No. 18-398

IN THE
Supreme Court of the United States

FCA US LLC AND HARMAN INTERNATIONAL INDUSTRIES, INCORPORATED,
Petitioners,

v.

BRIAN FLYNN, GEORGE & KELLY BROWN, AND MICHAEL KEITH, INDIVIDUALLY AND ON BEHALF OF OTHERS SIMILARLY SITUATED,
Respondents.

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

MOTION FOR LEAVE TO FILE AND BRIEF FOR AMICI CURIAE CTIA–THE WIRELESS ASSOCIATION®, CAUSE OF ACTION INSTITUTE, AND ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL IN SUPPORT OF PETITIONERS

MEGAN L. BROWN
Counsel of Record
MATTHEW GARDNER
PETER HYUN
KATHLEEN SCOTT
BETHANY CORBIN
KRYSTAL B. SWENDSBOE
WILEY REIN LLP
1776 K Street, N.W.
Washington, DC 20006
(202) 719-7000
Mbrown@wileyrein.com

October 29, 2018

Additional counsel listed on the inside cover

JOHN J. VECCHIONE
CAUSE OF ACTION INSTITUTE
1875 Eye Street. N.W.,
Suite 800
Washington, D.C. 20006
(202) 499-2415

THOMAS C. POWER
JACKIE MCCARTHY
MELANIE TIANO
CTIA–THE WIRELESS
ASSOCIATION®
1400 16th Street, N.W.,
Suite 600
Washington, DC 20036
(202) 785-0081

Counsel for Amici Curiae

MOTION FOR LEAVE TO FILE BRIEF OF AMICI CURIAE CTIA–THE WIRELESS ASSOCIATION®, CAUSE OF ACTION INSTITUTE, AND ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

This case involves the application of Article III standing in the novel context of cybersecurity and the Internet of Things (IoT). The Court should grant the petition to address how *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), limits cases based on speculative claims about unexploited security vulnerabilities. Amici CTIA–The Wireless Association® ("CTIA"), the Cause of Action Institute "(CoA"), and Association for Unmanned Vehicle Systems International ("AUVSI") are deeply concerned with this case. As explained in the attached brief, a wave of litigation founded on speculative harm could have harmful consequences for security in emerging technologies and ongoing work to share information to enhance cybersecurity. Amici's participation will aid the Court by explaining how the standing doctrine is particularly important given the unique nature of IoT security.

Through counsel, Amici notified the parties of their intention to submit this amicus brief as soon as able, on October 23, 2018. Petitioners provided their consent to the filing of this brief. Respondents did not consent, although counsel represented that he had consented to the filing of two other amicus briefs in this matter. Therefore, pursuant to Supreme Court Rule 37.2(b), Amici respectfully move the Court for leave to file the attached amicus brief in support of Petitioners.

CTIA represents the U.S. wireless communications industry and companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. CTIA's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. CTIA regularly appears before the Court in cases presenting issues of importance to the wireless industry, including *City of Arlington, Texas v. FCC*, 569 U.S. 290 (2013), *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011), and *Stolt-Nielsen S.A. v. Animalfeeds Int'l Corp.*, 559 U.S. 662 (2010). CTIA and its members have promoted cybersecurity in connected technology for decades, including through its Cybersecurity Working Group which is made up of security professionals who develop security solutions to protect consumers.

CoA is a nonpartisan, nonprofit strategic oversight group committed to protecting permissionless technological innovation. CoA uses various tools to educate the public about government accountability, transparency, and the rule of law to protect liberty and economic opportunity. CoA appears as amicus curiae before this and other federal courts, see, e.g., *McCutcheon v. Fed. Elec. Comm'n*, 572, U.S. 185, 224 (2014) (citing CoA amicus brief), and frequently represents third-party clients in actions against the federal government to scale back regulatory overreach. For example, CoA has challenged the Federal Trade Commission's ("FTC") enforcement actions involving data security where there was no harm to the consumer, as here. *See, e.g., LabMD, Inc. v. FTC*, No. 1:14-cv-00810, 2014 WL

1908716 (N.D. Ga. May 12, 2014), *aff'd*, 776 F.3d 1275 (11th Cir. 2015); *In re LabMD, Inc.*, FTC No. 9357. CoA has an interest in this case because class actions like the one presented in this case threaten innovation and economic opportunity, and Article III standing is a cornerstone of the rule of law.

AUVSI is the world's largest nonprofit organization dedicated to advancing the unmanned systems and robotics community. AUVSI members support the defense, civil, and commercial sectors, and AUVSI coordinates with the government regularly to enhance UAS safety and operations. AUVSI believes that cyber innovation, and the unmanned systems industry in particular, has tremendous potential to transform technology. AUVSI has advocated both at the federal and state level for common-sense regulations on unmanned systems that will allow the industry to grow while ensuring the safety of operations.

Amici and their members are well-suited to explain the complex IoT security landscape, including vulnerability management, and the need to protect collaboration. Amici are also able to address the ramifications of the Seventh Circuit's decision on innovation and security. Amici therefore respectfully request leave to file the attached amicus brief urging this Court to grant the petition.

Respectfully submitted,

MEGAN L. BROWN
Counsel of Record
MATTHEW GARDNER
PETER HYUN
KATHLEEN SCOTT
BETHANY CORBIN
KRYSTAL B. SWENDSBOE
WILEY REIN LLP
1776 K Street, N.W.
Washington, DC 20006
(202) 719-7000
Mbrown@wileyrein.com

JOHN J. VECCHIONE
CAUSE OF ACTION INSTITUTE
1875 Eye Street. N.W.,
Suite 800
Washington, DC 20006
(202) 499-2415

THOMAS C. POWER
JACKIE MCCARTHY
MELANIE TIANO
CTIA–THE WIRELESS
ASSOCIATION®
1400 16th Street, N.W.,
Suite 600
Washington, DC 20036
(202) 785-0081

Counsel for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF CONTENTS

Page(s)

TABLE OF CITED AUTHORITIES

Page(s)

Cases

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

U.S. Constitution

Statutes

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

Other Authorities and Materials

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

TABLE OF CITED AUTHORITIES (Continued)

Page(s)

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

TABLE OF CITED AUTHORITIES
(Continued)

Page(s)

STATEMENT OF INTEREST[1]

Amici Curiae, CTIA–The Wireless Association® ("CTIA"), Cause of Action Institute ("CoA"), and the Association for Unmanned Vehicle Systems International ("AUVSI"), submit this brief in support of petitioners FCA US LLC and Harman International Industries, Inc. Amici are concerned about the impact that a wave of litigation founded on speculative harm from claimed vulnerabilities will have on the security of emerging technologies and government efforts to encourage information sharing.

CTIA represents the U.S. wireless communications industry and companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA has launched a

---

[1] Pursuant to Supreme Court Rule 37.6, no counsel for a party authored this brief in whole or in part, and no such counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amicus curiae, or its counsel, made a monetary contribution to its preparation or submission. As discussed in Amici's Motion for Leave, Petitioners have consented to the filing of this brief and both parties were provided notice on October 23, 2018.

cybersecurity certification program for Internet of Things devices. CTIA was founded in 1984 and is based in Washington, D.C. CTIA regularly appears before the Court in cases presenting issues of importance to the wireless industry, including *City of Arlington, Texas v. FCC*, 569 U.S. 290 (2013), *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011), and *Stolt-Nielsen S.A. v. Animalfeeds Int'l Corp.*, 559 U.S. 662 (2010). CTIA has an interest in this case because its members are on the front lines of technological innovation and Internet-connected device security. CTIA and its members have promoted cybersecurity in connected technology for decades, including through its Cybersecurity Working Group which is made up of security professionals who develop security solutions to protect consumers.

CoA is a nonpartisan, nonprofit strategic oversight group committed to protecting permissionless technological innovation. CoA uses various tools to educate the public about government accountability, transparency, and the rule of law to protect liberty and economic opportunity. CoA appears as amicus curiae before this and other federal courts, see, e.g., *McCutcheon v. Fed. Elec. Comm'n*, 572 U.S. 185, 224 (2014) (citing CoA amicus brief), and frequently represents third-party clients in actions against the federal government to scale back regulatory overreach. CoA has challenged the Federal Trade Commission's ("FTC") enforcement actions involving data security where there was no harm to the consumer, as here. CoA is particularly interested in challenges to the FTC's overreaching enforcement of Section 5 of the FTC Act, 15 U.S.C. § 45. CoA has

defended businesses, including LabMD, against FTC enforcement actions in federal courts. *See, e.g., LabMD, Inc. v. FTC*, No. 1:14-cv-00810, 2014 WL 1908716 (N.D. Ga. May 12, 2014), *aff'd*, 776 F.3d 1275 (11th Cir. 2015); *In re LabMD, Inc.*, FTC No. 9357. CoA has an interest in this case because class actions like the one presented in this case threaten innovation and economic opportunity, and Article III standing is a cornerstone of the rule of law.

AUVSI is the world's largest nonprofit organization dedicated to advancing the unmanned systems and robotics community. Serving members from government, industry and academia, AUVSI is committed to fostering, developing, and promoting unmanned systems and robotics technologies, including unmanned aircraft systems ("UAS"). AUVSI members support the defense, civil, and commercial sectors, and AUVSI coordinates with the government regularly to enhance UAS safety and operations. AUVSI believes that cyber innovation, and the unmanned systems industry in particular, has tremendous potential to transform technology. AUVSI has advocated both at the federal and state level for common-sense regulations on unmanned systems that will allow the industry to grow while ensuring the safety of operations.

SUMMARY OF THE ARGUMENT

Connected devices, referred to as the "Internet of Things" ("IoT"), promise a digital revolution. Innovative wireless communications technology is at the forefront of major changes to transportation,

health care, entertainment, and more. Experts predict 20 billion connected devices by 2020.[2]

The ubiquity of connected devices and services, compounded by complexities in supply chains and evolving security challenges, makes IoT ripe for exploitative litigation. As one commentator observed, "somewhere is a conclave of plaintiffs' lawyers wringing their hands waiting to file suits" over IoT security.[3] Respondents' counsel in this case told Black Hat security that "[a]ll conditions are ripe for a wave of these lawsuits."[4]

Respondents' claims rely on novel theories instead of actual exploitations or hacks. Respondents cite unexploited security vulnerabilities, the mere existence of which they claim renders their purchased products less valuable. If accepted, such a theory would encourage litigation against entities that collect and share information about vulnerabilities as well as entities that attempt to remedy vulnerabilities in their systems and devices. For example, litigants have brought thirty-two cases against a major technology company, alleging vulnerabilities in

---

[2] *See* Gartner, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* (Feb. 7, 2017), https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

[3] Mike Mimoso, *IoT Hacks May Bring Frenzy of Litigation*, Flashpoint BLOG (Aug. 21, 2018), https://www.flashpoint-intel.com/blog/iot-hacks-may-bring-frenzy-of-litigation/.

[4] *Id.*

microprocessors, which have never been exploited.[5] Vulnerabilities vary in complexity and severity; some are never proven and many are never exploited. The threat of litigation based on speculative and attenuated harm from newly discovered vulnerabilities will stymie innovation.

This lawsuit attempts to sidestep Article III's case or controversy requirement, which demands that litigants have standing. If successful, plaintiffs will unleash a wave of litigation over speculative and potential harms. This threatens to stifle innovation. Worse, such lawsuits will undermine security by distorting incentives to collaborate on and make public disclosures about vulnerabilities.

Class action litigation should not drive the nation's IoT cybersecurity policy. The Seventh Circuit's approval of class certification is legally flawed and will have adverse consequences across the economy. This Court should grant the Petition.

ARGUMENT

I. THE COURT SHOULD GRANT CERTORIARI AND REAFFIRM THE IMPORTANCE OF THE STANDING DOCTRINE.

---

[5] *See* Muvija M, *Intel Hit with 32 Lawsuits over Security Flaws*, Reuters (Feb. 16, 2018), https://www.reuters.com/article/us-cyber-intel-lawsuit/intel-hit-with-32-lawsuits-over-security-flaws-idUSKCN1G01KX.

A. Some Courts Ignore or Misapply this Court's Precedents When Evaluating Article III Standing Related to Cybersecurity.

Article III is a limit on judicial power. It limits federal court jurisdiction to actual cases or controversies. U.S. Const. art. III, § 2. One element of this bedrock requirement is that a plaintiff demonstrate standing. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

To have standing, a plaintiff must show injury-in-fact. This involves an invasion of a protected interest that is not only "concrete and particularized," but "'actual or imminent, not conjectural' or 'hypothetical.'" *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (citation omitted); *see Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990) ("That injury, we have emphasized repeatedly, must be concrete in both a qualitative and temporal sense.").

In *Clapper v. Amnesty International, USA*, this Court unambiguously held that "threatened injury must be *certainly impending,*" 568 U.S. 398, 409 (2013) (citation omitted). Imminence "cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes," and "[a]llegations of *possible* future injury are not sufficient." *Id.* (internal quotation marks and citation omitted). Where a theory of standing "relies on a highly attenuated chain of possibilities," it does not satisfy the legal requirement that injury be certainly impending. *Id.* at 410. "[T]heories that rest on speculation about the decisions of independent actors" will not be entertained by courts. *Id.* at 414.

The Court reaffirmed in 2016 that "Article III standing requires a concrete injury even in the context of a statutory violation." *Spokeo,* 136 S. Ct. at 1549. Even then, Article III is not satisfied where the violation "may result in no harm." *Id.* at 1550.

The Seventh Circuit's decision reflects the confusion in some courts about how to analyze injury under *Clapper*. This is particularly hazardous in the context of cybersecurity and data breaches after *Spokeo*. *See* Robert D. Fram, et al., *Standing in Data Breach Cases: A Review of Recent Trends*, 16 Class Action Litig. Rep. 1054, 1055 (Sept. 25, 2017). Lower courts have diverged in their application of *Clapper*, with some misapplying the doctrine when injury is hypothetical and not certainly impending.[6]

B. Respondents Fail to Allege a Cognizable Harm and Instead Offer Dissatisfaction with Common Security Practices.

Respondents fail to satisfy the injury threshold that this Court described in *Clapper*.

As purchasers and lessees of vehicles, Respondents' putative class action is based on alleged design flaws in connected phone, navigation, and

---

[6] Some courts have addressed standing of plaintiffs made vulnerable by data breaches, finding that a risk of future harm, even if stolen data had not been misused, was sufficient for standing purposes. *See, e.g.*, *Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017), *cert. denied,* 138 S. Ct. 981 (2018); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 391 (6th Cir. 2016); *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 345 (W.D.N.Y. 2018); *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 747 (S.D.N.Y. 2017).

entertainment controls. They rely on controlled research reported in a *Wired* article and reports and letters from Senators Markey and Blumenthal. The base allegation is that uConnect design vulnerabilities exposed Respondents to a risk of injury, *see* Pet. App. 11a, namely that "[i]f employed by a bad actor, a similar hack could affect thousands of vehicles at once, with catastrophic consequences," Sec. Am. Compl.¶ 27, *Flynn v. FCA US LLC,* No. 3:15-cv-855 (S.D. Ill. Sept. 21, 2017), ECF No. 246.

Despite asserting that the uConnect system is "exceedingly hackable," there is no allegation that Respondents' vehicles were hacked. *See id.* ¶ 18. As the lower court noted, only four owners in over one million made any claim of safety-related concern about *potential* hacking, and there has been no substantiated claim of injury. Pet. App. 11a.

Respondents' allegations boil down to an assertion that because a vulnerability has been identified by researchers, their cars should have been better designed. *See* Pet. App. 8a, 10a-16a. The operative complaint is full of critiques about the timing and distribution of updates, including generalized frustration about the lack of over-the-air ("OTA") updates, an innovation that was not widely used in cars until recently and is itself subject to concern by some advocates.[7]

---

[7] "With more opportunities for OTA maintenance and repairs, car owners could reap the benefits of saved time and hassle, and automakers and dealers could save some serious money . . . . It all sounds great. But several experts tell Consumer Reports that OTA updates could create some uncharted, if unintended, safety and security issues." Keith Barry, *Automakers Embrace Over-*

The unique nature of security vulnerabilities is detailed below and demonstrates why a claimed vulnerability in a connected device, without more, cannot constitute an injury cognizable under Article III. *See Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 723 (9th Cir. 2017). The mere presence of a vulnerability does not create actual or imminent harm. Exploitation and possible eventual harm "rel[y] on a highly attenuated chain of possibilities" that, in turn, depend on the actions of independent third parties. *Id.*; *see Clapper*, 568 U.S. at 410, 414.

The chain of events that would need to occur for an injury to befall Respondents is lengthy and involves speculation about the acts of third parties. As the district court explained, first, Respondents' automobiles would need to be hacked. Pet. App. 12a. This would require a skilled hacker, proficient enough to access and tamper with the vehicles remotely. *Id.* (noting that the research that generated the *Wired* article was conducted by individuals with physical access to the vehicles). Next, the hacker would need to access critical vehicle systems. Not only that, the hacker must manipulate or hijack those systems to interfere with the operation of the vehicle to cause harm. *Id.* Further, such a hack must occur despite the fact that a recall fixed numerous vulnerabilities that were referenced in the *Wired* article. *Id.*

---

the-Air Updates, But Can We Trust Digital Car Repair? (Apr. 20, 2018), https://www.consumerreports.org/automotive-technology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair/.

Respondents rely on a mountain of "ifs" that may never occur. The biggest "if"— the one that makes this case different than routine product defect cases— is the necessary occurrence of a deliberate criminal act by a third party in violation of at least one federal law, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

This is not enough under Article III. Respondents' feared harms can, in no way, be "certainly impending." *Clapper*, 568 U.S. at 409. A rejection of standing here is consistent with the Ninth Circuit's decision in the other lawsuit based on the *Wired* article, *Cahen v. Toyota Motor Corp.*, which found no the "alleged risks and defects [were] speculative." 717 F. App'x at 723. There, plaintiffs could not establish standing based on the mere possibility of a connected vehicle hack. *Id.*

The Seventh Circuit wrongly certified this class because, among other flaws,[8] Respondents' speculative injury is inadequate under Article III.

---

[8] Class certification is inappropriate where there is such diversity in class members. End users have different attitudes when it comes to security, including their interest in and willingness to accept updates. As the FTC observed of mobile device updates, "uptake depends on consumer deferrals and rejections. Forcing the device to update . . . improves the uptake rate but may bother users, particularly those who are actively attempting to avoid functionality changes." FTC, *Mobile Security Updates: Understanding the Issues* 32 (Feb. 2018), https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf (hereinafter "*FTC Mobile Security Report*"). Typicality and uniformity are elusive when speculating about action taken in response to vulnerabilities.

II. LITIGATION BASED ON SPECULATIVE HARM WILL UNDERMINE CYBERSECURITY IN IOT.

If Respondents can proceed on their novel theory of injury, innovators will face countless lawsuits based on speculation. This threat of litigation will stifle innovation and chill security work.

Lawsuits like this will change companies' incentives and raise concern about collaboration, which Congress and agencies have been trying to foster. The Cybersecurity Information Sharing Act of 2015 aimed to change incentives to share cybersecurity information by preventing lawsuits against companies that voluntarily share information in certain circumstances. *See* 6 U.S.C. § 1505. Lawsuits like Respondents' create the opposite incentive by threatening limitless potential liability for cyber vulnerabilities. A few examples illustrate this concern.

Patching and updating are a challenge. In IoT, supply and distribution chains are complex and security patches can face technical hurdles.[9] As the FTC noted, testing is one of the "reasons why a security update may take weeks, months, or even years to be completed."[10] As a National Telecommunications and Information Administration

---

[9] *See* U.S. Dep't of Homeland Security, *Recommended Practice for Patch Management of Control Systems* 1 (Dec. 2008), https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf.

[10] *FTC Mobile Security Report* at 3.

("NTIA") multi-stakeholder group observed, "[d]evices may have vulnerabilities that cannot reasonably be addressed through updates."[11] This requires mitigations and other efforts. Fear of litigation may change how companies approach updates, making them cautious about what they communicate to consumers or encouraging them to push out updates prematurely, before testing is complete.

Likewise, if litigation is based on how promptly a company notifies the public about vulnerabilities, companies may feel pressed to disclose too much, too soon. This would have negative consequences, including making it difficult for consumers to assess risk. Crowdstrike has observed "alert fatigue," in which "security teams are inundated with alerts, making it impossible for them to investigate and respond to each one. Consequently, a serious alert can be overlooked until it it's too late."[12] "[I]t's human nature to become inured to alerts if the majority of them are false."[13] So too will consumers grow weary of a barrage of vulnerability notifications, particularly when many pose no risk and there is little they might be able to do. National Institute of Standards and Technology ("NIST") researchers observed that

---

[11] IEEE, *Voluntary Framework for Enhancing Update Process Security* 2 (Oct. 31, 2017), http://sites.ieee.org/icps-ehe/files/2017/11/NTIA-IoT-Capabilities-Oct31-clean-File-16-118.docx.

[12] Falcon Product Team, *What Causes IT Alert Fatigue and How to Avoid it*, Crowdstrike BLOG (Apr. 21, 2017), https://www.crowdstrike.com/blog/causes-alert-fatigue-avoid/.

[13] *Id.*

"[u]sers are tired of being overwhelmed by the need to be constantly on alert, tired of all the measures they are asked to adopt. . . , and tired of trying to understand the ins and outs of online security. All of this leads to security fatigue, which causes a sense of resignation and a loss of control."[14] NIST's National Vulnerability Database has received 1,200 reports in October;[15] over-notifying consumers may do more harm than good.

This sort of lawsuit also risks undermining cooperation with the research community. Not only would researchers be sought by plaintiffs' counsel,[16] companies may be deterred from working with the research community out of fear that identification of vulnerabilities exposes them to litigation risk.

Respondents' theory threatens to distort incentives for information sharing and responsible risk management. The specter of the nearly half-billion dollar judgment sought here may cause

---

[14] Brian Stanton, et al., *Security Fatigue*, IT Prof., Sept.-Oct. 2016, https://inside.mines.edu/UserFiles/File/ccit/security/NIST-Security_Fatigue.pdf.

[15] NIST, *NVD Dashboard*, https://nvd.nist.gov/general/nvd-dashboard (last visited Oct. 26, 2018).

[16] Already, some firms have noted the effects of these types of cases and publicize their settlements. *See* Edelson, *Representative Cases*, https://edelson.com/inside-the-firm/privacy-and-technology/ (last visited Oct. 25, 2018). Respondents' attorney has said that "as there are more suits, plaintiff lawyers are going to be more knowledgeable and you'll end up with a snowball effect that takes off quickly. The plaintiffs' bar is talking about this. They're salivating over this. It's going to be a feeding frenzy." Mimoso, *supra* note 3.

companies to retreat from collaborating on vulnerabilities, as might discovery tactics. Respondents sought third party discovery about vulnerabilities from the Automotive Information Sharing and Analysis Center ("ISAC"), raising alarm about cooperation.[17] Litigation-driven caution could threaten the success of efforts to facilitate information sharing between the federal government and the private sector, like the Department of Homeland Security's new National Risk Management Center ("NRMC") and Secretary Nielsen's goals for "collective defense."[18] These are just a few of the worrisome consequences of permitting this case to proceed.

III. IOT DIVERSITY AND EVOLVING SECURITY THREATS REQUIRE COLLABORATION, NOT LITIGATION.

---

[17] *Cybersecurity, Information Sharing and Partnership*, Hearing Before Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce (Apr. 4, 2017) (Testimony of Denise Anderson), https://docs.house.gov/meetings/IF/IF02/20170404/105831/HHRG-115-IF02-Wstate-AndersonD-20170404.pdf (describing subpoena to Auto-ISAC, noting "the concern is that if courts were to allow broad sweeps for information and using ISACs as one-stop shops to accomplish it, such actions would effectively kill information sharing").

[18] *See* U.S. Dep't of Homeland Security, *Secretary Kirstjen M. Nielsen's National Cybersecurity Summit Keynote Speech* (July 31, 2018), https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech.

A. Connected Devices and Services Will Be Transformative.

Experts expect innovations in telemedicine, transportation, education, business processes, and consumer engagement. IoT innovations range from conveniences that make life easier (such as smart coffee makers) to life altering devices like wireless infusion pumps and self-driving cars.[19] "IoT is changing the way people live," and consumers are poised to "reap [the] benefits."[20] The economic benefit of IoT is expected to be in the trillions of dollars, with some predicting an impact of $11 trillion by 2025.[21] Over the next twenty years, IoT could add up to $15 trillion to global GDP.[22] IoT security is imperative and depends on industry collaboration, which is undermined by class action litigation.

---

[19] *See* U.S. Chamber of Commerce & Wiley Rein, LLP, *The IoT Revolution and Our Digital Security: Principles for IoT Security* 12 (2017), https://www.uschamber.com/IoT-security.

[20] *Id.* at 10.

[21] *See* James Manyika, et al., *Unlocking the Potential of the Internet of Things* 2, Mckinsey Global Institute (June 2015), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[22] Gil Press, *Internet of Things by the Numbers: Market Estimates and Forecasts*, Forbes (Aug. 22, 2014), https://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/#572d6173b919.

B. Security Vulnerabilities Vary in Severity and Risk of Exploitation.

Perfect security does not exist. Virtually every IoT system and device will confront security issues and need updates and patches. This is because security is not static; bad actors experiment with tactics, and research reveals issues not contemplated by product designers.

To put this case in context, it is important to understand what a "vulnerability" in a connected device or system means. Though definitions vary, a "vulnerability" is commonly understood to be "a weakness in an information system . . . that ***could*** be exploited by a threat source."[23] IoT vulnerabilities are avenues for potential harms, but they do not equate to an injury necessary to find standing.

The existence of a vulnerability does not mean that harm is inevitable or that there is a real risk. Some vulnerabilities are theoretical and difficult to validate.[24] Even when there is a proof of concept, not all vulnerabilities are of the same severity.

Vulnerabilities are validated and assessed by a range of actors. The government maintains databases of more than 100,000 vulnerabilities of

---

[23] NIST, *Guide for Conducting Risk Assessments* 9 (Sept. 2012), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (emphasis added).

[24] Anthony Alves, *Vulnerable vs. Exploitable: Why These are Different & Why it Matters*, Threat Stack (June 13, 2017), https://www.threatstack.com/blog/vulnerable-vs-exploitable-why-these-are-different-why-it-matters.

varying seriousness.[25] Private entities also look for vulnerabilities, from Google's Project Zero[26] to malicious actors looking to do harm. The security research community rates vulnerabilities low, medium, high, or critical, using the Common Vulnerability Scoring System ("CVSS"), based on the likelihood of exploitation and the potential impact of exploitation. The CVSS shows that not all vulnerabilities have the same potential for harm.

This is why, in order to effectively address IoT security, companies prioritize vulnerabilities in terms of risk. According to Verizon's Data Breach Investigations Report, companies "may have longer or shorter patch cycles that are dependent on the particular vulnerabilities discovered."[27] Verizon advises that "organizations will need to factor in threat rates as well as potential impact to establish their own time-to-patch duration."[28] Companies should not be punished for risk management, which requires weighing relative severity, ease of exploitation, and difficulties in patching, among other mitigations.

---

[25] NIST, *National Vulnerability Database*, https://nvd.nist.gov/ (last visited Oct. 23, 2018); MITRE, *Common Vulnerabilities and Exposures*, https://cve.mitre.org/ (last updated Oct. 11, 2018).

[26] *See* Margaret Rouse, *Google Project Zero*, SearchSecurity, https://searchsecurity.techtarget.com/definition/Google-Project-Zero (last updated Apr. 2015).

[27] Verizon, *2017 Data Breach Investigations Report* 13, https://enterprise.verizon.com/content/dam/resources/reports/2017/2017_dbir.pdf (hereinafter "*Verizon DBIR Report*").

[28] *Id.*

C. IoT Security Requires Unprecedented Collaboration.

1. IoT Security is Layered Across Devices, Networks and People.

As the President's National Security Telecommunications Advisory Committee observed, "the IoT is made up of devices, transport networks, applications, and the companies and users deploying them. Each segment confronts threats and requires attention."[29] Interconnection between "humans, non-human physical objects, and cyber objects" is "complex and inherits a core set of trust concerns, most of which have no current resolution."[30] As a result, IoT security is layered and requires work at the device, enterprise, and system levels. "The nature of the endpoints and the sheer scale of aggregation require special attention in the overall architecture to accommodate [IoT] challenges."[31]

---

[29] NSTAC, *Report to the President on Internet and Communications Resilience* § 2.1 (2018), https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20DRAFT%20-%20508%20compliant.pdf.

[30] NIST, *Internet of Things (IoT) Trust Concerns* (Oct. 17, 2018), https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/10/17/iot-trust-concerns/draft/documents/iot-trust-concerns-draft.pdf.

[31] Cisco, *Securing the Internet of Things: A Proposed Framework*, https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html (last visited Oct. 26, 2018).

This complexity requires industry and government to collaborate. One area of collaboration is the security of code that goes into devices and systems. Consider the NTIA's Software Component Transparency initiative.[32] Other groups look at supply chain and application development, and efforts are underway to educate consumers about their role in accepting security updates. The FTC has evaluated the complexities of updating mobile devices and observed that "[t]he more consumers understand the importance of updates, the more likely they are to install available updates."[33] As discussed above, litigation like this undermines collaboration by diminishing the trust of consumers and the willingness of private actors to work together on information sharing.

2. Vulnerability Management is Complex.

Respondents gloss over complexities in vulnerability management by critiquing FCA and Harman for everything from their response to a *Wired* article to "problems associated with [their] method for delivering the software patch." Sec. Am. Compl. ¶ 42, ECF No. 246. Respondents overlook the complexities and challenges of managing security vulnerabilities.

---

[32] The Software Component Transparency initiative "explore[s] how manufacturers and vendors can communicate useful and actionable information about the third-party software components that comprise modern software and IoT devices," NTIA, *Software Component Transparency*, https://www.ntia.doc.gov/SoftwareTransparency (last visited Oct. 25, 2018).

[33] *FTC Mobile Security Report* at 5.

Cybersecurity vulnerabilities are part of overall "risk management," in which companies balance risk and do not strive for perfection.

As an initial matter, companies may not be able to immediately evaluate the validity or seriousness of a claimed vulnerability in the immediate aftermath of its discovery. "Bug bounty" programs, in which companies offer incentives for experts to identify vulnerabilities, may help,[34] but the research community has varied motives. Some push the bounds of ethical and legal behavior.[35] Even if verified, most vulnerabilities are unlikely to be exploited, and, if they are exploited, they would result in minimal harm.[36]

---

[34] For example, the Department of Defense partnered with HackerOne for the first federal bug bounty program. *See* U.S. Dep't of Defense, *Defense Secretary Ash Carter Releases Hack the Pentagon Results* (June 17, 2016), https://dod.defense.gov/News/News-Releases/News-Release-View/Article/802929/defense-secretary-ash-carter-releases-hack-the-pentagon-results/. 1,400 hackers participated and discovered 138 unique vulnerabilities. *Id.*

[35] In 2016, Muddy Waters Capital LLC released a report claiming that pacemakers created by St. Jude Medical, Inc., were vulnerable to cyberattacks that could effectively stop the devices from functioning. See Jim Finkle, et al., *St. Jude Stock Shorted on Heart Devise Hacking Fears; Shares Drop*, Reuters (Aug. 25, 2016), https://www.reuters.com/article/us-stjude-cyber-idUSKCN1101YV. Just before releasing the vulnerability report, Muddy Waters shorted St. Jude's stock, allowing it to profit when the stock dropped after the report became public. *Id.*

[36] As noted, more than 100,000 vulnerabilities have been cataloged. Approximately half are "Low" or "Medium," severity. CVE Details, *Current CVSS Score Distribution for All*

There are also misconceptions about the benefits of public disclosure. It is incorrect to assume that all vulnerabilities should be made public or communicated directly to consumers. Finding a possible vulnerability is distinct from developing a solution.[37] Unlike traditional consumer products, nefarious third parties, including nation states, hacktivists and terrorists, seek to exploit vulnerabilities.[38] Alerting the public alerts potential attackers.[39] Responsible vulnerability disclosure is

---

Vulnerabilities, https://www.cvedetails.com/cvss-score-distribution.php (last visited Oct. 25, 2018).

[37] When Google's Project Zero identifies a vulnerability, it generally allows ninety days for the responsible company to fix it before announcing it to the public. On several occasions, companies have been unable to fix vulnerability within that timeframe. *See* Rohith Bhaskar, *Google's Project Zero Discloses a Vulnerability in Microsoft Edge*, PC Mag. (Feb. 20, 2018), https://in.pcmag.com/google-1/119237/googles-project-zero-discloses-a-vulnerability-in-microsoft.

[38] *See Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*, Hearing Before the Subcomm. on Terrorism and Illicit Finance of the H. Comm. on Financial Services (Mar. 15, 2018) (Testimony of Lillian Ablon), https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf.

[39] For example, on April 7, 2014, researchers identified a vulnerability, Heartbleed, in protocols that facilitate a large percentage of web traffic. The same day a patch was released, and the race was on. Companies and governments scrambled to deploy patches, change passwords and adapt their networks to prevent attacks as hackers began exploiting the now widely publicized vulnerability. *See* CTIA, *Today's Mobile Security: Information Sharing* 16, https://api.ctia.org/docs/default-

imperative. It may be entirely reasonable not to disclose claimed vulnerabilities if, for example, there is little risk of exploitation. Premature or inappropriate disclosure—which fear of litigation may prompt—would alarm consumers or inure them to security issues that do require action.

These considerations necessitate coordination, not recrimination. "Vulnerability disclosure can be a complicated process, especially when multiple parties (usually multiple vendors) are involved," as is often the case in complex systems and the IoT.[40] As the House Energy and Commerce Committee recognized, often "organizations do not discover [security] incidents on this own—they are told by outside parties."[41] Groups like HackerOne and Bug Crowd help companies evaluate their own products and services and advise on policies that "give[] ethical hackers clear guidelines for reporting potentially unknown and harmful security vulnerabilities."[42]

---

source/default-document-library/ctia_informationsharing.pdf (last visited Oct. 25, 2018).

[40] Forum of Incident Response and Security Teams, Inc., *Guidelines and Practices for Multi-Party Vulnerability Coordination* 6 (Fall 2016), https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination-draft.pdf.

[41] U.S. H. Energy and Commerce Comm., Majority Staff, *The Criticality of Coordinated Disclosure in Modern Cybersecurity* (Oct. 23, 2018), https://energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf.

[42] HackerOne, *Here Are the 5 Critical Components of a Vulnerability Disclosure Policy*, https://ma.hacker.one/rs/168-

Each element of cybersecurity coordination is critical to managing vulnerabilities. As experts note, it is not possible or desirable to "patch" every vulnerability; sometimes other mitigations are appropriate.[43] It is only by working together that the security of devices and systems improves.

3. The Government Promotes Collaboration to Address Security Vulnerabilities, Which the Private Sector is Leading.

The government recognizes the need for cooperation and has sought to increase communication with the private sector about vulnerabilities, threat indicators, and defensive measures. In 2015, Congress enacted the Cybersecurity Information Sharing Act, which provides authority and protection for cybersecurity information sharing between and among the private sector and the government.[44]

In 2018, the Department of Homeland Security ("DHS") announced the creation of the NRMC to facilitate contextualized sharing of information

---

NAU-732/images/5-critical-elements-vdp-guide-1pager.pdf (last visited Oct. 25, 2018).

[43] *See Verizon DBIR Report* at 13.

[44] See U.S. Dep't of Homeland Security & Dep't of Justice, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities Under the Cybersecurity Information Sharing Act of 2015* (June 15, 2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

between the federal government and the private sector on a cross-sector basis.[45] Several parts of DHS promote vulnerability disclosure programs, including the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"). ICS-CERT created the ICS-CERT Vulnerability Policy to "balance the need of the control system community to be informed of security vulnerabilities with the vendors' need for time to respond effectively."[46]

The Department of Justice ("DOJ") provides a *Framework for a Vulnerability Disclosure Program for Online Systems*.[47] The DOJ emphasized in its *Cyber Digital Task Force Report* the need for "building relationships and sharing cyber threat information" but recognized that it "initially may seem difficult to achieve, given concerns about

---

[45] U.S. Dep't of Homeland Security, *National Risk Management Center (NRMC)*, https://www.dhs.gov/national-risk-management-center (last visited Oct. 26, 2018).

[46] ICS-CERT, *ICS-CERT Vulnerability Disclosure Policy*, https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy (last visited Oct. 25, 2018).

[47] U.S. Dep't of Homeland Security, Cybersecurity Unit, Computer Crime & Intellectual Property Section Criminal Division, *A Framework for a Vulnerability Disclosure Program for Online Systems* (July 2017), https://www.justice.gov/criminal-ccips/page/file/983996/download.

privacy, legal privileges, and the protection of sensitive information."[48]

The private sector is actively working on IoT security. Industries formed ISACs and Information Sharing and Analysis Organizations ("ISAOs") to share information, including about vulnerabilities. They "help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards."[49] The communications sector and other sectors work on vulnerabilities. Connected car development is one of the fastest growing IoT markets, and many groups offer multi-layered security.[50] "[T]he Auto-ISAC is the central hub for coordination and communication around industry-wide sharing of cyber threats and vulnerabilities to the connected vehicle."[51]

---

[48] U.S. Dep't of Justice, *Report of the Attorney General's Cyber Digital Task Force* 83 (July 2, 2018), https://www.justice.gov/ag/page/file/1076696/download.

[49] National Council of ISACs, Homepage, https://www.nationalisacs.org/ (last visited Oct. 25, 2018).

[50] *See, e.g.,* Trend Micro, *Cybersecurity Solutions for Connected Vehicles* (2017), https://www.trendmicro.com/us/iot-security/content/main/document/IoT%20Security%20for%20Auto%20Whitepaper.pdf; IMS, *Deploying a Connected Car Solution with Confidence*, Deploying-Connected-Car-Solutions-with-Confidence.pdf (last visited Oct. 23, 2018).

[51] ISAO Standards Organization, *Automotive ISAC*, https://www.isao.org/information-sharing-group/sector/automotive-isac/ (last visited Oct. 25, 2018).

Industry stakeholder organizations are creating security programs to address the evolving nature of cybersecurity threats and responses. CTIA created a voluntary Cybersecurity Certification Program for IoT, with minimum criteria for security and privacy including "automatic and manual installation of unmodified software patches . . . to correct software problems and fix vulnerabilities."[52] CTIA's Authorized Test Labs will be ready to accept devices for testing in October 2018. Underwriters Laboratories administers its Cybersecurity Assurance Program, which tests and certifies network-connectable IoT products and systems.[53] Other organizations have best practices and protocols addressing IoT security. The Institute of Electrical and Electronics Engineers ("IEEE") produced the *Internet of Things (IoT) Security Best Practices* white paper in February 2017,[54] and is working on *IEEE*

---

[52] CTIA, *Cybersecurity Certification Test Plan for IoT Devices*, part 3.5 (Aug. 2018), https://api.ctia.org/wp-content/uploads/2018/08/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1_0.pdf

[53] Underwriters Laboratories, *UL Cybersecurity Assurance Program (UL CAP)*, https://services.ul.com/service/ul-cybersecurity-assurance-program-ul-cap/ (last visited Oct. 23, 2018).

[54] IEEE Internet Technology Policy Community White Paper, (Feb. 2017), https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf.

2413 – Standard for an Architectural Framework for the Internet of Things (IoT).[55]

These are just a few examples of innovative work on IoT security, which demonstrate the importance of flexible, iterative approaches. Using class actions to second-guess and punish companies' vulnerability management decisions—particularly without any demonstrated harm—will undermine these efforts.

CONCLUSION

Permitting standing based on unexploited vulnerabilities contravenes this Court's teachings in *Clapper* and risks stifling innovation. For the reasons set forth herein and in the Petition, Amici Curiae respectfully request that this Court grant Petitioners' Petition for Writ of Certiorari.

---

[55] IEEE Standards Association, *Project Details*, https://standards.ieee.org/project/2413.html (last visited Oct. 23, 2018); *see also* ATIS, *Securing Internet of Things (IoT) Services Involving Network Operators* (May 2017), https://www.atis.org/docstore/product.aspx?id=28313; GSMA, *IoT Security Guidelines* (Oct. 31, 2017), https://www.gsma.com/iot/wp-content/uploads/2018/08/CLP.-11-v2.0.pdf.

Respectfully submitted,

MEGAN L. BROWN
Counsel of Record
MATTHEW GARDNER
PETER HYUN
KATHLEEN SCOTT
BETHANY CORBIN
KRYSTAL B. SWENDSBOE
WILEY REIN LLP
1776 K Street, N.W.
Washington, DC 20006
(202) 719-7000
Mbrown@wileyrein.com

JOHN J. VECCHIONE
CAUSE OF ACTION INSTITUTE
1875 Eye Street. N.W.,
Suite 800
Washington, DC 20006
(202) 499-2415

THOMAS C. POWER
JACKIE MCCARTHY
MELANIE TIANO
CTIA–THE WIRELESS
ASSOCIATION®
1400 16th Street, N.W.,
Suite 600
Washington, DC 20036
(202) 785-0081

Counsel for Amici Curiae

October 29, 2018