwhelming the common issues).

267 *Campbell*, 315 F.R.D. at 266-67.
platform agreements containing caveats with respect to the software’s collection of personal data can form the basis of consent necessary to evade Wiretap Act scrutiny.268 But other courts have reached the opposite conclusion.269 These outcomes speak to the merits of each case, rather than class certification dispositions, yet those merits holdings are influential for district courts at the certification stage.270 Congress could also specify that this bar extends even further to prohibit the use of media reports on certain data privacy practices as establishing some form of user consent—an argument Google successfully tested in both Gmail and Brown.271 Such claims are dubious as a practical matter, but as it stands, the Wiretap Act and other anti-surveillance laws allow them.

To cabin this categorical legislative bar, Congress could clarify that a platform whose core purpose is creating user profiles through personal data collection is exempt from this bar, provided that user knowledge of that purpose is objectively reasonable.272 These are interpretive issues on which courts have reached varying conclusions. But Congress could harmonize these varied approaches across jurisdictions and states through a well-crafted bar on certain bases for establishing consent, paired with thoughtful exemptions.

268 See, e.g., Lopez v. Apple, Inc., 519 F. Supp. 3d 672, 685 (N.D. Cal. 2021) (holding that Apple’s Siri user agreement contained a “general disclaimer . . . nowhere near specific and unambiguous enough to represent that Siri may activate by accident” and thus that Apple could not establish user consent on the basis of that agreement); In re Meta Pixel Healthcare Litig., No. 22-CV-03580, 2022 WL 17869218, at *10 (N.D. Cal. Dec. 22, 2022) (noting that although the Wiretap Act requires actual consent that is either express or implicit, Meta failed to establish that its policies with respect to collection of user health information demonstrated either explicit notice to consumers or accordance with users’ reasonable expectations as to what Meta was doing with their data); Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1045-46 (N.D. Cal. 2014) (“Apple relies solely on the bolded language in the iOS license agreement in arguing that current Apple device users have consented to its interception . . . . [A] reasonable iMessage user would not be adequately notified that Apple would intercept his or her messages . . . .”); In re Google Assistant Priv. Litig., 457 F. Supp. 3d 797, 823 (N.D. Cal. 2020) (holding that Google’s privacy policy for the Google Assistant voice recognition feature was “too general to conclusively establish consent” because the policy “says nothing about the types of information” that Google would send to third-parties for processing).

269 See, e.g., In re Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1028-29 (N.D. Cal. 2014) (concluding that Yahoo Mail users explicitly consented to Yahoo’s interception, scanning, and analyzing of emails exchanged with non-Yahoo Mail users by agreeing to Yahoo’s terms of service).

270 For example, the Gmail court cited several cases that related directly to the merits of consent exceptions to individual communications interceptions in its predominance holding. See In re Google Inc. Gmail Litig., No. 13-MD-02430, 2014 WL 1102660, at *16-17 (N.D. Cal. Mar. 18, 2014).

271 See supra Section II.A.3.

272 See In re Pharmatrak, Inc., 329 F.3d 9, 20 (1st Cir. 2003) (arguing that where it is “self-evident” that companies are curating services to develop individual user profiles for targeted advertising, such that the inference of user non-consent would be unreasonable, the consent exception to the Wiretap Act should not apply).
C. A Hybrid Regulatory-Private Enforcement Model

This Section offers some concluding thoughts on a statutory framework that, accounting for the shortcomings of the litigation approach, allows for both public and private enforcement to achieve policy goals on privacy like the ones contemplated in the FTC’s commercial surveillance rulemaking. For a policy design to support a hybrid enforcement model that effectively reins in surveillance harms, lawmakers would have to pay careful attention not only to litigation hurdles—as this Comment explores—but also to choice of regulatory approach.

Regulation can generally be classified across two axes: (1) means or ends and (2) micro or macro. The former axis concerns the effect of a regulatory mandate (i.e., mandating certain actions versus mandating certain outcomes), whereas the latter axis concerns the location of the mandate in a causal chain (i.e., addressing the causal pathway versus addressing the final outcome). Choice of one or more of the four regulatory approaches stemming from this classification depends on the particulars of the policy goal and the realities of the practices or entities targeted. A micro-means regulation, for example, involves the prescription of one type of behavior or technology among regulated entities—such as a business’s use of one type of cybersecurity software to protect against breaches. By contrast, a micro-ends regulation looks to target specific outcomes measured among regulated entities: for example, a requirement that online platforms dealing with certain types of sensitive user data stay below a certain threshold of data privacy incidents annually. Furthermore, a macro-ends design, also known as “management-based regulation,” seeks to prescribe certain risk management strategies among regulated entities, including mandates that businesses perform data privacy “impact assessments” and other types of data protection audits.

Perhaps most relevantly, a macro-ends regulatory approach, which can be labeled a “general liability” or “general duty” paradigm, simply exposes regulated entities to ex post liability for failing to meet a certain end. A private right of action that equips plaintiffs with the ability to certify a class

273 See supra Section I.C and Part II.
274 See supra notes 14–15, 39–41 and accompanying text.
275 See generally Cary Coglianese, Managing the Performance of Regulatory Agencies, in HANDBOOK ON REGULATORY AUTHORITIES 284 (Martino Maggetti, Fabrizio Di Mascio & Alessandro Natalini eds., 2022).
276 See id.
277 See id.
278 See id.
280 See generally Coglianese, supra note 275.
and seek money damages under Rule 23(b)(3) for surveillance harms ensuing from a defendant’s privacy practices is a type of macro-ends regulation. But another type of macro-ends regulation is the statutory authorization of agencies to seek penalties, disgorgement, and other ex post remedies from entities that violate some type of legislative rule. The discussion in which this Comment has participated on addressing surveillance harms fits squarely into the macro-ends camp of regulatory paradigm. But that camp is broad enough to encompass strategies that many would traditionally bifurcate into “regulation” and “litigation.” The ADPPA represents a significant attempt at finding a middle ground between pure public and pure private enforcement and recognizes the unique public and private rights implicated by modern data privacy practices and harms.

In other words, what really matters is that lawmakers can equip two sets of regulators (so to speak)—agencies and private individuals—with enforcement authority. In the case of data privacy, such a statute could involve both a private right of action—carefully crafted to avoid the problems highlighted in the rest of this Comment—and civil penalty authority. But that statute would also probably go beyond mere ex post liability: it might take a macro-means approach and require internal privacy audits, or it might take a micro-ends approach and place a cap on third-party data sharing. It might even take a micro-means approach and require specific rights of access and control for users. These, too, are crucial questions of statutory design.

I say statutory because rulemaking could prove an imperfect vehicle for remedying these harms. Although the FTC has long taken certain privacy enforcement actions under Section 5’s unfairness and deception provisions, it has been mostly unable or unwilling to enforce the specific anti-surveillance harms outlined in the Wiretap Act, CFAA, SCA, and other statutes. The agency’s latest commercial surveillance rulemaking represents an attempt to give itself a hook to wield something close to that missing enforcement authority. But that rulemaking has apparently stalled at the time of writing—the FTC has not proceeded past the advance notice of proposed rulemaking stage. Perhaps this stall is due to the complexity of creating a GDPR-like regime by rule, which raises possible Major Questions Doctrine scrutiny.281

The only other venue for public enforcement of those anti-wiretapping rights

---

has been in proceedings where criminal defendants have at times been entitled to suppression remedies as a result of illicit wiretaps by the government. But for those alleging surveillance harms against private companies, civil lawsuits have been the primary, if imperfect, tool.

The ADPPA remedies this gap by conferring an enforcement mandate on the FTC that is explicitly in addition to, but not overlapping with, the FTC’s Section 5 authority.282 The bill also creates a private right of action, but it has notice requirements that limit the pace at which class actions can be brought. The statute does not deal with the particulars of class actions as outlined above, and it does not fully contemplate the specific hurdles that damages classes face in both the certification and standing inquiries in litigation. This point relates to the notice requirements in the sense that, if eventual ADPPA class actions fail for the same reasons current anti-surveillance class actions do, then the FTC’s regulatory authority matters even more than the draft ADPPA would let on. In sum, the question of whether the FTC is capable of redressing surveillance harms in an ADPPA world, or in any world in which the United States has an omnibus federal privacy law, without the additional effective deterrent of private enforcement, is worthy of intense congressional inquiry in the legislative debates to come.

The approach that this Comment takes to designing private rights of action in the data privacy context is grounded in the proposition posed by Professors Burbank, Farhang, and Kritzer that “class action mechanisms should not be designed or deployed . . . on a general (trans-substantive) basis, an approach that necessarily neglects the different regulatory policies and goals of different bodies of substantive law.”283 The policy objectives of privacy law in the consumer context have their own hierarchy—one that will inevitably differ from, for example, environmental law and employment discrimination. In the consumer privacy context, policymakers care about incentivizing claims aggregation to mitigate the natural collective action problems that exist in small-dollar claims litigation.284 But policymakers also worry about harm prevention, including through an agency’s choice to investigate businesses that perpetrate (or are likely to perpetrate) significant consumer injuries, obtain consent decrees in relatively quick fashion (compared to private civil litigation) against violators, create substantive law in the form of rules and common law-like adjudications, issue guidance, and promote all of the above through public-facing communications strategies.

282 See American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 401 (2022) (“The FTC may generally enforce the Act akin to any other violation under the FTC Act, but it may not bring an action under section 5(b) of that Act to stop the same conduct that it brings an enforcement against under this Act.”).
283 Burbank, Farhang & Kritzer, supra note 69, at 640-41.
These regulatory options are all critical to the protection of individual privacy and the prevention of rights-restricting forms of commercial surveillance. The value of individual privacy derives from the protection of user expectations about how their private information is accessed and used. Much of that value is lost due to nonconsensual disclosures of protected information. Accordingly, that value is enshrined in consent exceptions to privacy laws. Congress must ultimately recognize that a macro-ends-based approach which marries a private right of action and civil penalty authority is only as good as the substantive protections that such a hybrid regime offers.

CONCLUSION

As courts will often look to congressional purpose in articulating specific private statutory rights, lawmakers must be explicit in codifying a set of harms that it seeks to redress through data privacy legislation—including, perhaps, the typology of privacy harms (psychological, reputational, economic, and so on) that Citron and Solove discuss in their pathbreaking article. Such action would go a long way in assisting litigants in obtaining statutory standing that satisfies Article III and the Court’s gloss on Article III in TransUnion. In addition, reworking federal privacy law’s model of consent would help parties alleging surveillance harms to form more economical and administrable collective actions that meet Comcast’s two-pronged standard. In the process, those parties might also find avenues for redress that regulatory agencies, especially in the wake of heightened constitutional scrutiny of delegated authority, are currently poorly equipped to provide. Congress’s task, then, in structuring a new private right of action will necessarily entail some level of attention to the fate of lawsuits that have sought to hold firms accountable for these practices under existing privacy laws.

285 Warren and Brandeis alluded to this point in their seminal article on privacy, well over a century ago. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 199-200 (1890) (stating that, with respect to the individual right to determine “to what extent his thoughts, sentiments, and emotions shall be communicated to others,” an author—as an example of an individual who takes his thoughts and attempts to communicate it first to himself—loses that right “only when . . . [he] publishes it.”).

286 See Citron & Solove, supra note 10, at 830-61.