No. 20-3202

IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

LATRINA COTHRON, individually,
and on behalf of those similarly situated,

Plaintiff-Appellee,

v.

WHITE CASTLE SYSTEM, INC.,

Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District of Illinois
No. 19-cv-00382
Hon. John J. Tharp, Jr.

BRIEF OF INTERNET ASSOCIATION AS AMICUS CURIAE IN SUPPORT OF DEFENDANT-APPELLANT

Lauren R. Goldman
Michael Brandon
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
(212) 506-2500
lrgoldman@mayerbrown.com
mbrandon@mayerbrown.com

Jed W. Glickstein
Counsel of Record
Matthew D. Provance
David S. Levine
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606
(312) 782-0600
jglickstein@mayerbrown.com
mprovance@mayerbrown.com
dlevine@mayerbrown.com

Counsel for Internet Association

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 20-3202

Short Caption: Cothron v. White Castle System, Inc.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

☐ **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):

Internet Association

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Mayer Brown LLP

(3) If the party, amicus or intervenor is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:

N/A

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ Jed W. Glickstein Date: 4/5/2021

Attorney's Printed Name: Jed W. Glickstein

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ☑ **No** ☐

Address: 71 S. Wacker Drive

Chicago, IL 60606

Phone Number: +1 312 782 0600 Fax Number: +1 312 701 7711

E-Mail Address: jglickstein@mayerbrown.com

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 20-3202

Short Caption: Cothron v. White Castle System, Inc.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

☐ **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):

Internet Association

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Mayer Brown LLP

(3) If the party, amicus or intervenor is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:

N/A

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ Lauren R. Goldman Date: 4/5/2021

Attorney's Printed Name: Lauren R. Goldman

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ☐ **No** ☑

Address: 1221 Avenue of the Americas

New York, New York 10020

Phone Number: +1 212 506 2500 Fax Number: +1 212 262 1910

E-Mail Address: lrgoldman@mayerbrown.com

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 20-3202

Short Caption: Cothron v. White Castle System, Inc.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

☐ **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):

Internet Association

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Mayer Brown LLP

(3) If the party, amicus or intervenor is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:

N/A

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ Matthew D. Provance Date: 4/5/2021

Attorney's Printed Name: Matthew D. Provance

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ☐ **No** ☑

Address: 71 S. Wacker Drive

Chicago, IL 60606

Phone Number: +1 312 782 0600 Fax Number: +1 312 701 7711

E-Mail Address: mprovance@mayerbrown.com

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 20-3202

Short Caption: Cothron v. White Castle System, Inc.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

☐ **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):

Internet Association

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Mayer Brown LLP

(3) If the party, amicus or intervenor is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:

N/A

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ Michael Brandon Date: 4/5/2021

Attorney's Printed Name: Michael Brandon

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ☐ **No** ☑

Address: 1221 Avenue of the Americas

New York, New York 10020

Phone Number: +1 212 506 2500 Fax Number: +1 212 262 1910

E-Mail Address: mbrandon@mayerbrown.com

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 20-3202

Short Caption: Cothron v. White Castle System, Inc.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

☐ **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):

Internet Association

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Mayer Brown LLP

(3) If the party, amicus or intervenor is a corporation:

i) Identify all its parent corporations, if any; and

N/A

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:

N/A

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ David S. Levine Date: 4/5/2021

Attorney's Printed Name: David S. Levine

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ☐ **No** ☑

Address: 71 S. Wacker Drive

Chicago, IL 60606

Phone Number: +1 312 782 0600 Fax Number: +1 312 701 7711

E-Mail Address: dlevine@mayerbrown.com

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Internet Association states that it is a trade association representing leading global internet companies on matters of public policy. Internet Association does not have any parent corporation and does not issue stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE

Internet Association ("the Association") represents more than 40 of the world's leading technology companies, from social networking services and search engines to travel sites and online marketplaces. The Association's members are Airbnb, Amazon, Ancestry, Discord, Doordash, Dropbox, eBay, Etsy, Eventbrite, Expedia Group, Facebook, Google, Groupon, Grubhub, Handy, IAC, Indeed, Intuit, LinkedIn, Lyft, Matchgroup, Microsoft, Notarize, PayPal, Pinterest, Postmates, Quicken Loans, Rackspace, Rakuten, Reddit, Snap Inc., Spotify, Stripe, SurveyMonkey, Thumbtack, Tripadvisor, Turo, Twitter; Uber, Upwork, VRBO, Zillow, and ZipRecruiter. *See* https://internetassociation.org/our-members (all websites cited in this brief were last visited on April 5, 2021).[1]

On behalf of its members, the Association advances policies that foster internet freedom, promote innovation, and empower small businesses and the public, and, equally importantly, that protect the privacy interests of users and consumers. As such, the Association has a strong interest in the proper application of laws that regulate emerging technologies, including Illinois's Biometric Information Privacy

[1] Pursuant to Fed. R. App. P. 29(a)(2), the Association states that all parties have consented to the filing of this brief. No party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund preparing or submitting this brief; and no person other than the Association, its members, and its counsel contributed money that was intended to fund preparing or submitting the brief. *See* Fed. R. App. P. 29(a)(4)(E).

Act ("BIPA"), 740 ILCS 14. The Association has filed several amicus briefs in federal and state courts regarding BIPA and related issues. *E.g.*, *Patel v. Facebook, Inc.*, No. 18-15982 (9th Cir. 2019); *Rosenbach v. Six Flags Entm't Corp.*, No. 123186 (Ill. 2018).

The issue presented in this case—which goes to the heart of BIPA's statutory scheme—is particularly important to the Association and its members. The Association agrees with Defendant-Appellant White Castle Systems, Inc. that under traditional accrual principles, BIPA 15(b) and 15(d) claims accrue once, upon the first alleged use or alleged disclosure of the plaintiffs' biometric data. But the district court's decision does not just conflict with Illinois accrual principles. It also conflicts with the text and structure of BIPA itself, threatening a flood of meritless claims against technology companies and those in many other sectors.

As explained below, the typical plaintiff bringing BIPA claims against a company seeks vast sums in statutory damages—in many cases, reaching into the billions of dollars. The decision below expands BIPA's reach even further, contrary to the intention of the General Assembly, and will result in more meritless litigation against the Association's members. The Association submits this brief to emphasize additional errors by the court below and the implications of that court's ruling for companies targeted in BIPA suits. It respectfully suggests that these provide additional reasons to reverse the decision of the district court.

INTRODUCTION AND SUMMARY OF ARGUMENT

The Illinois General Assembly enacted BIPA in 2008 to regulate the use of biometric technologies in "financial transactions and security screenings." 740 ILCS 14/5(a). In recent years, however, the plaintiffs' class action bar has deployed the statute with increasing frequency, and well outside the context that the General Assembly intended to regulate. In 2015, seven years after the statute was enacted, plaintiffs began filing BIPA class action claims against technology and other companies around the country. These included, for example, claims that companies violated BIPA by using facial-recognition or voice-recognition technology.[2]

Because BIPA's liquidated damages provisions allow plaintiffs' lawyers to claim up to $5,000 in damages per "violation," the claimed liability in these putative class action lawsuits is staggering. The decision below, taken to its logical conclusion, will raise these amounts to even more astronomical heights. The district court held that BIPA is separately "violated" each time a defendant "collects, captures, or otherwise obtains" or "discloses or otherwise disseminates" biometric data without consent. *Cothron v. White Castle Sys., Inc.*, 477 F. Supp. 3d 723, 732-33 (N.D. Ill. 2020). That will inevitably lead enterprising plaintiffs' lawyers to seek

[2] In many cases, plaintiffs may name not just the employer or end-user of the technology in question, but also various companies involved in its creation or distribution—as in this case, where the plaintiff initially named vendor Cross Match Technologies as a defendant before agreeing to a voluntary dismissal. *See Cothron v. White Castle Sys., Inc.*, No. 19-cv-382 (N.D. Ill.), Dkt. 43.

liquidated damages awards for tens, hundreds, or even thousands of "violations" allegedly suffered by each individual plaintiff as part of the exact same course of conduct. Such amounts, which could easily reach into the millions on a per-plaintiff basis, would be wildly disproportionate to any realistic appraisal of harm. Aggregated across a putative class, moreover, the potential liability would cripple virtually any defendant, putting enormous pressure on companies to settle wholly meritless claims.

As explained below, the district court's interpretation of BIPA is contrary to the statute's text, purpose, and structure. BIPA seeks to regulate, not annihilate, companies who use biometric technology. Consistent with that goal, the statute is calibrated to create liability for each violation of "a provision" of the Act—not each scan or disclosure of biometric data without consent. Even if there were doubt on this score, federalism and constitutional avoidance principles confirm the error of a liability-expanding approach.

In addition to being legal error, the district court's approach will encourage more gigantic class actions, lead to larger unjustified settlements, and chill innovation in numerous spheres that the General Assembly did not seek to regulate, let alone eliminate, when it passed BIPA in 2008. Given how aggressively litigants have used BIPA to go after emerging technologies, these consequences underscore why it is critical that this Court reject the district court's interpretation of the statute.

I. THE DISTRICT COURT MISCONSTRUED BIPA.

The court below concluded that BIPA is "violated" each time a defendant collects or discloses biometric data without consent. *Cothron*, 477 F. Supp. 3d at 732-33. As the court acknowledged, *id*. that construction would impose potentially crushing liability on businesses, which is entirely disproportionate to BIPA's "preventative and deterrent" purposes. *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1207 (Ill. 2019). That result should have signaled that the court's interpretive process had gone badly awry. The district court, however, was undeterred. Unsurprisingly, its conclusion regarding BIPA "violations" is flatly contrary to the statute's text and structure.

A. The District Court's Ruling Is Contrary To BIPA's Plain Text.

The district court's interpretation of "what constitutes a violation of BIPA's terms" (477 F. Supp. 3d at 731) centered on Section 15 of the statute, which lays out substantive obligations on private parties in connection with the retention, collection, disclosure, and destruction of biometric data. Two provisions are at issue in this case: Section 15(b), which prohibits the collection of biometric data without consent; and Section 15(d), which prohibits the disclosure of biometric data without consent.[3] According to the district court, these provisions are violated anew with each

[3] The remaining provisions address written retention policies, Section 15(a); the sale of biometric data to third parties, Section 15(c); and storage requirements for biometric data, Section 15(e).

collection or disclosure of biometric data. *Id*. at 733-34. As shown below, however, this conclusion is not tenable for a host of reasons.

1. To begin, the district court's interpretation has radical consequences for BIPA's overall structure. Section 20 of BIPA gives "[a]ny person aggrieved by a violation" of the Act the right to bring a cause of action in federal or state court. 740 ILCS 14/20. A private entity "that negligently violates a provision of th[e] Act" is liable for the greater of $1,000 or actual damages. 740 ILCS 14/20(1). A private entity that "intentionally or recklessly violates a provision of th[e] Act" is liable for the greater of $5,000 or actual damages. 740 IL 14/20(2).

By providing that liquidated or actual damages are recoverable for "each violation" of "***a provision***" of the Act (emphasis added), Section 20 makes clear that BIPA violations occur on a per-provision, rather than per-scan or per-disclosure, basis. A defendant that negligently collects a plaintiff's biometric data without consent violates Section 15(b) of BIPA and is liable to the plaintiff for $1,000 in liquidated damages, or actual damages if the plaintiff so elects. If that same defendant collects the same plaintiff's data multiple times as part of a continued course of conduct, no new "provision" of BIPA is violated. The plaintiff can still choose to recover actual or liquidated damages—but the plaintiff cannot recover $1,000 for each scan conducted without consent.

In opposing an interlocutory appeal, Plaintiff argued that the district court's

construction of a BIPA "violation" for purposes of Section 15 did not implicate damages under Section 20. *See* Pet. Opp. 21 (contending that awarding "damages for each separate biometric scan" is "a result never advanced by Plaintiff"). But "[o]ne of the fundamental principles of statutory construction is to view all provisions of an enactment as a whole. Words and phrases should not be construed in isolation, but must be interpreted in light of other relevant provisions of the statute." *Michigan Ave. Nat'l Bank v. Cty. of Cook*, 191 Ill. 2d 493, 504 (2000). Indeed, as the petition for interlocutory appeal noted, Illinois courts have consistently rejected the position advocated by Plaintiff because "taken to its logical conclusion" that approach "would lead [defendants] to potentially face ruinous liability." Mem. and Order at 5, *Robertson v. Hostmark Hosp. Grp.*, No. 18-CH-5194 (Ill. Cir. Ct. May 29, 2020), Pet. A24-A25; *see also* Mem. and Order at 3, *Smith v. Top Die Casting Co.*, No. 19-L-248 (Ill. Cir. Ct. Mar. 12, 2020), Pet. A39 ("the interpretation plaintiff desires would likely force out of business—in droves—violators who without any nefarious intent installed new technology and began using it without complying with section (b)").

Furthermore, in holding that a separate BIPA violation occurs with "every unauthorized scan or disclosure" of biometric data , the district court agreed that its construction portended astronomical damages. *Cothron*, 477 F. Supp. 3d at 733. The court "fully acknowledge[d]" what it (euphemistically) called the "large damage

awards that may result" from its reading of the statute. *Id*. And it conceded that its construction "may penalize violations severely," given that a plaintiff "can recover 'for each violation.'" *Id*. at 734 (quoting 740 ILCS 14/20). That Plaintiff apparently shares the view that it is wrong to assess damages on a per-scan basis thus is a powerful reason to reject the district court's interpretation.

2. Even severed from Section 20, the district court's reading of Section 15 makes no sense.

Section 15(b) is not focused on the collection of biometric data *per se*, but rather the importance of consent. As this court has explained, Section 15(b) "confers a right to receive *certain information* from an entity that collects, stores, or uses a person's biometric information." *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617, 621 (7th Cir. 2020) (emphasis added). Section 15(b) recognizes, moreover, that biometric data necessarily is collected, stored, and used for a "specific purpose" and "length of time." 740 ILCS 14/15(b)(2).

Once a defendant "fails to adhere to the statutory procedures and thereby denies someone the ability to make an informed decision about whether to provide her biometric identifier," "the right of the individual to maintain his or her biometric privacy vanishes into thin air." *Bryant*, 958 F.3d at 621 (quoting *Rosenbach*, 129 N.E.2d at 1206); *see also Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274 (9th Cir. 2019) (same). Thus, when a defendant collects the same information from the same

plaintiff without consent, there is no incremental harm to the interests Section 15 protects, and therefore no separate "violation."

The same is true of Section 15(d). Like Section 15(b), Section 15(d) is focused on consent rather than on disclosure of biometric data *per se*. And like Section 15(b), once biometric data is disclosed to a given third-party without consent, the injury targeted by Section 15(d) is complete. Additional disclosures of the same data to the same third parties for the same purposes inflicts no additional harm on the fundamental informational interest protected by the statute.[4]

3. The district court did not address BIPA's other substantive provisions, but its interpretation would lead to bizarre results there as well. *See Michigan Ave. Nat'l Bank*, 191 Ill. 2d at 504 (courts must construe statutes as a whole).

For instance, Section 15(a) requires private entities to develop a public written policy governing the retention and destruction of biometric data. *Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1150 (7th Cir. 2020). That provision obviously can be "violated" only once; it would make no sense to allow a plaintiff to sue each "time" a defendant fails to offer a public, written policy. Moreover, by requiring that a policy address "a retention schedule and guidelines for permanently destroying

[4] The district court noted that Section 15(d) addresses both the "disclosure" and the "redisclosure" of biometric data. 477 F. Supp. 3d at 733. That shows that a plaintiff who consents to a single disclosure can bring a claim if there is a subsequent re-disclosure without consent.

biometric identifiers and biometric information [*i.e.*, biometric data] when the initial purpose for collecting or obtaining such . . . information has been satisfied *or* within 3 years of the individual's last interaction with the private entity" (emphasis added), Section 15(a)—consistent with Section 15(b)(2)—explicitly recognizes that biometric data is collected for a continuing purpose, providing further confirmation that BIPA was not targeted at repeated collections or disclosures of the same information by the same entities.

Similar problems arise under Section 15(c). That provision prohibits the sale of biometric data. On the district court's logic, however, a defendant who intentionally sells biometric data to a third party would be liable for only $5,000 in liquidated damages, while a defendant who negligently discloses that same data to the same third party would be deemed to have "violated" the statute dozens or hundreds of times over. That is absurd. Surely the legislature would not have wanted to penalize companies that simply *disclose* biometric data to a third-party far more severely than companies which *sell* the data.

B. The District Court's Ruling Is Contrary To Other Interpretive Principles.

Other interpretive principles confirm that the district court was wrong to conclude that BIPA is separately violated each time a defendant collects or discloses biometric data without consent.

1. In crafting BIPA's private right of action, the General Assembly allowed a recovery of "liquidated damages" for each violation. 740 ILCS 14/20(1)-(2). Where, as here, the legislature uses a term in a statute that "has a settled legal meaning," courts "will normally infer that the legislature intended to incorporate the established meaning." *People v. Young*, 960 N.E.2d 559, 562 (Ill. 2011).

Liquidated damages in Illinois law have long been understood to refer to a *reasonable* estimate of harm—one that "bear[s] some relation to the damages that might occur." *Smart Oil, LLC v. DW Mazel, LLC*, 970 F.3d 856, 863 (7th Cir. 2020); *see also Pace Commc'ns, Inc. v. Moonlight Design, Inc.*, 31 F.3d 587, 593 (7th Cir. 1994) (under Illinois law, a liquidated damage clause is enforceable only if it appears to be "a good faith attempt to estimate what actual damages would be"). But providing liquidated damages for each separate scan or disclosure of the same biometric data to another party—in amounts that could easily reach into the millions of dollars per plaintiff—is not a "good faith" estimate of damages. It is a draconian penalty.

This cuts decisively against the district court's interpretation. When a liquidated sum is "far in excess of the probable damage on breach, it is almost certainly a penalty" and will be unenforceable. *Damages*, Black's Law Dictionary (11th ed. 2019) (defining "liquidated damages"); *cf. also Rosenbach*, 129 N.E.3d at 1205 (considering Black's Law Dictionary of "aggrieved" in interpreting BIPA).

The legislature would not have authorized "liquidated damages" for each BIPA violation if it believed that individual plaintiffs could show hundreds or even thousands of violations resulting from the exact same course of conduct.

2. What is more, if the General Assembly had intended to make each individual scan or disclosure of biometric data a separate violation, and in the process create potentially annihilative liability for defendants in the guise of "liquidated damages," it stands to reason that it would have said so clearly and expressly. *See Nelson v. Artley*, 40 N.E.3d 27, 35 (Ill. 2015) (rejecting interpretation that would subject certain companies to "unlimited liability" after finding "no clear reason why the legislature would have wanted" to do so); *Estate of Moreland v. Dieter*, 576 F.3d 691, 702 (7th Cir. 2009) (presuming that Indiana General Assembly did not "hide elephants in mouseholes" and thus rejecting interpretation that would subject a defendant to massive liability under state law). The absence of such evidence is particularly conspicuous because the General Assembly specified when it wanted continuing conduct to be treated as a separate violation, and when it wanted statutory damages to stack over time, in other statutes.[5]

[5] *See, e.g.*, 820 ILCS 325/5-20 ("Each day that a violation continues constitutes a separate violation."); 30 ILCS 570/7.15(a)(2) ("Each violation of this Act for each worker and for each day the violation continues constitutes a separate and distinct violation."); 815 ILCS 511/10(c) ("The injured person . . . may elect, in lieu of recovery of actual damages, to recover the lesser of $10 for each and every unsolicited electronic mail advertisement transmitted in violation of this Section, or $25,000 per day."); 720 ILCS 5/17-51(b)(5) (injured person "may elect . . . the

3. Finally, although the district court attempted to brush aside the dramatic implications of its ruling on two grounds, both were incorrect.

First, the Court suggested that the consequences of its decision were "not necessarily 'absurd'" because BIPA seeks to use liquidated damages to encourage compliance with the statute's goals of protecting biometric data. *Cothron*, 477 F. Supp. 3d at 733 (citing *Rosenbach*, 129 N.E.3d at 1207). But BIPA seeks to promote the use of biometric technology by regulating its use. As Illinois courts have recognized, *see* p. 7 *supra*, BIPA does not seek to make such technology radioactive. Indeed, the decision to cap liquidated damages thresholds at $5,000 and $1,000 per violation confirms that the legislature did *not* want to impose effectively unlimited liability on companies—even those that "intentionally or recklessly" violated BIPA's provisions. 740 ILCS 14/20(2).

Second, the district court argued that notwithstanding any absurdity, "where statutory language is clear, it must be given effect." *Cothron*, 477 F. Supp. 3d at 733. As shown above, however, the statutory language points in exactly the opposite direction. At a minimum, the statute is ambiguous as to when a "violation" occurs. The evident absurdity of the district court's interpretation thus is highly relevant. Courts routinely interpret statutes to avoid absurd or unjust consequences like those

---

greater of $10 for each unsolicited electronic mail advertisement transmitted in violation of this Section, or $25,000 per day.").

that flow from the district court's decision. *See, e.g.*, *People v. Casler*, – N.E.3d –, 2020 IL 125117, ¶ 24 ("a court presumes that the General Assembly did not intend absurdity, inconvenience, or injustice in enacting legislation"); *Dynak v. Bd. of Educ. of Wood Dale Sch. Dist. 7*, – N.E.3d –, 2020 IL 125062, ¶ 16 (same).

Federal law provides other analogues. In *Stillmock v. Weiss Markets, Inc.*, 385 F. App'x 267 (4th Cir. 2010), for instance, the court addressed a provision in the Fair and Accurate Credit Transaction Act that authorized consumers to recover statutory damages from a defendant who printed more than the last 5 digits of a credit card number on any receipt provided to the consumer at the point of sale. 15 U.S.C. §§ 1681c(g)(1), 1681n(a)(1)(A). The Fourth Circuit concluded that such damages "are to be awarded on a per-consumer basis"—*i.e.*, for each consumer whose card number was printed without truncation, regardless of how many times that occurred. 385 F. App'x at 272; *see also In re Trans Union Corp. Privacy Litig.*, 741 F.3d 811, 813 (7th Cir. 2014) (stating that § 1681n(a) "authorizes statutory damages . . . per consumer for willful violations").

As Judge Wilkinson explained, "Section 1681n provides that any person who willfully violates the statute 'with respect to *any consumer* is liable *to that consumer*' for, among other things, actual or statutory damages," reflecting "a per-consumer rather than a per-receipt approach to damages." *Stillmock*, 385 F. App'x at 275 n.* (Wilkinson, J., concurring in part); *compare* 740 ILCS 14/20 (authorizing recovery

only by a "person aggrieved"). "Were we to adopt a per-receipt approach," Judge Wilkinson continued, the statute "would be transformed from a shield for protecting consumer privacy into a sword for dismembering businesses." *Stillmock*, 385 F. App'x at 275 n.*. Here too, "[t]he potential for such abuse counsels against the plaintiffs' preferred . . . interpretation." *Id.*; *see also Friedman v. Live Nation Merchandise, Inc.*, 833 F.3d 1180, 1192 (9th Cir. 2016) (rejecting a "broad reading" of the statutory damages provision in the Copyright Act, which would "lead[] to extremely unlikely results, with direct infringers becoming liable for astronomical sums"); *Cmty. Television Sys. v. Caruso*, 284 F.3d 430, 435 (2d Cir. 2002) (imposing a "limiting construction" on the Federal Communication Act's descrambler provision to avoid unreasonably expansive statutory damages).

C. Federalism And Avoidance Principles Also Require Reversal.

Even assuming that the text and structure of the statute were not clear, two tiebreaking principles confirm the district court's error.

First, it is well-established that "when given a choice between an interpretation of state law which reasonably restricts liability, and one which greatly expands liability," federal courts "should choose the narrower and more reasonable path." *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 635-36 (7th Cir. 2007) (cleaned up); *see also, e.g.*, *Insolia v. Philip Morris Inc.*, 216 F.3d 596, 607 (7th Cir. 2000) ("When confronted with a state law question that could go either way, the federal

courts usually choose the narrower interpretation that restricts liability."). Contrary to this principle, the interpretation below does not just expand liability. It threatens to enlarge it to astronomical levels. *See* Part II *infra*.

Second, construing BIPA to create liability vastly disproportionate to the actual damages suffered would raise very serious due process concerns. *See, e.g.*, *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 416-17 (2003) ("The Due Process Clause of the Fourteenth Amendment prohibits the imposition of grossly excessive or arbitrary punishments on a tortfeasor."); *St. Louis, I.M. & S. Ry. Co. v. Williams*, 251 U.S. 63, 66-67 (1919) (statutory damages may violate due process where "the penalty prescribed is so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable"); *Golan v. FreeEats.com, Inc.*, 930 F.3d 950, 962 (8th Cir. 2019) (reducing statutory damages on account of due process principles).

Federal courts should construe state statutes to "avoid [constitutional] problems" unless such a construction is "plainly contrary to the intent" of the legislature. *Pub. Citizen v. U.S. Dep't of Justice*, 491 U.S. 440, 466 (1989) (collecting cases); *S. Utah Mines & Smelters v. Beaver Cty.*, 262 U.S. 325, 331 (1923) (where a state law is "susceptible of a construction which will . . . resolve all doubt in favor of [its] constitutionality, it is our duty to adopt it"); *Braun v. Ret. Bd. of Fireman's Annuity & Ben. Fund of Chi.*, 108 Ill. 2d 119, 127 (1985) (stating a

similar principle under Illinois law). Without a clear statement from the General Assembly that it intended to create constitutionally dubious and unnecessary liability, there is no basis for interpreting BIPA to achieve this result.

II. THE DISTRICT COURT'S RULING WILL DRAMATICALLY EXPAND LIABILITY AND CHILL INNOVATION.

The practical consequences of the district court's construction of BIPA underscore the urgent need for a course correction. Although the General Assembly passed BIPA to regulate the use of biometric technologies in financial transactions and security screenings in Illinois, in recent years, the plaintiffs' class action bar has deployed the statute against companies of all stripes. *E.g.*, *Crumpton v. Octapharma Plasma, Inc.*, 2021 WL 168965 (N.D. Ill. Jan. 19, 2021) (plasma-donation)*; Crooms v. S.W. Airlines Co.*, 459 F. Supp. 3d 1041 (N.D. Ill. 2020) (airlines); *Acaley v. Vimeo, Inc.*, 464 F. Supp. 3d 959 (N.D. Ill. 2020) (mobile applications); *Vance v. Int'l Bus. Machines Corp.*, 2020 WL 5530134 (N.D. Ill. Sept. 15, 2020) (technology company); *Salkauskaite v. Sephora USA, Inc.*, 2020 WL 2796122 (N.D. Ill. May 30, 2020) (cosmetics); *Gray v. U. of Chicago Med. Ctr.*, 2020 WL 1445608 (N.D. Ill. Mar. 25, 2020) (healthcare); *Rogers v. BNSF Ry. Co.*, 2019 WL 5635180 (N.D. Ill. Oct. 31, 2019) (railroads). And that is merely a sampling of recent cases in the Northern District.

Plaintiffs' lawyers file these massive no-injury class to leverage the difficulty in defeating BIPA claims on the pleadings in order to extract gigantic settlements

without any showing of harm. Any expansion of this status quo—let alone the sea change that the district court's interpretation would engender—would cripple many of these companies, harm consumers, and chill innovation in the important and emerging sphere of biometric technology.

This section makes three main points. *First*, the plaintiffs' class action bar already targets technology companies innovating in the biometric space, and given the difficulty in defeating these claims on the pleadings, can extract massive settlements on even weak or meritless claims. *Second*, adopting the district court's interpretation would turbocharge this trend and could lead to bankruptcy for even the most successful companies. *Third*, this result would harm consumers and significantly chill innovation in biometric technology—exactly the opposite of the General Assembly's purpose in passing BIPA.

A. By Targeting Innovative Companies, The Plaintiffs' Bar Seeks To Extract Massive Settlements On Weak Claims.

The plaintiffs' class action bar already targets technology and other companies under BIPA to extract massive settlements. That is so for several reasons. Among the most significant: such cases often involve enormous putative classes with significant potential exposure, and even meritless claims are exceedingly difficult to defeat without expensive discovery.

The first factor needs little explanation. In BIPA cases concerning the use of voice and facial recognition technology, putative classes often contain millions of

members. *See, e.g., In re Facebook Biometric Info. Priv. Litig.*, 2021 WL 757025, at *8 (N.D. Cal. Feb. 26, 2021) (estimating between 6.9 and 9.4 million class members); *In re TikTok, Inc., Consumer Privacy Litig.*, No. 20-CV-4699 (N.D. Ill.), Dkt. 122 at 17, 28 (estimating 1.4 million individuals in the BIPA sub-class). Even with current uncertainty regarding the meaning of "each violation," the exposure for these putative class actions can easily reach into the hundreds of millions or billions of dollars. Plaintiffs also perceive these technology companies as able to pay these astronomical amounts.[6]

A less obvious factor driving these lawsuits is that these high-exposure claims, even if meritless, are very difficult to defeat without expensive discovery. Part of the problem applies to all BIPA defendants: Even if the plaintiff signed a BIPA-compliant consent, fact questions may remain regarding the circumstances of the consent (*e.g.* whether it preceded the scan) and the treatment of the collected data (*e.g.* whether and how it was shared with a third party). This case provides a good example. The plaintiff did not plead details about the purportedly unlawful disclosure to third-parties, and the court held that this fact question could not be

[6] Employment class actions typically involve putative classes that are smaller by several orders of magnitude, although the consequences of liability for smaller firms can be similarly crippling. *E.g., Jones v. CBC Rest. Corp d/b/a Corner Bakery Café*, No. 1:19-cv-06736 (N.D. Ill. Oct. 22, 2020), Dkt. 53 (class of approximately 4,000 employees); *Fluker v. Glanbia Performance Nutrition, Inc.*, No. 2017-CH-12993 (Cook Cty. Cir. Ct. Aug. 20, 2020) (921 employees).

resolved without discovery and the attendant threat of gigantic damages.[7]

Part of the problem, however, is unique to technology-company defendants: They have innovative products that do not fit neatly into BIPA's definitions—a problem that is magnified because courts are seldom comfortable making technical determinations at the outset of the case.

In the *Facebook* litigation, for example, the plaintiffs challenged Facebook's "Tag Suggestions" feature, which makes it easier for people to tag friends in photos. BIPA expressly states that it does not regulate "information derived from" a "photograph." 740 ILCS 14/10. Yet when Facebook argued for dismissal on the basis that the statute "categorically excludes from its scope all information involving photographs," the district court deferred, noting that "as the facts develop, it may be that 'scan' and 'photograph' with respect to Facebook's practices take on technological dimensions that might affect the BIPA claims." *In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d 1155, 1171-72 (N.D. Cal. 2016).

[7] *Cothron*, 477 F. Supp. 3d at 732 n.7 (noting that one "question that may be of particular significance to liability under Section 15(d) is where the comparison takes place. Must White Castle send the newly collected fingerprint scan to one of the third parties in order for the comparison to be made at an off-site location or does White Castle retrieve the information from the off-site location such that the comparison takes place at the White Castle location?"); *see also, e.g.*, *Roberson v. Maestro Consulting Servs. LLC*, 2020 WL 7342693, at *12 (S.D. Ill. Dec. 14, 2020) (denying motion to dismiss because while "the BIPA Consent Forms are dated, Defendants have not shown that Plaintiffs were informed and consented before their biometric information was collected").

As new technologies emerge, the problems with applying BIPA's requirements will become only more acute. A particular technology may only *appear* to capture biometric data, for example—but expensive discovery would still likely be needed to establish that the technology does not in fact do so. *See, e.g.*, *In re Facebook Biometric Info. Priv. Litig.*, 2018 WL 2197546, at *2 (N.D. Cal. May 14, 2018) ("While the parties have no serious disagreement about the literal text of Facebook's source code, they offer strongly conflicting interpretations of how the software processes human faces."). The result is a tremendous potential for *in terrorem* settlements by defendants with strong cases but facing immense exposure—a serious problem identified by this and other courts. *E.g.*, *In re Rhone–Poulenc Rorer Inc.*, 51 F.3d 1293, 1297-98 (7th Cir. 1995) ("Judge Friendly, who was not given to hyperbole, called settlements induced by a small probability of an immense judgment in a class action 'blackmail settlements.' Judicial concern about them is legitimate . . . .") (citation omitted).[8]

[8] *See also AT&T Mobility LLC v. Concepcion*, 131 S. Ct. 1740, 1752 (2011) ("[W]hen damages allegedly owed to tens of thousands of potential claimants are aggregated and decided at once, the risk of an error will often become unacceptable. Faced with even a small chance of a devastating loss, defendants will be pressured into settling questionable claims."); *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 445 n.3 (2010) (Ginsburg, J., dissenting) ("When representative plaintiffs seek statutory damages, [the] pressure to settle may be heightened because a class action poses the risk of massive liability unmoored to actual injury."); *Kohen v. Pac. Inv. Mgmt. Co. LLC*, 571 F.3d 672, 677-78 (7th Cir. 2009) (noting the "*in terrorem* character of a class action"); *Thorogood v. Sears, Roebuck & Co.*, 547 F.3d 742, 745 (7th Cir. 2008) (similar).

B. The Ruling Below Will Lead To More Meritless Class Actions And Threaten A Host Of Companies.

As just shown, enormous potential liability, perceived deep-pocketed defendants, and claims that require expensive discovery regardless of merit are unfortunate features of BIPA class actions today. But the district court's opinion will worsen these trends, threatening crippling liability for even the most successful companies. To understand why, it helps to consider typical features of cases against technology-company defendants.

First, as explained above, the putative classes in technology-company cases often exceed one million members. *See* pp. 18-19 *supra*. This directly affects the defendant's potential exposure.

Second, this difference is exacerbated the number of potential "scans" or "disclosures" plaintiffs' lawyers might claim. In the consumer-technology context, individual consumers on any given day may upload hundreds of photographs and ask their digital assistants dozens of questions. *E.g.*, *Wilcosky v. Amazon.com, Inc.*, 2021 WL 410705 (N.D. Ill. Feb. 5, 2021) (Alexa digital assistant); *Hazlitt v. Apple Inc.*, 2020 WL 6681374 (S.D. Ill. Nov. 12, 2020) (Apple Photos); *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017) (Google Photos). As a result, the number of scans per individual—and thus the level of exposure under the district court's rule—can be nearly limitless.

Third, technology products are often open to members of the public, creating

an obvious potential for gamesmanship. Consider the BIPA plaintiff who deliberately uploads thousands of photographs in the hopes of increasing her liquidated damages, or the computer-savvy plaintiff who uses an automated process to do the same in even more dramatic fashion. The incentive to multiply claims in order to enlarge damages or increase settlement pressure reaches unacceptable levels under the district court's rule. *See, e.g.*, *Deutsche Bank Nat'l Tr. Co. v. Quicken Loans Inc*., 810 F.3d 861, 868 (2d Cir. 2015) (rejecting an interpretation that would "invite litigation gamesmanship"); *Stillmock*, 385 F. App'x at 275 n.* (Wilkinson, J., concurring in part) ("[o]pportunistic cardholders could intentionally make hundreds, if not thousands, of purchases, hoard their receipts, and stream into federal court to collect statutory damages on each one").

Imagine a conservative case: a company with 1 million users in Illinois with an active user base generating an average of 250 scans per user over the applicable statute-of-limitations period. If the collection were deemed "negligent" and thus subject to $1,000 per scan in liquidated damages under the district court's rule, the potential liability would be $250 billion. If deemed "intentional" or "reckless," the potential exposure would be $1.25 *trillion*. Even the most successful companies—whose user base or scan numbers might well exceed the conservative assumptions above—could face bankruptcy under this interpretation.

It is worth emphasizing again that these effects do not require that the claims

be supported by the facts. The district court's rule would usher in a regime where weak claims are easy to generate, difficult to defeat, and—if the weak claim should prove successful—ruinous to the defendant. That is not the regime the General Assembly envisioned in passing BIPA.

C. The District Court's Ruling Will Harm Consumers And Chill Innovation.

The district court's interpretation would not only prove ruinous for technology companies, but it would deter innovation and harm consumers, contrary to the General Assembly's intent in passing BIPA.

Consumers appreciate, enjoy, and increasingly expect features like voice and face recognition in the products and services they use. One recent publication, for instance, notes that nearly 40 million Americans currently own a smart speaker, 58% of people have used voice search to find information about a local business, and 72% of people who use voice search devices claim the devices have become part of their daily routines. *See* Denis Metev, Review42, *2020's Voice Search Statistics – Is Voice Search Growing?* (updated Mar. 8, 2021), https://review42.com/resources/voice-search-stats. By next year, 55% of households in the US are expected to own a smart speaker. *Id.*; *see also Wilcosky*, 2021 WL 410705, at *1 ("Digital assistants are a part of everyday modern life.").

The General Assembly has also recognized that such technology has tremendous potential for good. *See, e.g.*, 740 ILCS 14/5(a) (describing "streamlined

financial transactions and security screenings"); *Patel*, 932 F.3d at 1269 (recognizing "costs and benefits of biometric data use"). Using biometrics or similar technology, security cameras can recognize strangers outside a home, fingerprint readers can prevent access to sensitive information, and facial recognition systems can locate missing children online. As a recent report detailed, biometric technologies may soon be able to increase driver safety by identifying driver fatigue and school safety by identifying unauthorized individuals on school grounds. *See* CBInsights, *9 Industries Biometrics Technologies Could Transform* (Dec. 12, 2019), https://www.cbinsights.com/research/biometrics-transforming-industries/.

If BIPA is construed to impose colossal liability, far outstripping any actual damage, then companies will naturally be hesitant to develop these technologies, knowing that even meritless claims may lead to an unacceptable risk of a judgment from which a defendant could not recover. Alternatively, as the legal risks become unacceptable, companies may choose not to deploy their new technologies in Illinois. *See, e.g.*, Jack Nicas, *Why Google's New App Won't Match Your Face to Art in Some States*, Wall St. J. (Jan. 18, 2018), https://on.wsj.com/3wjID1w. Construing BIPA to apply even more punitively to easily alleged "violations" will exacerbate this trend, harming Illinois businesses, Illinois consumers, and the companies that serve them.

To be sure, in passing BIPA the legislature determined that the privacy

implications of biometric technologies require regulation. But the General Assembly achieved that purpose through generous liquidated damages awards and the potential for larger actual damages. There is no need to fundamentally transform the statute to achieve the legislature's preventative and deterrent goals.

In short, the district court's construction of BIPA would upend the balance struck by the legislature, discourage companies from developing new products, and incentivize companies to eliminate desirable technologies in their existing products for fear of liability. That is another reason the district court's interpretation should be rejected.

CONCLUSION

The Court should vacate the district court's order.

Dated: April 5, 2021

Respectfully submitted,

/s/ Jed W. Glickstein

Jed W. Glickstein
Counsel of Record
Matthew D. Provance
David S. Levine
MAYER BROWN LLP
71 S. Wacker Drive
Chicago, IL 60606
(312) 782-0600
jglickstein@mayerbrown.com
mprovance@mayerbrown.com
dlevine@mayerbrown.com

Lauren R. Goldman
Michael Brandon
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
(212) 506-2500
lrgoldman@mayerbrown.com
mbrandon@mayerbrown.com

Counsel for Internet Association

CERTIFICATE OF COMPLIANCE

This brief complies with: (1) the type-volume limitation of Circuit Rule 29 because it contains 6,221 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii); and (2) the typeface and type style requirements of Federal Rule of Appellate Procedure 32(a)(5) and (a)(6) and Circuit Rule 32 because the body and the footnotes of the brief have been prepared in 14-point Times New Roman font using Microsoft Word 2016.

Dated: April 5, 2021

/s/ *Jed W. Glickstein*
Jed W. Glickstein

Counsel for Amicus Curiae Internet Association

CERTIFICATE OF SERVICE

I hereby certify that on April 5, 2021, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Dated: April 5, 2021

/s/ *Jed W. Glickstein*
Jed W. Glickstein

Counsel for Amicus Curiae Internet Association