No. 24-14

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ASHLEY POPA, individually and on behalf of all others similarly situated,
Plaintiff - Appellant,
v.
PSP GROUP LLC, doing business as Pet Supplies Plus;
MICROSOFT CORPORATION,
Defendants – Appellees.

On Appeal from the United States District Court
for the Western District of Washington
Case No. 2:23-cv-00294-JLR (Hon. James L. Robart)

BRIEF FOR *AMICUS CURIAE* RETAIL LITIGATION CENTER IN SUPPORT OF DEFENDANTS-APPELLEES

Deborah R. White
Larissa M. Whittingham
RETAIL LITIGATION CENTER, INC.
99 M Street SE, Suite 700
Washington, DC 20003
(202) 869-0200

Aileen M. McGrath
Zach ZhenHe Tan
AKIN GUMP STRAUSS HAUER & FELD LLP
100 Pine Street, Suite 3200
San Francisco, California 94111
(415) 765-9500
amcgrath@akingump.com

Attorneys for Amicus Curiae Retail Litigation Center

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(a)(4)(A), Retail Litigation Center states that it is not a publicly traded corporation; it has no parent corporation; and there is no public corporation that owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

<u>Cases</u>:

<u>OTHER AUTHORITIES</u>:

Qualtrics, *Session replay: Definition, benefits & how to use it effectively* (last visited June 13, 2024) 6, 7, 8, 18

INTEREST OF *AMICUS CURIAE*[1]

The Retail Litigation Center, Inc. ("RLC") is the only trade organization solely dedicated to representing the United States retail industry in the courts. The RLC provides courts with the perspective of the retail industry on important legal issues affecting its members, and on potential industry-wide consequences of significant court cases. Since its founding in 2010, the RLC has filed more than 200 amicus briefs on issues of importance to retailers. Its amicus briefs have been favorably cited by multiple courts, including the Supreme Court of the United States. *See, e.g.*, *South Dakota v. Wayfair, Inc.*, 585 U.S. 162, 184 (2018); *Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519, 542 (2013); *Chewy, Inc. v. United States Dep't of Lab.*, 69 F.4th 773, 777 (11th Cir. 2023). Its member retailers employ millions of workers throughout the United States, provide goods and services to hundreds of millions of consumers, and account for more than a trillion dollars in annual sales.

The RLC has a particular interest in this case because many of its retail members have faced class action lawsuits based on the generic use of Session Replay Code. The RLC submits this brief to provide this Court with important context about

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(2), counsel for *amicus curiae* certifies that all parties have consented to the filing of this brief. Pursuant to Rule 29(a)(4), counsel for *amicus curiae* states that no counsel for a party authored this brief in whole or in part, and no person other than *amicus curiae*, its members, or its counsel made a monetary contribution to its preparation or submission.

the benefits Session Replay Code provides to retailers and consumers alike, the absence of any harm that flows from the use of this commonplace tool, and the urgent need to tamp down on the persistent wave of Session Replay Code lawsuits targeting retailers across the country.

SUMMARY OF ARGUMENT

As the district court below recognized, "[t]his case is one of dozens of proposed class actions being litigated in federal courts across the country challenging the use of 'Session Replay Code[.]'" ER-007. Because Session Replay Code is widely used by retailers with an online presence to improve customer service experiences, retailers as diverse as those selling pet supplies, car tires, plane tickets, outdoor sporting goods, and pizza have been forced to defend themselves against claims of illegal surveillance and wiretapping.

But as the district court correctly concluded below in dismissing this case, those lawsuits run headlong into Article III's limits—particularly the limits the Supreme Court recently emphasized in *TransUnion LLC v Ramirez*, 594 U.S. 413 (2021).[2] Here, Plaintiff "alleges only that she 'brow[s]ed for pet supplies,' and

[2] In the majority of cases challenging the use of Session Replay Code, plaintiffs have advanced novel interpretations of decades-old state "wiretapping" statutes. Those statutes were never intended to (and do not) prohibit harmless forms of website analytics technology like Session Replay Code such that, for this and other reasons, Session Replay Code lawsuits also fail on the merits. Microsoft Answering Br. 40-44.

'communicated with [Pet Supplies Plus's] website by using her mouse to hover and click on certain products.'" ER-015. Such information "reveals nothing more than the products that interested [Plaintiff] and thus is not the type of private information that the law has historically protected." ER-015. Far from being the exception, Plaintiff's allegations are typical of those raised in the lion's share of similar class actions proliferating across the country—many of which have likewise failed due to the plaintiffs' inability to identify any actual injury caused by the use of Session Replay Code. Indeed, it is precisely *because* Session Replay Code does not harm website users that plaintiffs have consistently failed to allege any cognizable Article III injury.

The surge of Session Replay Code lawsuits has created significant burdens for retailers. The plaintiffs in Session Replay Code cases typically purport to represent broad putative classes—often seeking to include *any* individual who has visited a given defendant's website—to ratchet up the defendant's potential exposure. Accordingly, despite the reality that individuals who voluntarily visit a retailer's website suffer no harm from (and, indeed, interact with a more helpful website because of) Session Replay Code, retailers are often forced to expend significant time and money investigating and responding to these claims—with some retailers reasonably opting to avoid these costs through early settlement. Indeed, the sheer volume of Session Replay Code cases suggests that plaintiffs' lawyers are bringing these cases with precisely this outcome in mind.

This Court should affirm the district court's judgment of dismissal and issue a clear rule: The use of Session Replay Code, without more, does not give rise to Article III standing. Such guidance will allow lower courts to efficiently manage the ongoing wave of Session Replay Code lawsuits and preserve the use of commonplace technology that is mutually beneficial for both retailers and their customers.

ARGUMENT

A. SESSION REPLAY CODE IS A VALUABLE RETAILER TOOL THAT PROVIDES VISIBILITY INTO WEBSITE ENGAGEMENT

While umbrella terms like "website analytics" are used colloquially to refer to a wide variety of technological tools, this case centers on Session Replay Code—a specific analytical tool that allows a website operator to recreate a user's interactions on a website in a similar manner to what the user actually experienced. A website operator can use this technology to discover patterns of visitor use, based on an aggregate view of user behavior, that can help the business update the website to best serve its visitors.

By way of a simple example: A customer interested in buying a chew toy for his puppy may visit the Pet Supplies Plus website, spend a minute hovering over different links on the website's homepage, and then navigate to the product category of "Dog," then "Toys & Apparel," then "Play & Chew Toys." That customer then opens a few different browser tabs to compare "Plush Seahorse," "Fat Rooster Dog Toy," and "Heavy Chew Bacon Wishbone." After scrolling through and reading customer reviews of "Plush Seahorse" for another couple of minutes, the customer adds that product to the cart and checks out. Retailers using Session Replay Code can identify such patterns of customer mouse movements, scrolls, and clicks—allowing those retailers to replicate customers' online shopping experiences to detect issues, similar to the way that in-store customer service associates can tell that customers who spend an unusual amount of time moving about in one aisle may be having difficulty locating an item.

Such a tool has practical benefits for both retailers and their customers. Session Replay Code allows online retailers to better understand consumer behavior, leading to more optimized marketing and website design. In particular, Session Replay Code gives online retailers the chance to review "[w]here users get lost or distracted," "[h]ow the page design appears on their browser," "[w]hich site elements grab their attention," and "[w]hat they do before leaving."[3] The result is an improved purchasing experience that helps consumers engage more effectively

[3] Glassbox, *What Is Session Replay? The Complete Guide*, https://www.glassbox.com/session-replay/ (last visited June 13, 2024).

and efficiently with retailers' websites—an outcome that benefits retailers and consumers alike.

For example, if information produced through Session Replay Code demonstrates that many online customers are forced to spend considerable amounts of time navigating through different product categories before finding and selecting their desired product, that information can indicate that the retailer might wish to re-categorize its products or otherwise re-design its website.[4] To carry through the example given above: Based on the information collected from Session Replay Code over the course of many customer website visits, Pet Supplies Plus might choose to display a link to dog "Play and Chew Toys" directly on the home page of its website so that interested consumers can navigate directly to that category of items. Similarly, if a retailer wishes to determine the success of an online promotional pop-up campaign, Session Replay Code can tell that retailer how long it takes for users to notice and respond to those pop-ups, or whether those advertisements are being ignored altogether.[5]

[4] Heap by Contentsquare, *What Is Session Replay & Recording?*, https://www.heap.io/topics/session-replays-recordings (last visited June 13, 2024) ("Watching session replays can give you a good idea of the hindrances and hurdles your customers have to overcome and help you ensure that features of your site function as intended, that the interface is user-friendly, and that content loads ASAP.").

[5] Qualtrics, *Session replay: Definition, benefits & how to use it effectively*, https://www.qualtrics.com/experience-management/customer/session-replay/ (last

Session Replay Code also allows online retailers to identify glitches, bugs, or other problems or inefficiencies on their websites that might negatively affect the customer experience. For example, Session Replay Code can log and identify the following types of user actions that suggest users are experiencing friction on a given webpage:

Rage Clicks: These occur when a user clicks or taps the same area of a website multiple times in quick succession, indicating that a link is either taking too long or not working at all.[6]

Mouse Thrashes: These occur when a user moves their cursor back and forth quickly and erratically, again indicating frustration that something on the website is not working as intended.[7]

Dead Clicks: These occur when a user clicks on parts of a webpage that have no interactive element to them, indicating a misunderstanding of the website's intended design or a missing link.[8]

By identifying those clicks, scrolls, and mouse movements, Session Replay Code helps retailers to redesign their websites or fix problem areas—much as

visited June 13, 2024) ("Using session replay software is a game of spotting missed chances. If you're tracking the success of a specific campaign, for example, you might learn that *** promotional pop-ups are being ignored.").

[6] *Id.*

[7] *Id.*

[8] *Id.*

employees at brick-and-mortar retail locations can observe confused customers, aisles that get overly crowded, or other pressure points in their store, and then work to fix those problems for a smoother shopping experience.

B. NO ACTUAL HARM, MUCH LESS CONSTITUTIONALLY COGNIZABLE INJURY, FLOWS FROM THE ORDINARY USE OF SESSION REPLAY CODE

As the above description of Session Replay Code demonstrates, there is nothing nefarious about the use of this now-commonplace technology. To underscore that point, it is worth understanding several of the inherent limitations of Session Replay Code, which typically prevent collection of private or sensitive information.

First, Session Replay Code does not provide website operators with an actual video or screen recording of a user's website activity.[9] Instead, Session Replay Code logs only certain specific interactions, such as clicks, scrolls, and other mouse movements. *Second*, for similar reasons, Session Replay Code captures information based on the user's own outward interactions with the website. If the user never divulges any private information, Session Replay Code does not extract that information on its own. *Third*, many websites that use Session Replay Code on product pages do *not* use it on pages where individualized information is more likely

[9] *Id.* ("You could be forgiven for thinking that session replay is a video or a screen recording. ***[W]hat you're seeing is a *video-style reconstruction of the user's journey*.").

to be submitted (such as checkout pages). *Finally*, most (if not all) Session Replay Code providers use encryption and masking technology to protect sensitive and private information. For example, any personally identifying information that a customer might input into a website page—such as log-in information—is typically encrypted so that it is accessible only to website operators with a business justification and private encryption key. Similarly, IP addresses are partially encrypted so that they are likewise not typically viewable by the website operator. And for website operators that do use Session Replay Code on pages such as product checkout pages, potentially sensitive information, like credit card numbers, is typically masked (*i.e.*, blocked) entirely and not transmitted to the website operator (or even to the session replay vendor).[10] Indeed, many Session Replay Code products have a "Private by Default" setting that, when enabled, automatically masks all text on certain pages from collection.[11]

Given the reality of how Session Replay Code works, the district court correctly held that the Plaintiff in this case failed to allege any form of cognizable Article III injury caused by the generic use of Session Replay Code. Plaintiff

[10] ECF No. 76-1, Declaration of Doug Camus, ¶¶ 5-11, *In re: BPS Direct, LLC & Cabela's, LLC, Wiretapping*, No. 2:23-md-03074-MAK (E.D. Pa. Nov. 10, 2023).

[11] *See* Fullstory, Inc., *Fullstory Private by Default*, https://help.fullstory.com/hc/en-us/articles/360044349073-Fullstory-Private-by-Default (last visited June 20, 2024).

"alleges only that she 'brow[s]ed for pet supplies' and 'communicated with [Pet Supplies Plus's] website by using her mouse to hover and click on certain products.'" ER-015. Such information "reveals nothing more than the products that interested [Plaintiff] and thus is not the type of private information that the law has historically protected." ER-015. And while Plaintiff speculates that a user's address may be captured "*if* a user enters their address for delivery," ER-037 (emphasis added), she never claims that she actually provided Defendants with any of that information, or that she has any good faith reason to believe the Session Replay Code used on PSP's website operated on any pages with the opportunity to enter a customer address, let alone without masking that potential information.

Far from being an outlier, Plaintiff's complaint and her allegations of harm (or lack thereof) are typical of the mine-run of Session Replay Code lawsuits that are being litigated across the country. For that reason, district courts have repeatedly held that plaintiffs in those lawsuits have failed to allege the types of concrete harm that can qualify as an Article III injury. *See, e.g.*, *Smidga v. Spirit Airlines, Inc.*, No. 2:22-cv-1578-MJH, 2024 WL 1485853, at *5 (W.D. Pa. Apr. 5, 2014) (following the "well-worn paths of other courts around the country that have rejected standing in nearly identical claims" challenging the use of Session Replay Code). For example, in a suit against Bloomingdale's, the district court rightly found that the plaintiff's allegations that the retailer monitored her "mouse movements, clicks, keystrokes, and search terms in real time *** failed to satisfy the injury-in-fact element required for Article III standing." *Jones v. Bloomingdales.com, LLC*, No. 4:22-cv-01095-SEP, 2023 WL 6064845, *1-2 (E.D. Mo. Sept. 18, 2023). In a lawsuit against General Motors, another district court found that plaintiffs failed to "allege that any of their information collected by the Session Replay software was personal or private," and thus failed to allege a constitutionally cognizable injury. *Massie v. General Motors LLC*, No. 21-cv-787-RGA, 2022 WL 534468, at *3 (D. Del. Feb. 17, 2022).

Numerous other examples abound. *See, e.g.*, *Adams v. PSP Grp., LLC*, No. 4:22-cv-1210 RLW, 2023 WL 5951784, at *7 (E.D. Mo. Sept. 13, 2023) ("[I]mportantly, the Complaint does not allege or describe what information Plaintiff provided to Defendant while she was visiting its website. There are no allegations that Plaintiff typed any information about herself, such as her name, address, phone number, or email address into data fields on Defendant's website."); *Thomas v. Papa John's Int'l, Inc.*, No. 22cv2012 DMS (MSB), 2024 WL 2060140, at *4-5 (S.D. Cal. May 8, 2024) (finding "mouse movements, clicks, [and] keystrokes" to be a "far cry from the type of data that supports a finding of a reasonable expectation of privacy"); *see also Mikulsky v. Noom, Inc.*, 682 F. Supp. 3d 855, 864 (S.D. Cal. 2023); *In re BPS Direct LLC, and Cabela's, LLC, Wiretapping*, 2:23-md-03074-MAK, 2023 WL 8458245, at *12-15 (E.D. Pa. Dec. 5, 2023); *Farst v. AutoZone, Inc.*, No. 1:22-cv-

1435, 2023 WL 7179807, at *5 (M.D. Pa. Nov. 1, 2023); *Cook v. GameStop, Inc.*, 689 F. Supp. 3d 58, 65-67 (W.D. Pa. 2023).

As those district courts have also recognized, the Supreme Court's teachings from *TransUnion* further underscore the inherent Article III deficiency in the typical Session Replay Code lawsuit. The central holding of *TransUnion* is that a bare statutory violation alone is insufficient to demonstrate Article III injury in fact because the focus of the standing inquiry must be "whether plaintiffs have identified a close historical or common-law analogue for their asserted injury." 594 U.S. at 424; *Perry v. Newsom*, 18 F.4th 622, 632 (9th Cir. 2021) (further emphasizing that plaintiff must find "[a]n analogy to a traditionally recognized cause of action" *and* corresponding "injury"). To that question, plaintiffs across the country have consistently failed to identify any such injury, given the way Session Replay Code typically works. *See, e.g.*, *Cook*, 689 F. Supp. 3d at 64 (noting that plaintiff's reliance on a bare statutory violation "runs directly counter to the Supreme Court's clarification" in *TransUnion*). Instead, the most plaintiffs have mustered is to equate the recording of clicks, scrolls, and cursor movements to traditional common-law torts such as "invasion of privacy" or "intrusion upon seclusion." ER-009. But district courts have time and again rejected such false equivalencies, holding that clicks, scrolls, and cursor movements captured by Session Replay Code are not the sorts of "sensitive, personal, or confidential information" that those traditional torts protect. *See, e.g.*, *Adams*, 2023 WL 5951784, at *7-8; *In re BPS Direct, LLC*, 2023 WL 8458245, at *12. And they have properly, and repeatedly, dismissed invasion of privacy and intrusion upon seclusion claims premised on the use of Session Replay Code. *See, e.g.*, *Thomas*, 2024 WL 2060140, at *4-5; *see also Mikulsky v. Bloomingdale's, LLC*, --- F. Supp. 3d ---, 2024 WL 337180, at *8 (S.D. Cal. Jan. 25, 2024); *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 524-525 (C.D. Cal. 2021).

Instead, putting plaintiffs' "rhetoric" of surveillance and wiretapping aside and viewing their allegations in the proper light, courts have found that a website's use of Session Replay Code is best analogized to the commonplace retailer practice of observing customer movements in brick-and-mortar shops. *See, e.g.*, *In re BPS Direct, LLC*, 2023 WL 8458245, at *1, *12; *see also Cook*, 689 F. Supp. 3d at 66; *Farst*, 2023 WL 7179807, at *5. In particular, a customer's "physical movements in the store are like her mouse movements, her pauses to look at the inventory are like her mouse pointed hovering over products, and her picking up [desired products] off the shelf are [sic] like placing those same [products] in her virtual cart." *Cook*, 689 F. Supp. 3d at 66. Because customers "certainly d[on't] have a reasonable expectation of privacy in this kind of public shopping behavior in the physical world," they "d[on't] have it in the digital world, either." *Id.* And because there is no close historical recognition for any injury flowing from being observed and assisted by sales-floor employees when a potential customer voluntarily chooses to enter a brick-and-mortar store, plaintiffs challenging the generic use of Session Replay Code simply cannot, without more, establish any Article III injury.

C. A CLEAR RULE IS NEEDED TO MANAGE THE ONGOING WAVE OF SESSION REPLAY CODE LAWSUITS

Despite the fundamental Article III deficiencies with Plaintiff's case and the many others like hers, online retailers and other website operators have nevertheless had to defend themselves against a barrage of lawsuits challenging the common use of Session Replay Code. As a subset of an even wider onslaught of lawsuits challenging website analytical tools in general (of which "five to ten" new cases are "filed per week"[12]), there have now been more than one hundred federal putative class-action lawsuits filed over the past two years, often by the same plaintiffs and/or plaintiffs' counsel, asserting various federal and state claims against online retailers based on the use of Session Replay Code.

Apart from a consistent failure to identify any cognizable Article III injury, another common feature of these lawsuits is an attempt by putative class-action plaintiffs (or perhaps more accurately, the class-action plaintiffs' bar) to pursue lawsuits on behalf of extremely broad classes. Below are a few examples:

[12] NetDiligence, *3 Key Takeaways: Website Tracking Tech as a Liability Risk* (Feb. 14, 2023), https://netdiligence.com/blog/2023/02/what-is-meta-pixel/.

Case	Jurisdiction	Proposed Class Definition
Schnur v. Papa John's Int'l, Inc., No. 2:22-cv-1620	W.D. Pa.	"All natural persons in Pennsylvania whose Website Communications were captured in Pennsylvania through the use of Session Replay Code embedded in www.papajohns.com."
Cook v. Gamestop, Inc., No. 22-cv-01292	W.D. Pa.	"All natural persons in Pennsylvania whose Website Communications were captured through the use of Session Replay Code embedded in www.gamestop.com."
Calvert v. Cabela's, Inc., No. 22-cv-1460	W.D. Pa.	"All natural persons in Pennsylvania whose Website Communications were captured in Pennsylvania through the use of Session Replay Code embedded in www.cabelas.com."
Calvert v. Tru Value Co., No, 22-cv-1461	W.D. Pa.	"All natural persons in Pennsylvania whose Website Communications were captured in Pennsylvania through the use of Session Replay Code embedded in www.truevalue.com."
Perkins v. Zillow Grp., No. 2:22-cv-1282	W.D. Wash.	"[A]ll natural persons in the United States and its territories whose Website Communications were intercepted through the use of Session Replay Code embedded in www.zillow.com."
Adams v. Zillow Grp. Inc., No. 22-cv-1737	W.D. Wash.	"[A]ll Missouri citizens whose Website Communications were intercepted at Zillow's direction and use of Session Replay Code embedded on the webpages of www.zillow.com[.]"
Margulis v. Zillow Grp. Inc., No. 22-cv-1736	W.D. Wash.	"[A]ll Illinois citizens whose Website Communications were intercepted at Zillow's direction and use of Session Replay Code embedded on the webpages of www.zillow.com[.]"

Case	Jurisdiction	Proposed Class Definition
Popa v. Zillow Grp. Inc., No. 22-cv-1696	W.D. Wash.	"[A]ll Pennsylvania citizens whose Website Communications were intercepted through Zillow's procurement and use of Session Replay Code embedded on the webpages of www.zillow.com[.]"
Jones v. Bloomingdales.com, LLC, No. 22-cv-01095	E.D. Mo.	"All natural persons in the United States whose Electronic Communications were intercepted through Defendant's procurement and use of session replay technology embedded in www.bloomingdales.com."
Alves v. Goodyear Tire and Rubber Co., No. 22-cv-11820	D. Mass.	"All natural persons in Massachusetts whose Website Communications were captured in Massachusetts through the use of Session Replay Code embedded in www.goodyear.com."
Montecalvo v. Cabela's Inc., No. 22-cv-11837	D. Mass.	"All natural persons in Massachusetts whose Website Communications were captured in Massachusetts through the use of Session Replay Code embedded in www.cabelas.com."
Curd v. Spirit Airlines, No. 22-cv-03174	D. Md.	"All natural persons in Maryland whose Website Communications were captured in Maryland through the use of Session Replay Code embedded in www.spirit.com."
Curd v. Papa John's Int'l, Inc., No. 22-cv-03185	D. Md.	"All natural persons in Maryland whose Website Communications were captured in Maryland through the use of Session Replay Code embedded in www.papajohns.com."
Thomas v. Papa John's Int'l, Inc., No 22-cv-02012	S.D. Cal.	"All natural persons in California whose Website Communications were captured in California through the use of Session Replay Code embedded in www.papajohns.com."

Case	Jurisdiction	Proposed Class Definition
Price v. Carnival Corp., No. 23-cv-00236	S.D. Cal.	"All natural persons in the United States whose Website Communications were captured in the United States through the use of Session Replay Code embedded in www.carnival.com."
Mandeng v. Spirit Airlines, Inc., No. 23-cv-00233	S.D. Cal.	"All natural persons in California whose Website Communications were captured in California through the use of Session Replay Code embedded in www.spirit.com."
Matousek v. Noom, Inc., No. 23-cv-01639	C.D. Cal.	"All natural persons in California whose Website Communications were captured in California through the use of Session Reply Code embedded in www.noom.com."
Toston v. Jet Blue Airways Corp., No. 23-cv-01156	C.D. Cal.	"All natural persons in California whose Website Communications were captured in California through the use of Session Replay Code embedded in www.JetBlue.com."
Posadas v. Goodyear Tire & Rubber Co., 23-cv-00402	S.D. Cal.	"All natural persons in California whose Website Communications were captured through the use of Session Replay Code embedded in www.goodyear.com."

As these examples demonstrate, plaintiffs in Session Replay Code lawsuits typically attempt to represent broad classes encompassing *any* individuals who have visited a given defendant's website. This is regardless of any differences in individual customer behavior, such as purchasing behavior, browsing history, or the kinds of information voluntarily provided in the course of a particular website interaction, and whether the Session Replay Code collected or masked particular information. Thus, while plaintiffs' complaints often make the generic allegation that Session Replay Code *may* capture certain forms of information like addresses, *if* an individual types that information into the website, *see, e.g.*, ER-037, the scope of the proposed classes is often untethered from that specific kind of user behavior. *See also Straubmuller v. Jetblue Airways Corp.*, No. DKC 23-384, 2023 WL 5671615, at *4 (D. Md. Sept. 1, 2023) ("[I]t is dispositive that Plaintiff only alleges that Session Replay Code *could* capture personal information, not that it actually captured Plaintiff's personal information."); *Cook*, 689 F. Supp. 3d at 69 ("It's not enough for [Plaintiff] to allege the potential capabilities of Session Replay Code. Rather, she needed to allege that [Defendant], in fact, harnessed the capabilities she describes, and it had the result of capturing the contents of specific communications. But she did not do that."). But specificity is exactly what is needed for courts to adequately determine standing to represent a putative class.

Plaintiffs' generic allegations are designed to obscure the fact that Session Replay Code vendors typically design their technology to shield or mask any sensitive information.[13] Accordingly, even if it is theoretically possible to hypothesize scenarios in which an individual user might submit private information

[13] *See, e.g.*, Qualtrics, *Session replay: Definition, benefits and how to use it effectively*, *supra* note 5 ("Most modern suites can actively guard against capturing personally identifiable information[.]"); Heap by Contentsquare, *What Is Session Replay & Recording?*, *supra* note 4 ("A Session Replay is private and secure by default. [Personally Identifiable Information] data is not collected, and if it is part of a given workflow, [it] is masked.").

that is captured by Session Replay Code, Session Replay Code lawsuits typically lack such particularized allegations.

The pattern of Session Replay Code class-action lawsuits has imposed significant harm on retailers, notwithstanding the difficulties plaintiffs have experienced in filing successful claims. In the majority of cases, plaintiffs seek statutory penalties, calculated on a per-violation basis, based on entirely novel applications of state "wiretapping" statutes enacted well before the development of online retail opportunities. *See, e.g.*, ER-048 (seeking, in addition to other relief, damages under the Pennsylvania Wiretap Act for each class member "at the rate of $100/day for each violation or $1,000, whichever is higher"); Complaint at 21, *Alves v. Goodyear Tire and Rubber Co.*, 683 F. Supp. 3d 111 (D. Mass. 2023) (No. 1:22-cv-11820-WGY), ECF No. 1 (seeking same class-wide damages under the Massachusetts Wiretap Statute); First Amended Complaint at 29, *Price v. Carnival Corp.*, No. 3:23-cv-00236-GPC-MSB, 2024 WL 221437 (S.D. Cal. Jan. 19, 2024), ECF No. 22 (seeking class-wide damages of at least "$5,000 per violation" of the California Invasion of Privacy Act). Those penalties, when multiplied across the broad putative classes plaintiffs typically purport to represent, result in suits threatening millions of dollars in alleged penalties and damages based on nothing more than technology that facilitates website maintenance and design.

Retailers across the country are put to an untenable choice: They must either incur costly responsive measures to these suits or instead opt for early settlement to avoid the financial burden of defense. When early cost-avoidance settlements do occur, those cases never benefit from a judge's independent "responsibility" to ensure that plaintiffs have properly invoked Article III jurisdiction. *TransUnion*, 594 U.S. at 426; *see also Nuclear Info. & Res. Serv. v. Nuclear Regul. Comm'n*, 457 F.3d 941, 949 (9th Cir. 2006) ("As the Supreme Court has recently reiterated, 'we have an obligation to assure ourselves of litigants' standing.'") (quoting *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 340 (2006) (additional citation and alterations omitted)).

Given this context, this Court should issue a clear rule that allows lower courts to efficiently manage the numerous Session Replay Code lawsuits that continue to proliferate across the country. While the district courts that have had the opportunity to address threshold Article III issues have overwhelmingly come to the right conclusion, *supra* pp. 9-11, many of those decisions are now the subject of pending appeals and there remains a dearth of appellate authority on this subject. *See, e.g.*, *Cook v. GameStop, Inc.*, 689 F. Supp. 3d 58 (W.D. Pa. 2023), *appeal pending* (3d Cir. No. 23-2574); *Adams v. PSP Group LLC*, No. 4:22-cv-1210 RLW, 2023 WL 5951784 (E.D. Mo. Sept. 13, 2023), *appeal pending* (8th Cir. Nos. 23-3303, 23-3304, 23-3606).

Clear appellate guidance would be especially valuable in this Circuit, where plaintiffs have insisted on relying on outdated pre-*TransUnion* caselaw to circumvent *TransUnion*'s central teachings and muddy the Article III standing inquiry. ER-015–016 (correctly holding that *TransUnion*'s clear instructions supersede contrary pre-*TransUnion* Circuit authority). That guidance is sorely needed, not only by defendants seeking to assess their risks but also by district courts seeking to navigate Session Replay Code cases while remaining faithful to *TransUnion*. Indeed, at least one district court in this Circuit has formally stayed proceedings in a consolidated set of Session Replay Code lawsuits, holding that "there is a significant possibility that the Ninth Circuit's decision in [this] appeal will simplify the issues and questions of law in this matter and further the orderly course of justice." *In re Zillow Grp., Inc. Session Replay Software Litig.*, No. C22-1282JLR, 2024 WL 69732, at *2 (W.D. Wash. Jan. 5, 2024).

To that end, this Court should affirm the rule applied by the district court below—and other courts throughout the country—which requires plaintiffs to identify an actual and particularized injury flowing from the use of Session Replay Code. Under that rule, a plaintiff must specifically allege, and then prove, that their private experience with Session Replay Code—beyond the generic collection of unspecified clicks, scrolls, and mouse movements—resulted in harm comparable to that recognized through "historically protected privacy interests." ER-017; *see also*

Cook, 689 F. Supp. 3d at 65 (requiring the public disclosure of "private facts or private affairs"). Absent such harm, mere allegations that a given website employs Session Replay Code cannot satisfy a plaintiff's Article III burden.

This rule—which accurately captures the basic premise that the use of Session Replay Code is not *per se* harmful—would help district courts guard against the potential circumvention of the demands of Article III. It would also prevent abuse of the class action device by clarifying that plaintiffs cannot proceed on behalf of an overbroad class of *all* website users without any meaningful attempt to identify those actually injured (if any) by the use of Session Replay Code.

CONCLUSION

This Court should affirm the judgment of the district court.

Dated: June 21, 2024

Respectfully submitted,

/s/ *Aileen M. McGrath*

Aileen M. McGrath
Zach ZhenHe Tan
AKIN GUMP STRAUSS HAUER & FELD LLP
100 Pine Street, Suite 3200
San Francisco, CA 94111

Deborah R. White
Larissa M. Whittingham
RETAIL LITIGATION CENTER, INC.
99 M Street SE, Suite 700
Washington, DC 20003

Attorneys for Amicus Curiae
Retail Litigation Center

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the length limits permitted by Federal Rule of Appellate Procedure 29(a)(5) and Ninth Circuit Rule 32-1. The brief is 5,062 words, excluding the portions exempted by Federal Rule of Appellate Procedure 32(f) and Ninth Circuit Rule 32-1(c). The brief's type size and type face comply with Federal Rule of Appellate Procedure 32(a)(5) and (6) and Ninth Circuit Rule 32-1(d).

Dated: June 21, 2024

/s/ *Aileen M. McGrath*
Aileen M. McGrath