No. 20-297

IN THE

Supreme Court of the United States

TRANS UNION LLC,

Petitioner,

v.

SERGIO L. RAMIREZ,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF RESPONDENT

Cindy A. Cohn
Adam Schwartz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
adam@eff.org

James Pizzirusso
Counsel of Record
Michael D. Hausfeld
Ian Engdahl
HAUSFELD LLP
888 16th Street, N.W.
Suite 300
Washington, DC 20006
(202) 540-7200
jpizzirusso@hausfeld.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Regulations

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

Amicus curiae the Electronic Frontier Foundation (EFF) is a nonprofit organization that works to ensure that technology supports freedom, justice, and innovation for all the people of the world. *See generally* https://www.eff.org/. *Amicus* was founded in 1990 and has more than 35,000 members. It advocates before courts and legislatures to protect the privacy of technology users and consumers from corporations that collect and monetize their personal information. EFF filed an *amicus* brief with this Court in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), and in numerous other cases that apply constitutional doctrine to emerging technologies. *See, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017); *City of Ontario v. Quon*, 560 U.S. 746 (2010).

INTRODUCTION AND SUMMARY OF ARGUMENT

In 1997, the computer scientist Michael Lesk set out to estimate the amount of data that would be required to store the millions of books, photographs, films, and sound recordings that made up the Library of Congress' collection. Michael Lesk, *How Much Information Is There in the World?* (1997),

---

[1] Pursuant to Rule 37.6, *amicus* affirms that no counsel for a party authored this brief in whole or in part and that no person other than *amicus* and its counsel made a monetary contribution to its preparation or submission. The parties' letters consenting to the filing of this brief have been filed with the Clerk.

https://perma.cc/XUG4-UDU3. He estimated that, all told, the entire collection would amount to approximately three million gigabytes of data.

Today, a single company—Facebook—captures and stores more than three million gigabytes of data about its users *every day*. *See* Janet Wiener & Nathan Bronson, *Facebook's Top Open Data Problems*, Facebook Research Blog (Oct. 22, 2014), https://perma.cc/Z79N-7YDT. The vast data collected by companies such as *amici* Google and Facebook can be used to reveal a user's most intimate and sensitive personal information and secrets, including their religious beliefs, mental health struggles, or sexual identity and activity. *See* EFF, *Behind the One-Way Mirror: A Deep Dive into the Technology of Corporate Surveillance* 5 (2019), https://www.eff.org/wp/behind-the-one-way-mirror.

Just as the information collected about consumers is expanding at an unprecedented rate, so too are the risks associated with the unfettered assembly of such data. As more and more facets of daily life depend on the data collected in vast corporate databases, mistakes in this data can have serious consequences for many consumers. For example, such errors can have a significant influence on the prices we are charged, the homes we can rent or buy, the mortgages we can qualify for, the romantic partners we are matched with, and the jobs we can get. Incorrect data can even create the risk of an erroneous adverse immigration action. *See* Drew Harwell, *ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations*, Wash. Post (Feb. 26, 2021), http://wapo.st/2OCVwCE. Behind the scenes, the data collected about us is being used constantly,

often in ways that we do not even see or recognize. Yet ultimately, all Americans depend on the accuracy of this information, whether we realize it or not.

A company that undertakes to aggregate, store, use, and disseminate users' sensitive personal data also takes on a grave responsibility. When data about a consumer is wrong, misused, or unprotected, that consumer faces real-world, concrete harms. Whether these harms manifest in ways that are tangible, as they did for Mr. Ramirez here, or remain intangible, as they did for others in the class, they are sufficient to confer Article III standing. These shared harms also are sufficient to satisfy the "typicality" element of Rule 23 of the Federal Rules of Civil Procedure.

In the shadow of this unprecedented growth in consumer data gathering and the potential harms stemming from these practices, TransUnion and *amici* Facebook and Google ("Big Tech *Amici*")[2] lead a frontal attack on Article III and Rule 23. If accepted, this constrained view of standing and class-action doctrine would hamstring consumers' ability to hold companies accountable for the injuries caused by companies' failures to properly handle consumers' sensitive data.

When personal data is incorrect or mishandled, the injuries suffered by consumers may be hard to quantify, but they are no less concrete than other harms such as those caused by defamation and other

---

[2] *See* Brief for *Amici Curiae* eBay, Inc., Facebook, Inc., Google LLC, Computer & Communications Industry Association, the Internet Association, and Technology Network Supporting Petitioner.

longstanding torts. This Court has long recognized that certain intangible or hard to quantify harms are sufficient to confer Article III standing. *See Spokeo v. Robins*, 136 S. Ct. 1540, 1549 (2016). Recognition of these harms is even more vital today as the depth and breadth of information gathered about every consumer—and the potential for concrete harm stemming from errors in such data—grows by the day.

The harms suffered by class members in this case demonstrate the critical importance of Congress' role in identifying and elevating such harms. Every member of the class had a damaging "OFAC alert" listed on their credit file identifying them as a potential "terrorist," and TransUnion made this damaging and erroneous information available to a vast number of creditors at a moment's notice. This placed all class members at grave and immediate risk of financial injury and social stigma. Further, the disclosures that TransUnion sent to class members failed to comply with the clear mandates of the Fair Credit Reporting Act (FCRA), thus exacerbating the harm and making it harder for class members to understand how to correct the false information on their credit file. The FCRA reflects Congress' sound judgment that the harms inflicted by such egregious errors—and the real risks they create—give rise to cognizable injuries sufficient to establish Article III standing.

The cases cited by the Big Tech *Amici* further reinforce the importance of protecting consumers from privacy and data misuse harms in the digital age. The Big Tech *Amici* attack holdings granting plaintiffs standing under a range of state and federal data-privacy laws such as the Illinois Biometric

Information Privacy Act. These laws reflect states' judgments that consumers are harmed when their sensitive data is mishandled. Because these harms, while concrete, may be difficult to prove or measure, the states and Congress can provide statutory damages that compensate consumers for these injuries and thereby incentivize corporations to avoid imposing the harms that these statutes seek to prevent.

Because these concrete harms affect many individuals and are significant in the aggregate, Rule 23 also provides an essential tool that enables classes of consumers to vindicate their legally protected interests. While the claims and defenses of a class representative must be "typical" of the class, Rule 23 does not require perfect uniformity. That is particularly so where, as here, statutory damages eliminate the burden of individualized injury determinations. It is the statutory violation itself that must be typical among class members in such a Rule 23 class action, not the actual manifestation of the injury resulting from the violation.

ARGUMENT

I. The unprecedented rise in the collection and use of sensitive personal information puts consumers at increased risk of suffering significant harms.

An increasing share of American life is now experienced online. Americans use the products and services of Internet giants such as Facebook and Google for the most mundane to the most intimate and sensitive parts of daily life. Americans increasingly rely on online services to socialize with

friends, discover new romantic partners, debate the issues of the day, or practice their faith. While this sea-change in the way many people live their lives has many benefits, it is also fraught with unique risks.

Many of the companies that provide these online services gather a previously unimaginable amount of data from consumers. Some of the world's largest companies—including *amici* Facebook and Google—gather and use this data to build detailed profiles of consumers that give these companies and their business partners uncanny insight into the thoughts, aspirations, and desires of their users. *See* EFF, *Behind the One-Way Mirror* 5–6 (2019).

Credit reporting agencies such as TransUnion also gather an increasing amount of data on consumers. Federal studies show that the data collected by such agencies are frequently materially inaccurate. A recent FTC report on the accuracy of consumer credit reports found that 26% of consumers have at least one potentially material error on their credit file. Fed. Trade Comm., *Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003* (Jan. 2015). Consumer Financial Protection Bureau data show that consumer complaints regarding credit reports more than doubled in 2020. Ann Carrns, *More Consumers Complain About Errors on Their Credit Reports*, N.Y. Times (Feb. 19, 2021), http://nyti.ms/3cdqqcL.

These common errors can have dire consequences for consumers. Consumers with errors on their credit reports face difficulties getting hired and verifying their identities, and they pay higher interest rates and higher insurance costs. Consumers

Union, *Errors and Gotchas: How Credit Report Errors and Unreliable Credit Scores Hurt Consumers* 18–22 (2014). For many Americans, inaccuracies on their credit reports put nothing less than the American dream at risk.

II. Robust recognition of the harms caused by the mishandling of personal information is consistent with this Court's Article III jurisprudence.

The unprecedented aggregation of vast quantities of consumer data puts consumers at increased risk of real-world harms. When consumers' sensitive data is misused, unprotected, or inaccurate, consumers face concrete harms sufficient to confer Article III standing. While these harms may be hard to quantify, they are no less genuine than traditional harms from long-recognized torts such as defamation.

Accordingly, this Court has long recognized that certain intangible harms are sufficient to confer Article III standing. *See Spokeo*, 136 S. Ct. at 1549. Congress plays a critical role in "identifying and elevating" harms that were previously inadequate to confer Article III standing. *Id.* Congress' power to identify legally cognizable harms is particularly important where "harms may be difficult to prove or measure." *Id.* By identifying a "risk of real harm" and providing a statutory remedy, *id.*, Congress may "define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before," *id.* (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring in part and concurring in judgment)).

Recognition of such harms is more vital than ever before, as the depth and breadth of information gathered about every consumer—and the potential for concrete harm flowing from data collection, errors, and mishandling—grows daily. This unprecedented rise in the aggregation of sensitive data has led to a commensurate rise in harms suffered by consumers.

The FCRA is a key component of Congress' statutory privacy protection regime, establishing safeguards against privacy harms like those suffered by the class members here. Long before the modern era of data aggregation and the Internet, Congress anticipated that "with the trend toward . . . the establishment of all sorts of computerized data banks, the individual is in great danger of having his life and character reduced to impersonal 'blips' and key-punch holes in a stolid and unthinking machine which can literally ruin his reputation without cause." *Dalton v. Capital Associated Industries*, 257 F.3d 409, 414 (4th Cir. 2001) (quoting 116 Cong. Rec. 36570 (1970) (statement of Rep. Sullivan)). Congress addressed these concerns by enacting statutory provisions intended "to prevent consumers from being unjustly damaged because of inaccurate or arbitrary information in a credit report." *Cortez v. Trans Union, LLC*, 617 F.3d 688, 706 (3d Cir. 2010) (quoting S. Rep. No. 91–517, at 1 (1969)).

Congress has also identified and elevated similar harms in other privacy statutes that have gained renewed importance in the digital age. The Video Privacy Protection Act, 18 U.S.C. § 2710 *et seq.*, for instance, prohibits the unauthorized disclosure of a consumer's video viewing history. *See Eichenberger v ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017).

Likewise, the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, prohibits the intentional interception, use, or disclosure of the contents of telephone or digital network communications. These statutory privacy protections reflect Congress' critical role in identifying and elevating privacy harms for the purposes of standing.

But harms need not be recognized by Congressional edict to be sufficient for Article III standing. For example, courts have increasingly recognized that consumers whose sensitive personal information is exfiltrated in a data breach have suffered—or are at imminent risk of suffering—concrete and particularized injuries sufficient to confer Article III standing. *See In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 56 (D.C. Cir. 2019). The recognition of such harms is critical to protect consumers and their sensitive data from negligent cybersecurity practices and emerging threats to the privacy and integrity of their data. In recent years there has been a marked increase in both the number and severity of data breaches, due in no small part to the vast expansion in the collection of sensitive user data. From 2015 to 2019, for example, the data-breach losses reported to the FBI more than tripled, reaching $3.5 billion in 2019. Fed. Bureau of Investigation, 2019 Internet Crime Report 5 (2020).

III. The class members here have established Article III standing.

The class members in this case suffered exactly the sort of privacy harms that Congress recognized as cognizable Article III injuries and sought to prevent with the FCRA. In stark contrast to the

"incorrect zip code" that the Court viewed as insufficient to confer standing without a showing of additional injury, *Spokeo*, 136 S. Ct. at 1550, the class members here were all misidentified as potential terrorists.

It is difficult to conceive of a more harmful and distressing error than being falsely labeled as a person who uses physical violence against other people to achieve political or social objectives. Further, the Office of Foreign Asset Control (OFAC) list is "designed to deprive the target of the use of its assets and to deny it access to the U.S. financial system and the benefits of trade, transactions, and services involving U.S. markets, businesses, and individuals." Economic Sanctions Enforcement Guidelines, 74 Fed. Reg. 57,594 (Nov. 9, 2009).

Compounding this error and causing the class members further harm, the letters from TransUnion notifying the class members of their status as potential terrorists were misleading and failed to include the summary of rights mandated by the FCRA. That summary would have informed class members of their right to dispute the incorrect designation. Instead, class members were left with an incorrect terrorist designation and no clear way to address TransUnion's dangerous mistake.

TransUnion's attempt to downplay this statutory violation as simply a matter of "two envelopes instead of one," Pet. Br. at 20, ignores that this is precisely the harm that the FCRA's summary-of-rights requirements were intended to prevent: A material, dangerous error with no clear means of redress. The FCRA reflects Congress' judgment that the harms inflicted by such damaging errors, paired

with failures to comply with the statute's clear mandates, are cognizable injuries.

These harms are closely tied to a common-law analogue that has traditionally been sufficient to confer standing. In the context of defamation *per se*, courts have long recognized that the mere publication of certain damaging and inaccurate information gives rise to legally cognizable injuries, even in the absence of additional harms. The publication of libel "incompatible with the proper exercise of [an individual's] lawful business, trade, profession, or office" is actionable *per se*, regardless of whether any special harm was caused to the plaintiff because the "publication is itself an injury." Restatement (First) of Torts § 569 (1938). Publication encompasses a wide range of intentional or negligent communications. Restatement (Second) of Torts § 577 (1977). In the context of libel, publication includes communication to an agent of the defamer, a telegraph company employee reading the defamatory statement transmitted through telegram, communication between employees of the defamer, and even dictation to a stenographer. *Id.* comments e–i.

For defamation *per se*, "an action on the case may be had, without proving any particular damage to have happened, but merely upon the probability that it may happen." 3 William Blackstone, *Commentaries on the Laws of England* 124 (1769). Congress recognized that the FCRA was designed to protect consumers from these traditional common-law harms by explicitly preempting state-law claims based on defamation, invasion of privacy, and negligence in many cases. 15 U.S.C. 1681h(e).

As the Court explained in *Spokeo*, "the law has long permitted recovery" for such tort victims, "even if their harms may be difficult to prove or measure." 136 S. Ct. at 1549. Just as the common law permitted suit in such instances without proof of further injury, "a plaintiff in such a case need not allege any *additional* harm beyond the one Congress has identified." *Id.* By creating statutory requirements in the FCRA designed to protect consumers from the harms drawn from this common-law-defamation lineage, Congress identified these harms as sufficient to confer Article III standing, even without proof of additional harm.

While there may be some cases where an innocuous mistake would not cause a consumer harm or present a risk of real harm, *Spokeo*, 136 S. Ct. at 1550, the error here was no mere incorrect zip code. Here too, the common law is instructive. While traditional defamation required a showing of additional harm from certain incorrect and defamatory statements, the doctrine of defamation *per se* recognized that certain categories of errors were so significant and so likely to cause harm that injury was presumed.

These cognizable harms were suffered by class members regardless of whether their credit report was ever requested by a third party. A consumer may put off buying a car or a home for fear that the error will lead to denial of credit. Mr. Ramirez decided not to travel internationally out of fear of the error. Likewise, a consumer may avoid applying for a new job based on the reasonable fear that they may not only fail to get hired, but may also suffer irreparable reputational harm in their chosen field. Even if they never intend to seek an economic opportunity that

might ordinarily lead to a credit check, a consumer could reasonably fear that their false identification as a terrorist could lead to unanticipated and unknowable future injuries at any moment.

Because significant and damaging errors on credit reports predictably cause such concrete harms, Congress sought through the FCRA to prevent such harms and provide a mechanism for consumers to seek redress. While Congress provided a safe harbor for consumer reporting agencies that comply with the requirements of the statute, TransUnion lost that protection by violating the FCRA's clear mandates. The harm Congress sought to identify and prevent materialized as soon as TransUnion placed the damaging OFAC error on each class member's credit file. When TransUnion failed to comply with the FCRA's statutory requirements, the cause of action accrued, and the Article III injury was complete.

Even if these concrete harms themselves were not enough to confer standing, each class member also faced a significant risk of harm from the presence of this damaging error on their credit file. This "material risk of harm," *Spokeo*, 136 S. Ct. at 1550, was experienced by all class members and was sufficient to establish Article III standing.

The risks to class members were substantial and immediate. A credit file exists to be distributed to third parties at a moment's notice. A person wrongly identified as a potential terrorist, with whom no domestic entity can lawfully do business, is at imminent risk that TransUnion's systems will do exactly what they were designed to do: distribute this information instantaneously to third parties that will use it to make critical credit or employment decisions

about that consumer. Consumers have only limited control over the distribution of their credit file, and in some circumstances third parties can even access credit reports without consumers' knowledge. The FCRA reflects Congress' judgment that the real risk of harm from such damaging and inaccurate information on credit reports is sufficient to confer Article III standing when credit agencies fail to follow the requirements of the statute. Such a "real risk of harm" satisfies Article III. *Spokeo*, 136 S. Ct. at 1549.

Petitioner incorrectly argues that under *Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013), future injury must be "certainly impending" to satisfy Article III. In fact, the Court in *Clapper* acknowledged that standing does not always "require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about." *Id.* at 414 n.5. Rather, a "substantial risk" of harm can be sufficient to confer Article III standing. *Id.* Thus, the year after *Clapper*, this Court held that an "allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper*, 568 U.S. at 409, 414 n.5). And this Court held in *Spokeo*, 136 S. Ct. at 1549, that "the risk of real harm" can satisfy Article III, citing to *Clapper*.

The class members also suffered cognizable informational injuries when TransUnion failed to include the summary-of-rights disclosures required by the FCRA. When Congress requires the disclosure of information, plaintiffs may suffer harms sufficient to confer Article III standing when a party fails to

provide that information in compliance with the statute. *See Spokeo*, 136 S. Ct. at 1549 (citing *Federal Election Comm'n v. Akins*, 524 U.S. 11, 20-25 (1998); *Public Citizen v. Department of Justice*, 491 U.S. 440, 449 (1989)).

That is particularly so where, as here, Congress' statutory scheme employs mandated disclosures as a key prophylactic measure against the harms the statute seeks to prevent. Applying this principle to the FCRA, courts have concluded that plaintiffs suffer cognizable informational injuries when a party fails to comply with the Act's disclosure provisions. *See Syed v. M-I, LLC*, 853 F.3d 492, 499 (9th Cir. 2017). Particularly when paired with such a significant and damaging error, TransUnion's failure to comply with the disclosure provisions of the FCRA caused the class members to suffer a concrete injury sufficient to confer Article III standing.

IV. The outcome of this case will have serious implications for the recognition of harms caused by the unprecedented rise in the collection and use of sensitive user data.

The Big Tech *Amici* urge this Court to go beyond the context of this case and adopt a confined view of Article III standing and Rule 23 typicality that would hamstring consumers' ability to protect their sensitive data and hold data aggregators like the Big Tech *Amici* accountable. The Court should decline the invitation to undercut years of standing and Rule 23 jurisprudence, particularly at a time when consumers are facing emerging threats to their sensitive personal data as it is being tracked, stored, shared, and used in unprecedented ways.

The Big Tech *Amici* complain that in a host of cases, courts have denied motions to dismiss or found them liable for violations of state and federal statutes enacted to protect consumers against harms to their privacy interests. Much of their brief attempts to relitigate holdings against them in their own cases—even some where this Court has already denied *certiorari*. Big Tech *Amici* Br. at 14–17.

It should be no surprise that laws designed to protect sensitive personal data have strong application to these tech giants. The Big Tech *Amici* are at the vanguard of the trend toward the mass aggregation and use of consumer data. They are industry-leading innovators in finding new, boundary-defying methods of gathering and exploiting sensitive consumer data. The cases being filed against Big Tech *Amici* are not a mere coincidence, or a concerted effort by the plaintiffs' bar to extract "*in terrorem*" settlements out of them. Rather, they are a recognition by courts that Big Tech *Amici*'s collection and use of consumers' sensitive data often causes concrete harms to consumers.

In *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020), for instance, plaintiffs sued *amicus* Facebook, alleging that its use of face recognition technology violated Illinois' Biometric Information Privacy Act (BIPA). In recent years, many states have enacted privacy laws, such as BIPA, that identify certain types of data as particularly sensitive and provide consumers with statutory rights to protect their information from those harms. BIPA regulates the "collection, use, safeguarding, and storage of biometrics," including scans of hands or face geometry, and imposes various

obligations on private entities regarding the collection, retention, use, and destruction of such information. *Id.* at 1268–69 (citing 740 Ill. Comp. Stat. 14/1 *et seq*.). *See also Amicus* Br. of EFF *et al.*, *Patel v. Facebook, Inc.*, No. 18-15982 (9th Cir. Dec. 17, 2018).

The plaintiffs challenged Facebook's practice of collecting faceprints from its users, and storing those faceprints, without the opt-in consent required by BIPA. Finding that the statute had its roots in common-law privacy rights and considering the "Supreme Court's views regarding enhanced technological intrusions on the right to privacy," the Ninth Circuit concluded that "an invasion of an individual's biometric privacy rights 'has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit.'" *Patel*, 932 F.3d at 1273 (quoting *Spokeo*, 136 S. Ct. at 1549). As the Ninth Circuit stressed, "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." *Id.* (quoting *U.S. Dep't of Just. v. Reps. Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989)).

Drawing insight from this Court's Fourth Amendment jurisprudence, the Ninth Circuit found that the face recognition technology at issue could "obtain information that is 'detailed, encyclopedic, and effortlessly compiled,' which would be almost impossible without such technology." *Id.* (quoting *Carpenter v. United States*, 138 S. Ct. 2206, 2216 (2018)). As such, the Ninth Circuit held that BIPA protects consumers' concrete privacy interests and that Facebook's conduct presented a material risk of harm to these interests. *Id.* at 1274. Accordingly, the

court concluded that the plaintiffs had Article III standing. *Id.* This Court subsequently denied Facebook's petition for *certiorari*. *Facebook, Inc. v. Patel*, 140 S. Ct. 937 (2020).

Likewise, in *Campbell v. Facebook, Inc.*, 951 F.3d 1106 (9th Cir. 2020), consumers sued Facebook for capturing, reading, and accessing the content of private messages without consent and in violation of the California Invasion of Privacy Act (CIPA), Cal. Penal Code § 630 *et seq.*, and the federal Wiretap Act, 18 U.S.C. § 2510 *et seq*. Like its federal counterpart, CIPA provides consumers a private right of action against anyone who unlawfully intercepts or uses information obtained from an electronic or digital communication. *Id.* at 1117. The Ninth Circuit recognized that wiretapping statutes have their origins in traditional privacy torts such as intrusion upon seclusion, and thus "bear a 'close relationship' to ones that have 'traditionally been regarded as providing a basis for a lawsuit.'" *Id.* (quoting *Spokeo*, 136 S. Ct. at 1549). The court noted that traditional privacy torts recognized that the intrusion itself caused sufficient harm to subject a defendant to liability. *Id.* Accordingly, the court rejected Facebook's assertion that violations of the statutes' prohibition against intercepting communications was not actionable under Article III without some showing that the illegally obtained information was used to cause additional harm to putative plaintiffs. *Id*. at 1118–19.

Further, in *In re Facebook Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020), the Ninth Circuit concluded that Facebook's practice of tracking consumers even if they were logged out of Facebook and visiting third-party websites gave rise

to a concrete injury. Consumers alleged that Facebook collected information regarding logged-out users' browsing history, allowing Facebook to create "a cradle-to-grave profile without users' consent," in violation of, among other things, the Wiretap Act and CIPA. *Id.* at 599. The court found that the plaintiffs had Article III standing because the provisions codified "a substantive right to privacy, the violation of which gives rise to a concrete injury." *Id* at 598. In addition, the Ninth Circuit found that the plaintiffs sufficiently alleged that Facebook's practice of collecting information would cause a material risk of harm to their interest in controlling their personal information. *Id.* at 598–99.

Finally, in a case concerning *amicus* Google's misuse of user data collected from cookies, the Third Circuit rejected the notion that internet companies like Google and Facebook may collect consumer data free from repercussion. *See In re Google Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3d Cir. 2019). The court reasoned that in "an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion ... that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data ... is untenable. Nothing in *Spokeo* or any other Supreme Court decision suggests otherwise." *Id.*

A common thread connecting these cases, and many others to which the Big Tech *Amici* object, is an effort by Congress and state legislatures to regulate the activity of companies that collect and use massive amounts of consumer data and to safeguard the important privacy interests that consumers have in preventing their personal

information from being misused. The resulting injury often may not be tangible, but the harm that results from violations of these statutes is very real.

After all, like an individual who has had their phone tapped, consumers that have their personal browsing history secretly collected or their faceprint collected and stored without consent intuitively understand that such activity alone harms them, regardless of whether the information wrongfully amassed is later used to financially penalize them in some way. Recognizing that new statutory schemes have been adopted to account for how privacy harms manifest in the digital age, federal courts have conferred standing on plaintiffs alleging violation of these statutes, allowing them to have their day in court and requiring companies such as the Big Tech *Amici* to answer for their conduct.

The claimed "in terrorem" effect of such class actions is illusory. To the extent that the Big Tech *amici* face potentially significant liability from privacy class actions, this liability does not stem from some dangerous flaw in courts' application of Article III standing doctrine or Rule 23. Rather, it stems from those companies' own aggregation and failures to properly handle unprecedented volumes of sensitive user information, which Congress and state legislatures have sought to protect from misuse or error. The proper way for companies to avoid such lawsuits is to alter their behavior and comply with privacy laws—not attack consumers asserting their rights and seeking redress.

V. Rule 23 provides an essential tool that enables classes of consumers to vindicate their legally protected interests.

Rule 23 class actions have long played in integral role in protecting consumer rights. *See Deposit Guar. Nat'l Bank v. Roper*, 445 U.S. 326, 339 (1980) ("Where it is not economically feasible to obtain relief within the traditional framework of a multiplicity of small individual suits for damages, aggrieved persons may be without any effective redress unless they may employ the class action device.").

In line with this approach, courts have widely held that the bar to meet the typicality standard of Rule 23 is low. *See DG ex rel. Stricklin v. Devaughn*, 594 F.3d 1188, 1195 (10th Cir. 2010) (stating that "every member of the class need not be in a situation identical to that of the named plaintiff" to satisfy typicality requirement); *Stewart v. Abraham*, 275 F.3d 220, 227 (3d Cir. 2001) ("Cases challenging the same unlawful conduct which affects both the named plaintiffs and the putative class usually satisfy the typicality requirements irrespective of the varying fact patterns underlying the individual claims."); *In re Prudential Ins. Co. Am. Sales Practice Litig. Agent Actions*, 148 F.3d 283, 311 (3d Cir. 1998) ("'Even relatively pronounced factual differences will generally not preclude a finding of typicality where there is a strong similarity of legal theories' or where the claim arises from the same practice or course of conduct.") (citations omitted); *Alpern v. UtiliCorp United, Inc.*, 84 F.3d 1525, 1540 (8th Cir. 1996) ("Factual variations in the individual claims will not normally preclude class certification if the

claim arises from the same event or course of conduct as the class claims, and gives rise to the same legal or remedial theory.").

Moreover, it is claims or defenses—not injuries—that must meet the typicality requirement of Rule 23. A statutory violation itself must be typical among class members in a Rule 23 class action, not the actual manifestation of the injury resulting from the violation. The text of Rule 23 is clear: only the class representative's "*claims or defenses*" must be typical to those of the putative class. Fed. R. Civ. P. 23(a)(3) (emphasis added). A requirement that plaintiffs must have manifested the exact same injury as a result of a statutory violation is inconsistent with the Rule's clear text and would upend decades of class action jurisprudence.

As the leading class-action treatise states, "If different damage amounts defeated typicality, it would be almost impossible to maintain a class suit since it is often the case that class members have suffered varying amounts of injury as a result of the defendant's actions." 1 *Newberg on Class Actions* § 3:43 (5th ed. 2011). Thus, "Courts routinely find that the proposed class representative's claims are typical even if the amount of damages sought differ from those of the class or if there are differences among class members in the amount of damages each is claiming." *Id.*

Here, all class members have asserted the same claims against TransUnion and sought statutory damages as their relief. While Mr. Ramirez may have suffered particularly severe harms, he asserted the same claims as the entire class and sought only the statutory damages available under the FCRA. Thus,

the "claims or defenses" at issue were typical across the class. Fed. R. Civ. P. 23(a)(3).

* * *

With great power comes great responsibility. *Cf. Kimble v. Marvel Entm't, LLC*, 576 U.S. 446, 465 (2015). As increasing amounts of data and sensitive information are entrusted to companies, often without consumer knowledge, those companies have an even greater responsibility to protect this data and ensure its accuracy. When they do not, consumers are harmed and they should have the ability to seek redress in federal court. Just as importantly, those consumers should be entitled to aggregate their claims through the class device as the underlying violations of the statute at issue are typical across all members of the class. This Court should affirm the Ninth Circuit's opinion and reject Petitioner's and the Big Tech *Amici's* attempt to re-write Article III and Rule 23.

CONCLUSION

The judgment of the Court of Appeals should be affirmed.

Respectfully submitted,

Cindy A. Cohn
Adam Schwartz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
adam@eff.org

James Pizzirusso
Counsel of Record
Michael D. Hausfeld
Ian Engdahl
HAUSFELD LLP
888 16th Street, N.W.
Suite 300
Washington, DC 20006
(202) 540-7200
jpizzirusso@hausfeld.com

March 10, 2021